Brought to you by:

Symantec

Advanced Endpoint Security

for dummies®

A Wiley Brand

Stay ahead of the evolving threat landscape

Prevent ransomware and emerging threats

Save resources with simplified EDR

Naveen Palavalli

Symantec Special Edition

About Symantec

Symantec Corporation (NASDAQ: SYMC), one of the world's leading cyber security companies, helps organizations, governments, and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud, and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on Facebook, Twitter, and LinkedIn.

Advanced Endpoint Security

Symantec Special Edition

by Naveen Palavalli

for dummies®
A Wiley Brand

Advanced Endpoint Security For Dummies®, Symantec Special Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate Chichester, West Sussex, www.wiley.com

ISBN 978-1-119-48792-0 (pbk); ISBN 978-1-119-48793-7 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz or visit www.wiley.com/go/custompub. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Project Editor/Development Editor: Chad R. Sievers

Executive Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Frazer Hossack

Dummies Marketing: Jennifer Webb

Production Editor: Tamilmani Varadharaj

Table of Contents

Introduction

Today's workforce is increasingly nomadic. Employees use personal and company-owned devices — desktops, laptops, tablets, and smartphones with various operating systems — to access corporate resources over different networks from virtually anywhere. Roaming users and cloud-based applications have eroded the network perimeter where enterprises have traditionally focused their security controls.

In the wake of this disruption, vendors offered myriad point products that solve only a portion of the security problem. These products usually require costly custom integrations and high management overhead to boot.

Making matters worse, traditional security approaches can't address an evolving threat landscape that includes ransomware, stealthy attacks that dwell in a customer's environment for months, and threats targeting iOS and Android devices. In fact, the mobile workforce is more vulnerable than ever before.

About This Book

Advanced Endpoint Security For Dummies, Symantec Special Edition, consists of nine chapters that explore the following:

- The threat and vulnerability landscape, the attack life cycle, and a security framework for next-generation endpoint security (Chapter 1)
- Next-generation endpoint protection technologies including machine learning, exploit prevention, behavior monitoring, and more (Chapter 2)
- Application isolation and control techniques such as endpoint hardening, blacklisting/whitelisting, and application isolation (Chapter 3)
- The role of deception in modern cyberwarfare (Chapter 4)
- Important detection and response capabilities including threat analytics, cloud-based threat intelligence, and remediation (Chapter 5)

- The need to protect mobile devices (Chapter 6)
- The importance of effective patch management (Chapter 7)
- Endpoint security integration with enterprise systems such as web and email gateways, security information and event management (SIEM), and ticketing systems (Chapter 8)
- Endpoint security tips (Chapter 9)

And just in case you get stumped on any acronyms or terms, you can refer to a helpful glossary in the back of the book.

Foolish Assumptions

Mainly, I assume that you're an information technology leader, such as a chief information officer (CIO); chief information security officer (CISO), director, or manager; or a network or systems engineer or administrator. As such, I wrote this book primarily for technical readers, but if you're not technical don't be alarmed. I still explain any technical terms.

If any of these assumptions describe you, then this book is for you. If none of these assumptions describe you, keep reading anyway. It's a great book, and when you finish reading it, you'll know a quite a few things about endpoint protection.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:


REMEMBER

This icon points out information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays.


TIP

Tips are appreciated, never expected — and I sure hope you'll appreciate these tips. This icon points out useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not); they offer practical advice to help you avoid potentially costly or frustrating mistakes.

TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of nerd-vana, perk up. This icon explains the jargon beneath the jargon.

Where to Go from Here

With my apologies to Lewis Carroll, Alice, and the Cheshire cat:

"Would you tell me, please, which way I ought to go from here?"

"That depends a good deal on where you want to get to," said the Cat — err, the Dummies Man.

"I don't much care where . . .," said Alice.

"Then it doesn't matter which way you go!"

That's certainly true of *Advanced Endpoint Security For Dummies,* Symantec Special Edition, which, like *Alice in Wonderland,* is also destined to become a timeless classic.

If you don't know where you're going, any chapter will get you there — but Chapter 1 might be a good place to start. However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand alone, so you can read this book in any order that suits you (though I don't recommend upside down or backward).

I promise you won't get lost falling down the rabbit hole!

IN THIS CHAPTER

- Surveying the current threat landscape
- Examining the attack cycle
- Defining next-generation endpoint security

Chapter 1
Getting Started with Endpoint Security

In this chapter, you find out about evolving threats and vulnerabilities, the attack cycle, and a security framework for next-generation endpoint security.

The Evolving Threat Landscape

Cybercrime is big business. Cybersecurity Ventures estimates that by 2021, cyberattacks will cause $6 trillion in damages worldwide. As attackers evolve their tactics and use ever more sophisticated techniques to infiltrate networks, traditional security approaches are no longer adequate to address the rapidly evolving threat landscape.

Attackers continuously adapt to organizations' defenses by creating new variants of malware designed to evade network and endpoint security. The 2018 *Internet Security Threat Report* (ISTR) shows an enormous number of malware variants — nearly two

million — being detected every day (see Figure 1-1). The report also found the following:

- Ninety percent of targeted attack groups are motivated by intelligence gathering.
- Ransomware attacks increased 40 percent, and the number of ransomware variants was up 46 percent.
- 7.1 billion identities have been exposed in data breaches in the last eight years.
- One in 13 URLs analyzed at the gateway were found to be malicious. In 2016, this number was 1 in 20.
- The number of newly discovered mobile malware variants grew by 54 percent from 2016 to 2017.

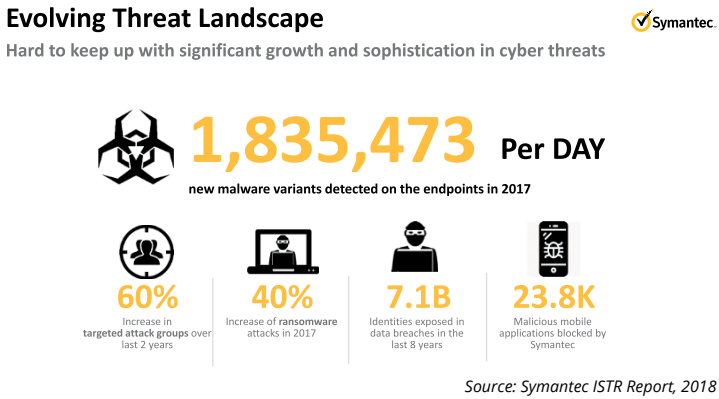


FIGURE 1-1: The evolving threat landscape.

In addition to malware, threat actors are employing new techniques and types of attacks, including:

- **Ransomware attacks:** Ransomware attacks, in which data on an infected machine is encrypted until a cryptocurrency ransom is paid, are trending upward as was evident with the WannaCry and Petya outbreaks (see the case study later in this chapter).
- **Living-off-the-land attacks:** These types of attacks have become increasingly popular over the past several years. Attackers use trusted off-the-shelf and pre-installed system tools to conduct these attacks. Many of these tools are

ubiquitous and are used by system administrators for legitimate work. This makes it harder for defenders to completely block access to these programs and allows the attackers to hide in plain sight. Even when log files are generated, it can be difficult to spot anomalies. System tools and common cloud services are used for data exfiltration to avoid raising any alarms. Even in the event that an attack is discovered, the living-off-the-land approach makes it difficult to attribute the attack to a specific attack group, as all groups use similar techniques and tools. The typical living-off-the-land attack chain consists of the following:

- **Incursion:** This could be achieved by exploiting a remote code execution (RCE) vulnerability to run shell code directly in memory. More commonly, it's an email with a malicious script inside a document or hidden in another host file such as a LNK file. The threat may implement multiple stages with downloader or self-decrypting parts, each of which might follow living-off-the-land techniques. Another method is misusing system tools by simply logging in with a stolen or guessed password.
- **Persistence:** After the endpoint is compromised, stage two may or may not be fileless with regard to the persistence method. The threat may also not be persistent at all, depending on the attacker's objective.
- **Payload:** The payload of the threat often makes use of dual-use tools.

» **Fileless attacks:** There are four main categories of fileless attacks, as follows:

- *Memory only threats*, such as SQL Slammer
- *Fileless persistence*, such as VBS load points in the registry
- *Dual-use tools*, such as psExec.exe
- *Non-portable-executable (non-PE) file attacks*, such as Office documents with macros or scripts

REMEMBER

Fileless attacks are sometimes referred to as *non-malware* or *malware-free* attacks — for example, when only dual-use tools are used, and no malware binary is dropped. Of course, this isn't fileless because a file is involved — namely, one or more system tools. The point is that such attacks don't drop a custom-built malware binary, but they may drop grayware tools or scripts. You could also call these attacks asymptomatic, because they don't exhibit

the usual symptoms users would expect from an infection, such as a malicious file on disk.

There are also slight variations on these tactics, such as using BITSAdmin in macros to download a malicious payload or hiding a PowerShell script that is triggered through an SCT file referenced in a registry run key. In some cases, stolen data is then exfiltrated through legitimate cloud services, hiding the event in normal traffic patterns. Figure 1-2 describes a typical living-off-the-land attack chain.

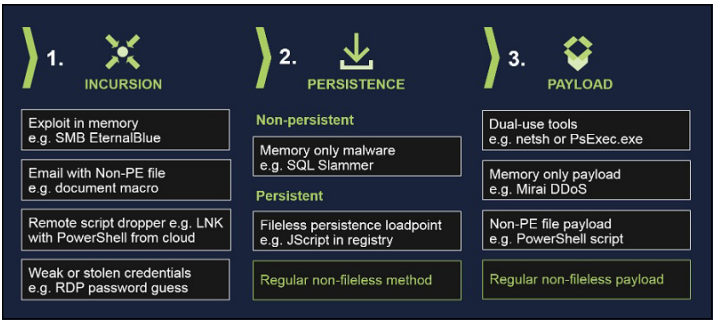


FIGURE 1-2: A typical living-off-the-land attack chain.

Further compounding these challenges, a growing shortage of qualified security professionals are available in the workforce, and they must master a dizzying array of security vendor point solutions. These challenges have created a perfect storm with too few trained IT security personnel attempting to protect increasingly complex operational environments against constantly evolving and increasingly sophisticated threats using disjointed security point products.

Understanding the Attack Cycle

Whether engaging a specific organization or network in a targeted attack or pursuing a random target of opportunity, attackers perform a series of steps to achieve their objectives — known as the *attack cycle* (see Figure 1-3):

- **Reconnaissance:** The attacker explores the attack surface, looking to discover the systems, services, applications, people, vendors, and so on, that make up your environment.
- **Delivery:** The attacker crafts and then delivers an attack. Often the delivery is achieved through email phishing, email attachments, malicious links, a watering hole, USB, or other removable drive.
- **Exploitation:** The attack is initiated, and the network is breached.
- **Execution:** The attacker will perform various actions in the network including:
  - **Establishing persistence:** This ensures the attacker will be able to remain in the network, even if a component of the attack is identified (for example, the attackers will try to ensure their reverse shell is maintained across system reboots). This is frequently achieved by application shimming or embedding themselves in startup items, registries, Windows authentication packages, and so on.
  - **Escalating privileges:** Privilege may need to be escalated to get access to critical assets. Some techniques attackers use include access token manipulation, AppInit dynamic link libraries (DLLs), application shimming, DLL injection, launch Daemon, and so on.
  - **Setup command and control:** Given that every environment is different, the attacker needs a general-purpose remote access Trojan (RAT) or reverse shell to explore the environment and plan his next course of action. Command and control traffic is frequently encrypted and tunneled inside HTTP or IRC to avoid detection by the firewall.
- **Lateral movement:** The attacker traverses the internal network, looking for critical assets. He may potentially use the credentials he has obtained (via privilege escalation).
- **Exfiltration:** After critical data is obtained, it's frequently encrypted and transferred out of the network. Encryption used by an attacker often follows the encryption preferences and tools used in the enterprise. Exfiltration will frequently upload data to cloud services used by the enterprise, such as Box, Dropbox, Google Drive, and so on, to avoid suspicion and detection.

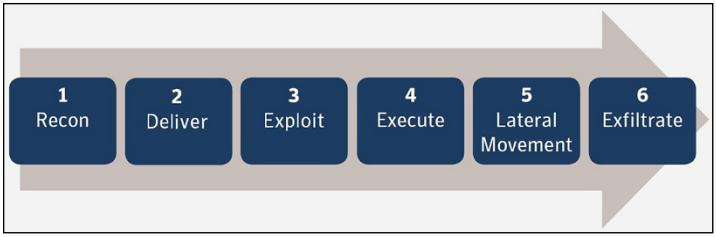


FIGURE 1-3: The attack cycle.

CASE STUDY: JUNE 27 PETYA OUTBREAK

The Ransom.Petya outbreak, which hit organizations in the Ukraine and many other countries on June 27, 2017, is a good example of an attack using living-off-the-land tactics.

The ransomware exhibited some wiper characteristics and immediately gained the attention of both security experts and the media because it was, among other propagation methods, exploiting the SMB EternalBlue vulnerability just like the headline-grabbing WannaCry (Ransom.WannaCry) did one month earlier. The threat made use of a clever supply chain attack as its initial infection vector by compromising the update process of a widely used accounting software program.

Petya also makes heavy use of system commands during the infection process. Once executed, Petya drops a recompiled version of LSADump from Mimikatz in a 32-bit and 64-bit variant, which is used to dump credentials from Windows memory. The account credentials are then used to copy the threat to the Admin$ share of any computers the threat finds on the network. After the threat accesses a remote system, it executes itself remotely using a dropped instance of PsExec.exe and the Windows Management Instrumentation (WMI) command line tool wmic.exe:

wmic.exe /node:[IP Address] /user:[USERNAME] /password:[PASSWORD] process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"

In order to hide its tracks on the compromised computer, the threat deletes various system logs by using the wevtutil and fsutil commands:

wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:

Petya then creates a scheduled task so that the computer restarts into the modified MBR and performs the final encryption task:

schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 14:42

This case is a classic example of system tools being used during an attack. Many system administrators are now looking into disabling remote PsExec execution or restricting WMI access in order to defend against the same attack pattern in the future.

Malware using WMI isn't a new occurrence. Last year, Symantec observed an average of 2 percent of analyzed malware samples making use of WMI for nefarious purposes, and the upward trend is clearly continuing.

A Security Framework for Next-Generation Endpoint Security

To address increasingly sophisticated threats that target endpoints, a new security framework for endpoint security that goes beyond antivirus protection is needed. Comprehensive next-generation endpoint security must include, in a single agent, the following capabilities and technologies:

- **Prevention** (refer to Chapter 2): Layered endpoint security goes beyond signature blocking to fuse signature-less technologies such as advanced machine learning (AML), behavioral analysis, memory exploit mitigation, and OS emulation, with traditional technologies such as intrusion prevention, reputation analysis, and application and device control.

- **Application isolation and control** (check out Chapter 3): Harden the endpoint against cyberattacks with complete visibility into the application attack surface, by isolating suspicious applications and protecting trusted applications from vulnerability exploits.
- **Deception** (head to Chapter 4): Turn the tables on attackers by deploying baits and decoys at scale to gain insights into attackers' intent and discover the tools and techniques they use.
- **Detection and response** (see Chapter 5): Perform incident investigations and remediation leveraging a single agent for protection and endpoint detection, and the other layered capabilities mentioned in this chapter. Ensure roaming users, macOS, and Linux devices can be supported without the overhead of an additional persistent agent. Ensure access to global telemetry to proactively identify advanced and targeted attacks. Look for agents with built-in remediation that quickly delete malicious objects and all associated artifacts.
- **Mobile threat defense** (refer to Chapter 6): Use a layered mobile threat defense approach to proactively identify and protect devices from malicious apps. Look for capabilities that detect novel and advanced threats including static and dynamic analysis, machine learning, and detection of specific indicators or compromise.
- **Endpoint vulnerability and patch management** (head to Chapter 7): When looking at endpoint security solutions, consider providers that can also address endpoint vulnerability and patch management. Automating the detection and remediation of security vulnerabilities is critical.

IN THIS CHAPTER

- Utilizing advanced machine learning
- Preventing zero-day exploits in your network
- Blocking malicious file and application behavior
- Looking at firewalls and intrusion prevention
- Using threat intelligence to determine file reputation
- Exposing unknown malware in a virtual sandbox
- Maintaining control of applications and devices
- Taking endpoint protection to the cloud

Chapter 2
Next-Generation Endpoint Protection Technologies

Endpoint protection has come a long way since the days of signature-based antivirus software. This chapter explains next-generation endpoint protection technologies necessary to protect all your organization's endpoints against the sophisticated cyber threats of today and the future.

All the next-generation security technologies that I discuss in this chapter are used to protect the endpoint against modern, sophisticated threats. However, remember that these technologies all complement traditional antivirus (AV) engines in a complete endpoint protection solution.

Much like everyday household soap kills 99 percent of all bacteria, traditional AV is still effective at preventing 99 percent of all malware infections. Next-generation security technologies protect the endpoint against the more sophisticated and potentially more dangerous one percent: zero-day threats and other advanced malware and exploits.

Understanding Machine Learning

Advanced machine learning (ML) is most useful for detecting unknown threats or evolving threat families (refer to Figure 2-1). It uses mathematical techniques across huge datasets to build models for interpreting actions and events for decision-making. As a result, if a variant of known malware surfaces, advanced ML is generally smart enough to detect it for zero-day protection. In the attack cycle (refer to Chapter 1 for more information about the attack cycle), it works during the early part of delivery, to prevent threats from infecting a target endpoint.

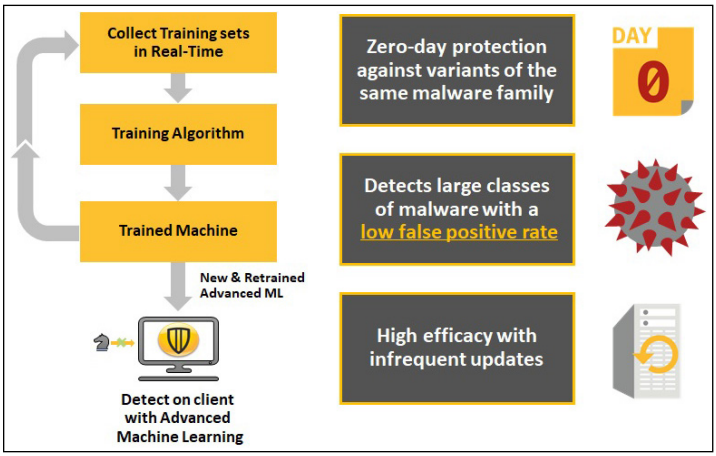


FIGURE 2-1: Advanced machine learning blocks unknown threats and mutating malware.

REMEMBER

The quality of the dataset that trains advanced ML determines the effectiveness of the technology. The power and scale of a global, real-time, cloud-based threat intelligence network enhances this effectiveness and helps enable advanced ML to detect large classes of malware with a low false positive rate.

Preventing Exploits

Many targeted attacks increasingly use zero-day exploits to take advantage of known or recently discovered vulnerabilities in popular software like Internet Explorer, Adobe Flash, or Microsoft Office (see Figure 2-2).

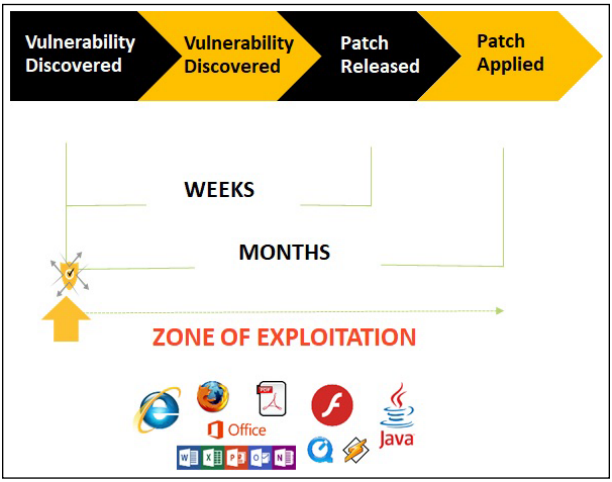


FIGURE 2-2: Zero-day attacks often exploit unpatched vulnerabilities for weeks or months until patched.

TIP

Symantec Endpoint Protection 14 (SEP 14) introduces Memory Exploit Mitigation, a key capability that can significantly reduce the time to protect in dealing with zero-day exploits. Memory Exploit Mitigation is signature-less and hardens the operating system to be able to stop an attack regardless of the flaw, bug, or vulnerability in the software. This protection is available on day zero, instead of waiting for a patch from the vendor to be released and applied, which can leave organizations vulnerable for several weeks or months.

Monitoring Behavior

Behavioral monitoring compares the actions of files or network packets to a list of accepted or suspicious actions. It uses artificial intelligence (AI), custom behavioral signatures, and lockdown policies (see Figure 2-3) to monitor normal file and script behavior

as it executes in real-time, identifying and blocking anomalous — and potentially malicious — file behavior. This protection provides a line of defense against threats such as system changes and suspicious behavior of unknown files as well as trusted ones. By identifying deviations from the norm, it uses intelligence to decide whether an anomaly poses a threat or can be ignored.

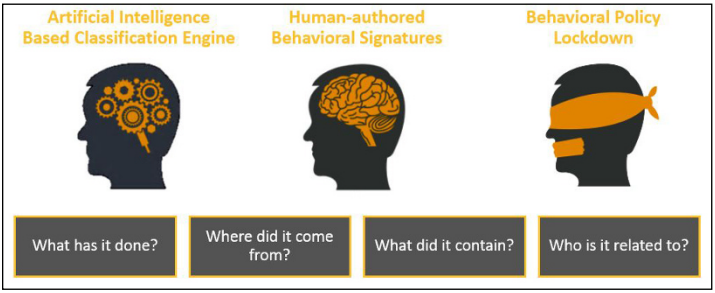


FIGURE 2-3: Behavioral monitoring stops zero-day and unknown threats.

Examining Intrusion Prevention and Firewalls

Host-based intrusion prevention systems (HIPS) and personal firewalls are an important component of endpoint security. HIPS detects potentially malicious network traffic that matches preconfigured signatures and blocks or drops the traffic based on custom rules.

A personal firewall provides packet filtering and stateful inspection of traffic and allows or blocks connections based on preconfigured firewall rules. Almost all enterprise networks use firewalls and intrusion prevention systems (IPS) on the network, but HIPS and personal firewalls extend the security of these technologies to the endpoint — both on and off the corporate network. According to Symantec, IPS was found to be particularly useful in preventing the spread of the WannaCry ransomware outbreak.

Considering File Reputation

File reputation services utilize real-time, cloud-based threat intelligence to quickly inspect, analyze, and classify files based

on numerous criteria, including age, download frequency, source, and other security metrics such as associations with malware (refer to Figure 2-4). Unique signatures are created for every file that is scanned (without exposing the data in the files), and big data analytics are then used to determine whether a file is good, bad, or unknown.

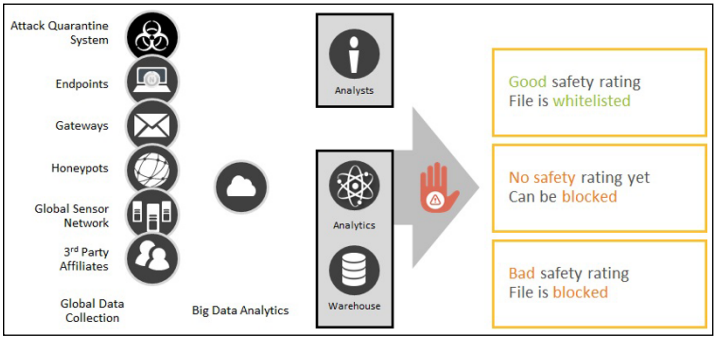


FIGURE 2-4: Age, frequency, and location are used to expose unknown threats with file reputation analysis.

Comprehending Emulation

Attackers use sophisticated tactics to hide malware, hoping the endpoint protection solution won't detect it until it's too late. Emulation technology foils malware's attempts to evade detection using polymorphic custom packers by unpacking files in a virtual environment that emulates OS API. Polymorphic malware are thus tricked into thinking that they're running on the actual OS. They start to unpack, revealing the malware family, which can then be identified (check out Figure 2-5).

A *polymorphic* virus is a virus that changes its appearance in host programs. For instance, it encrypts its body with a different key each time and prepends a decryption routine to itself. The decryption routine (known as the *decryptor*) is mutated randomly across virus instances, so as to be not easily recognizable. A *metamorphic* virus, by comparison, is a virus that also changes its appearance in host programs; however, it does so without necessarily depending on encryption. The difference in appearance comes from changes made by the virus to its own body.

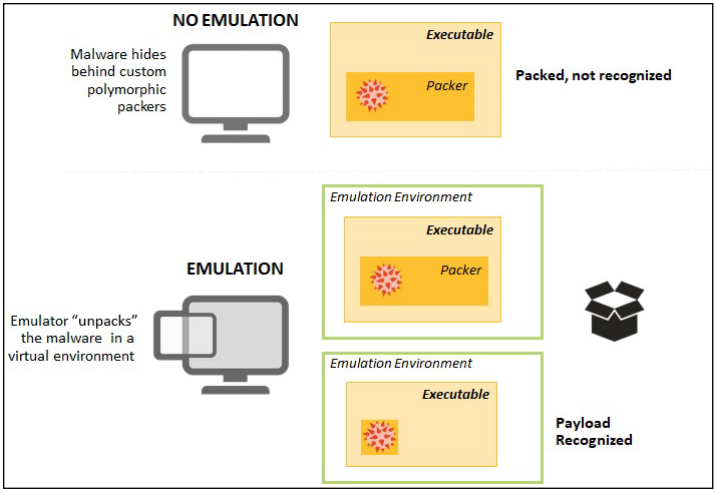


FIGURE 2-5: Emulation technology simulates file execution in a virtual environment to cause threats to reveal themselves.

Eyeing Application and Device Control

Application and device control (refer to Chapters 3 and 6 for more information) enables organizations to explicitly allow or block specific applications from running on endpoints, including mobile devices.

Reducing Costs and Complexity with a Single Agent Architecture

Deploying, maintaining, and managing multiple agents is cumbersome and expensive. IT organizations sometimes end up deploying four or more endpoint agents to implement the endpoint security technologies that I discuss earlier in this chapter. Look for an endpoint security solution that integrates all these technologies with a single agent architecture. At the same time, the single agent should have high performance and shouldn't hamper user productivity.

Extending Endpoint Protection to Cloud Workloads

Enterprises are rapidly adopting public cloud services such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform to increase business agility, relieve pressure on understaffed IT departments, and reduce costs associated with running an on-premises data center.

Many public cloud providers offer security certifications for their infrastructure up to the hypervisor level (security *of* the cloud); however, the *shared responsibility model* of security (refer to Figure 2-6) means that customers are still responsible for protecting any workloads running on that infrastructure (security *in* the cloud) against vulnerability exploits and malware.

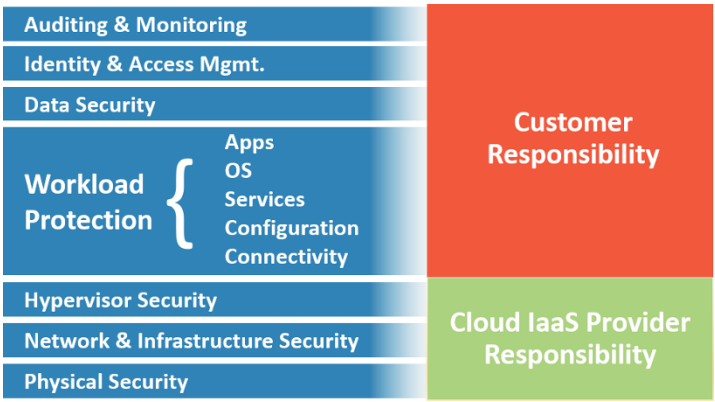


FIGURE 2-6: Infrastructure as a Service (IaaS) provider shared responsibility model of security.

While some enterprises choose to go all in with the public cloud, most are pursuing a hybrid cloud approach — using a combination of public cloud, private cloud, and on-premises resources and infrastructure to deliver applications and services to employees and customers.

Complications arise when businesses begin migrating workloads to the cloud and quickly discover that a *lift-and-shift* approach to security often fails, especially in the public cloud. Modern

operational practices must encompass DevOps continuous delivery workflows that are central to agile application delivery, workload scalability, and efficient public cloud operations.

TECHNICAL STUFF

The concept of *DevOps* combines modern cloud-native tools, philosophies, and practices toward a common goal of increasing the speed of applications and services delivery, along with their elasticity in the cloud. This provides a competitive advantage when serving their customers and employees.

To secure cloud deployments with the same efficacy and reliability as on-premises workloads, enterprises are often forced to consider the purchase of additional security solutions and hire additional operations personnel and security analysts to formulate and apply policies, respond to alerts, and remediate threats. What enterprises need is a security solution that allows them to discover, monitor, and protect all their workloads across their entire hybrid cloud — ideally from a single, efficient console.

TIP

Symantec Cloud Workload Protection (CWP) allows organizations to secure their critical workloads wherever they are — public clouds, private clouds, and physical on-premises data centers — all from a single cloud-based console. CWP automates workload security, providing discovery, visibility, and protection against malware and zero-day threats. CWP uses SEP 14 anti-malware engines and advance machine learning technologies to protect hybrid cloud workloads.

IN THIS CHAPTER

- Preventing fileless threats with application isolation
- Applying zero-trust model to applications
- Combining blacklisting, whitelisting, and application isolation

Chapter 3
Application Isolation and Control

Increasing layers of defense in enterprise networks have forced attackers to change their approach, using fileless attack techniques that are more difficult to detect by traditional means.

This chapter explores how application isolation can help you achieve a more holistic, layered approach to your endpoint and network security.

Recognizing the Need for Application Isolation

Attackers are increasingly taking advantage of applications that have already been installed on endpoints to achieve their attack objectives. They exploit vulnerabilities in common applications and use scripted content in document files to hide their activity in trusted applications. They're running attacks directly in memory and persisting in registry keys, using common scripting

languages, such as PowerShell, WMI, JavaScript, WScript, and so on, to avoid raising any suspicions. And because they aren't uploading malicious executables or files to the endpoint, traditional file-based detection methods are ineffective in detecting and preventing these types of attacks.

To defend against these living-off-the-land tactics, application isolation complements anti-malware detection by proactively blocking malicious behavior using a zero-trust model for well-known and possibly suspicious applications.

Understanding Why Trusted Applications Are the Riskiest

Many applications are critical for your day-to-day business operations and employee productivity. These include browsers, email clients, productivity applications (such as Microsoft Office), platform tools (such as Java), and common development tools (such as Visual Studio), among others. Most of these applications contain vulnerabilities that an attacker can exploit to take control over that application and get a foothold into your endpoint and ultimately your network.

Some documents, such as Microsoft Word, Excel, and Adobe PDF files, also allow scripted content, which means an attacker can run malicious code from seemingly harmless documents. Many of these applications use elevated privileges, particularly those that run in the context of privileged admin users. As a result, when attackers take control over these applications, they have unrestricted access to the endpoint. Attackers can use a compromised application to download a malware payload and then execute it within the context of that trusted application.

Mitigating some of these issues is possible by patching applications and upgrading them to the latest versions. However, rolling out patches or updates can be challenging in large environments. Plus, given how frequently zero-day vulnerabilities are discovered, even the most disciplined software update process

has trouble keeping up. Therefore it's critical to adopt proactive defensive measures that prevent attackers from exploiting or tampering with vulnerable applications to breach the endpoint.

Preventing Attacks from All Angles

The threat continuum paradigm (see Figure 3-1) is a useful way to analyze the right protection strategy for different threat vectors.

FIGURE 3-1: The threat continuum.

You can broadly classify the files and applications on your endpoints as follows:

- **Threats**
- **Potential threats**
- **Unknown**
- **Potentially good**
- **Known good**

REMEMBER

An effective endpoint security strategy will deliver protection along the entire threat continuum: *Threats* should be blocked and eliminated immediately, *potential threats* and *unknown* applications should be monitored to identify and then stop the behavior that could harm the operating system or other applications, and *potentially good* and *known good* applications should be protected from exploits and monitored to prevent fileless attacks.

Executing an effective endpoint strategy requires a solution that combines multiple controls across the threat continuum (see Figure 3-2), including:

- **Blacklisting** follows a default "allow" model, permitting everything to execute freely, unless it has been characterized as bad. This model enumerates the applications, processes, scripts, and so on, that are known to be malicious and eliminates them as soon as they're identified with high fidelity. If they're not characterized as bad, they're assumed to be good and are permitted. This has been the preferred security model for endpoints, such as end-user desktops and laptops that frequently change because it's easy to deploy with simple and effective policies. Blacklisting is effective at eliminating known threats, but it's not optimized to catch well-known applications that have been compromised and are performing malicious actions.
- **Whitelisting** follows a default "deny" model, allowing only the applications that are whitelisted, in a policy, to run. Nothing else is trusted or allowed, which makes it effective at reducing the overall attack surface. This model typically works well for environments that don't change frequently, but if it's well managed, it can also be used for potential threats that change frequently. Whitelisting also catches and prevents zero-day threats if they fall outside of what's allowed; however, it won't stop threat activity being performed by a whitelisted application.
- **Application isolation** follows a zero-trust model; it builds on whitelist security to allow not just approved applications but also restricts the behavior of approved applications. For example, an application isolation policy could define the acceptable network connections, file activity, registry activity, and so on of an application, so it's restricted to known good behavior. Non-whitelisted applications could be allowed to run but with very severe restrictions. This model is highly effective for reducing the overall attack surface. It can also mitigate zero-day threats by restricting an allowed application from doing something malicious, such as making changes to protected system settings or applications.

FIGURE 3-2: Mapping security controls across the threat continuum.

JAILS AND CASTLES IN ACTION

Symantec Endpoint Protection (SEP) combines blacklist, whitelist, and application isolation security models to provide comprehensive multi-layered protection against evolving threats targeting your endpoints.

SEP allows you to tune threat detection engines collectively, so you can effectively block against threats and detect potential threats in the continuum. For a file that is identified as a threat, intensive protection will delete or quarantine the file to stop it from doing any damage.

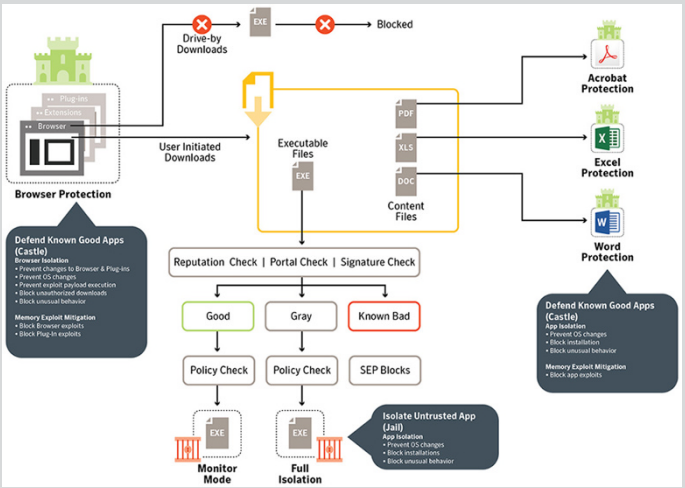
For an application that is classified as a potential threat or unknown, intensive protection will flag the file as suspicious and hand it off to application isolation, a key feature of the add-on product, Symantec Endpoint Protection Hardening.

Application isolation can run these suspicious apps in what's called *jail mode* (see the following figure), which allows an untrusted application to execute within a jail-like environment. It allows the application to run with limited privileges to protect the operating system and other good applications from any harm or tampering via such untrusted application. It can contain items opened from an untrusted source (for example, email or web) to mitigate risk they may pose and restrict these applications to only good behavior (expected and permitted application operations). The same treatment can be applied to potentially good applications, which are often applications that may not exhibit suspicious behavior but don't have a credible reputation yet to trust them entirely. Application isolation can run these applications in

(continued)

(continued)

what's considered an ankle-bracelet type of jail where their behavior is largely unrestricted but some privileged operations, like modifying the operating system or installing new applications, will be prevented.



Application isolation can also protect known good (whitelisted) applications, running them in castle mode to fortify these trusted applications and protect them from exploitation and tampering through a layered security approach. First, SEP's Memory Exploit Mitigation engine protects an application's process from a wide spectrum of exploit techniques against known and unknown vulnerabilities. Next, in the extreme event that an attacker gains control of an application's processes, the attacker won't be able to use its process privileges to install new software, change the system settings, or modify other application processes or resources, as such processes would be restricted from executing. All the operations that the application doesn't typically need to perform are blocked by the isolation policy. ***Note:*** The end user doesn't perceive any change when using the application, unless the application engages in malicious behavior. This requirement is critical for effective application isolation and ensures security doesn't come at the cost of productivity.

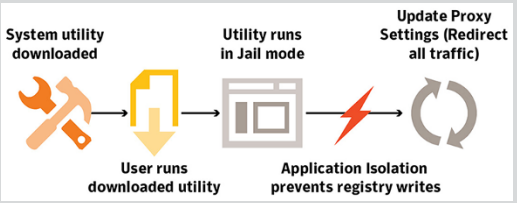
Case study 1: Using application isolation's jail mode to prevent a weaponized system utility

Problem: Jen, an end user, is looking for a utility to speed up her laptop's performance. She visits a popular downloader website to check

out a few utilities and downloads the SpeedUp.exe app. Jen is obviously unaware that SpeedUp.exe is weaponized and will modify the Window's proxy settings to redirect Web traffic to an attacker's server.

Solution: Application isolation neutralizes this threat and prevents the attacker from gaining a foothold on the endpoint.

How it works: As soon as SpeedUp.exe is downloaded, SEP performs an exhaustive analysis of the file. The intensive protection engine determines that SpeedUp.exe is suspicious (also known as a potential threat) but not confirmed to be malware. As a result, when the user launches the SpeedUp.exe application, application isolation automatically runs SpeedUp.exe in jail mode. While running in the jail, SpeedUp.exe can render its user interface and examine system performance, as long as it's not attempting to read or modify any protected operating system resources. However, when SpeedUp.exe attempts to modify the Windows proxy settings, by accessing the system registry, the jail will block the operation instantly and generate a security event. Jen will get a notification indicating that SpeedUp.exe was blocked from modifying the operating system, but she can continue to run the utility for its system performance functions. ***Note:*** SEP could be configured to prevent the download of any executable files from the Internet. However, in this example, SEP was configured to allow all files to be downloaded to demonstrate how jailing addresses the threat (see the following figure).



Benefits: Application isolation dynamically jails suspicious applications and prevents any malicious changes to the endpoint, so Jen can continue to work, without putting her endpoint or the network it connects to at risk.

Case Study 2: Using application isolation's castle mode to prevent a fileless attack using MS Excel

Problem: Sam receives a spear phishing email with a project quote from an attacker pretending to be a vendor with whom he regularly works. The email contains an attachment, QuoteForReview.xlsx, which

(continued)

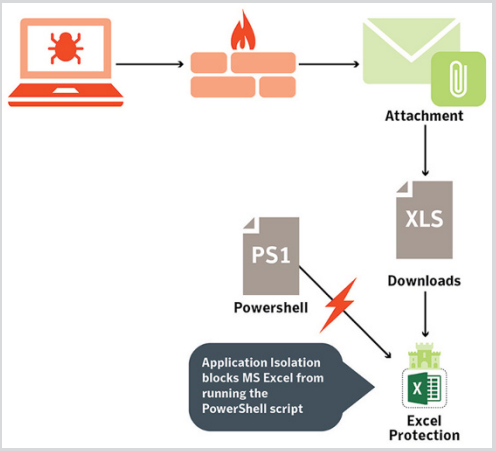
(continued)

is a weaponized document. When the document is opened in MS Excel, the spreadsheet looks deceptively similar to the quotes he normally receives. Sam gets tricked into disabling MS Excel's protected-view mode with an instruction that macros should be enabled for the quote's numbers to show up accurately. The sophisticated macro then runs a Visual Basic script that constructs a PowerShell script using snippets of code from the XLS file and runs the script using Windows PowerShell (a commonly used system tool on Windows). This initiates the attack sequence — the PowerShell script communicates with the attacker's hosted Command & Control (C2) server to download additional tools that are used to extract credentials, conduct network reconnaissance, and move laterally to other endpoints.

Solution: SEP Hardening can prevent a known good application from introducing a threat to the environment.

How it works: With SEP Hardening, Microsoft Excel runs in a castle that protects it from being tampered with and restricts its behavior. When Sam opens the weaponized XLS document, Excel will be able to render the document content. However, when the XLS file attempts to construct a PowerShell script file or run the script using the PowerShell utility, the castle will block the operation because MS Excel is neither allowed to create files of certain types nor launch any executables, particularly scripting tools like PowerShell (refer to the following figure).

Benefits: Application isolation can render the fileless attack useless, protecting Sam's device and eliminating the progression of the attack.



IN THIS CHAPTER

- Looking at honeypots, endpoint deception, and bait
- Recognizing the role of deception in disrupting the attack cycle

Chapter 4
The Art of Deception

Although endpoint and network security solutions protect you from being compromised, deception mitigates the effects of a compromise by detecting it early and helping to identify the attacker's objectives and tactics, which helps organizations coordinate a faster, more effective, and better response. This chapter looks more closely at the art of deception.

Eyeing the Evolution of Deception

Deception isn't a new concept. History has many examples of deception in nature and warfare. Many animals have developed sophisticated camouflage techniques to trick predators into passing them by, and some of the world's best wartime strategists have used deception to create an advantage over their enemies (for example, the Trojan horse). When it comes to cybersecurity, deception can be used to trick attackers into doing something different than what they intend.

Initially, cybersecurity deception started with simple network honeypots. These *honeypots* emulated a subset of a system's functionality, which was enough to fool script kiddies, but not sophisticated attackers. The limited capabilities (for example, a database that had a couple of relational datasets but couldn't do bulk uploads) made the systems easy to spot and avoid. Organizations

could try to improve the deception and increase the probability that an attacker would be fooled with larger deployments of honeypots, sometimes called a *honeynet* or *honeyfarm*, that added functionality and interaction complexity within a completely different, isolated subnet.

The more believable the fake network, the better chance it had to lure attackers into interacting with it to keep them away from the real resources. Unfortunately, it required a lot of time and expertise to deploy, manage, and maintain all the hardware and software needed to create a believable, isolated subnet — with all its fake credentials, databases, web servers, vulnerable systems, and content. These requirements made honeynets impractical or unsustainable for most organizations.

To put deception on individual endpoints, organizations traditionally had to rely on the reachability of the endpoint. This dependence quickly became complicated and unwieldy for endpoints behind firewalls, proxies, network address translation (NAT), or virtual private networks (VPNs). The challenge of reliably deploying and monitoring deception on endpoints within a large, distributed environment has led most vendors to focus on network deception, rather than endpoint deception.

REMEMBER

Symantec currently secures more than 350,000 customers, with 175 million endpoints — all these customers can now work with Symantec to turn on deception and deploy the high-interaction bait that is integrated in the SEP family to dramatically improve attack detection.

TIP

Because you know what your critical assets are and where they're located, you can exploit this knowledge to mislead attackers targeting your organization. You can deploy a wide variety of bait throughout your environment to trick attackers into revealing their attack objectives and techniques. Some examples of bait include the following:

- **Fake files:** You can create fake files to entice an attacker out into the open. Think of how attractive a "ConfidentialMerger" document would be on your CEO's desktop, a "FundraisingCycle" document on your CFO's desktop, or a "Salary" spreadsheet on your human resources server. The options are endless.

- **Fake credentials:** You can create and distribute fake passwords throughout systems to make it easy to identify an attacker; any attempt to use one of the fake passwords is evidence of malicious activity. Advanced, high-interaction deception systems can enable an attacker to log into a controlled system with a fake password and interact to reveal his tactics and true intent.
- **Fake network shares:** You can use fake network shares on desktops to prompt attackers into interacting with resources to reveal themselves. Any engagement with these network shares, such as clicking to open, copying files, and so on, indicates an attack.
- **Cached items:** You can use fake cache entries, such as a domain name system (DNS) cache, remote access tool caches, such as remote desktop protocol (RDP) and virtual network computing (VNC), and so on, to mislead an attacker and identify their potential targets.
- **Fake endpoints:** You can make fake nodes on the network visible to tempt an attacker into trying to access that machine remotely. Because the endpoint is fake, you know that as soon as someone tries to access it, it's an attack.


TIP

Deception can be more art than science; it's a game of evasion and counter-evasion. The key is to ensure the bait blends into your environment, so attackers will interact with it and reveal themselves.

Seeing the Need for Deception

Why do you need deception when you have so many other layers of defense already in place? Because you need to cover all your bases. Attackers are increasingly sneaky. Stealing user credentials is a top method for how they infiltrate networks. In addition, they use tools that are already installed on targeted computers. These *living-off-the-land tactics* often don't load malware and don't create new files on the device's hard disk (they run directly in memory). In addition, today's attack surface continues to grow and change. Deception can complement endpoint and network defenses, adding dynamic security mechanisms that can be customized for every environment.

REMEMBER

To combat increasingly sophisticated attacks, you need a variety of mechanisms in place to help you close the window of opportunity for attackers and shut down some of the attack vectors they are using, such as:

- **Social components**
  - Forty-three percent of the 42,068 security incidents analyzed in Verizon's *2017 Data Breach Investigations Report* (DBIR) involved social engineering attacks.
  - Microsoft estimates that the human attack surface will reach 4 billion by 2020. Enterprises have a revolving number of employees, partners, contractors, vendors, customers, and so on, who all have access to enterprise resources and can exfiltrate corporate data, both intentionally and unwittingly.
  - According to the Ponemon Institute's *2016 Cybersecurity Trend Report*, two-thirds of technology professionals identified phishing, spear phishing, and social engineering as the biggest threats to their organization. After attackers have the credentials needed to get the information they want, no further exploits are needed.
  - According to a 2016 study by Friedrich-Alexander University (FAU), 56 percent of email users and 40 percent of Facebook users will click on a link from an unknown sender.
- **Technology vulnerabilities**
  - Java, Adobe Reader, and/or Adobe Flash is installed on 99 percent of all computers, which means those computers are vulnerable to exploit kits, due to unpatched operating systems and/or software.
  - According to Symantec's *Internet Security Threat Report* (ISTR), more than 75 percent of all legitimate websites contain an unpatched vulnerability.
- **Endpoint weaknesses:** Endpoint protection may inadvertently not be deployed to all endpoints.
- **Misconfigurations:** Protection is often outdated, leaving assets exposed and vulnerable to attack, and capabilities designed to protect the endpoint may be turned off.

Deception adds an offensive layer to your security that increases the chances that an attacker in your network will be discovered.

You can quickly and easily place an infinite amount of bait in your enterprise (such as fake credentials, files, vulnerable endpoints, critical assets, and so on) to deceive attackers into revealing themselves. Deception picks up where other security technologies leave off, providing offensive tactics that can uncover the later stages of an attack.

REMEMBER

Although most security technologies are designed to identify and stop the early stages of an attack, deception is optimized to identify the later stages. Based on the following simplified attack sequence (see Figure 4-1), most security technologies focus on steps 1, 2, 3, and 6, whereas deception technologies target steps 1, 4, 5, and 6 to uncover the attack activity that's already in the network. A recent Ponemon Institute report found that attackers dwell, on average, 191 days in the network before they're detected; deception is designed to go on the offensive to reveal attackers in your network. It misleads attackers, disrupting their workflows and decisions, to quickly identify them and cut down on their dwell time, preventing them from accomplishing their attack objectives.

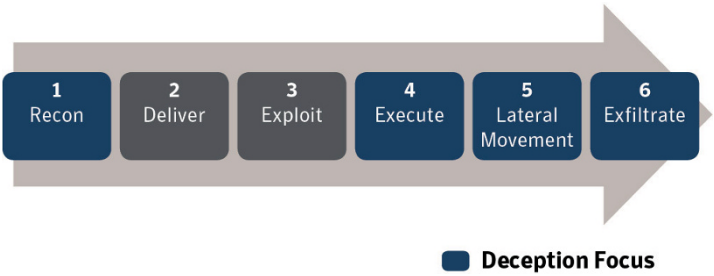


FIGURE 4-1: Deception targets the post-incursion stages of the attack cycle.

MODERN DECEPTION WITH SYMANTEC

Symantec enables you to easily deploy an infinite amount of customizable deceptors (also known as *bait*) on endpoints throughout your environment, so you can identify attackers in your network and prevent them from achieving their objectives. The Symantec deception approach solves the endpoint reachability problem that has plagued vendors in the past.

(continued)

(continued)

Using the Symantec Endpoint Protection agent and management console, the deception tools are already optimized to have minimal or even no tangible performance impact. There is no requirement to relax firewall rules or enable vulnerable endpoint services, and you don't have to procure, manage, or monitor any additional hardware. You simply turn on deception to add bait on the endpoints in your environment. By placing realistic bait on your endpoints, you significantly increase the probability that an attacker will find it. Because it's bait, there's no legitimate reason for someone to try to access the fake remote connections, credentials, files, network shares, and so on, so as soon as an attempt is made, you know you have an attacker. The bait is regularly tuned, monitored, and refined by Symantec Cyber Security Services.

Symantec's deception is supported by Symantec Cyber Security Services (CSS), for continuous threat monitoring and incident response expertise, and Symantec Consulting Services, to customize your deception deployment to fit the tactics, techniques, and procedures (TTPs) that will work best in your environment. Together, they support

- Deploying and customizing the initial bait embedded throughout your environment.
- Providing ongoing, 24x7, automatic monitoring of any alerts triggered by SEP's deception and other devices across your on-premises and cloud environments — a CSS Security Operations Center (SOC) analyst will contact you when an incident has been confirmed as critical, and provide you with the attack details, assets impacted, and any recommended courses of action.
- Supplying incident response, which often requires sealing the entire suspected ingress path, forensics, and endpoint detection and response (EDR) analysis.
- Closing the feedback loop to continue to refine the bait and optimize the deployment.

SEP's deception capabilities pick up where most security technologies leave off, adding a complementary layer of protection that enables you to go on the offensive and lure attackers out of hiding.

IN THIS CHAPTER

- Identifying potential attacks in your environment
- Using a two-phased approach to threat intelligence
- Stopping threats with real-time information
- Automating and orchestrating an effective response
- Providing visibility to your security operations center (SOC)

Chapter 5
Detection and Response

The old adage "an ounce of prevention is worth a pound of cure" is as true in cybersecurity as it is in personal health. But in much the same way that people still get sick despite eating healthy, exercising regularly, and practicing good hygiene, endpoints still get infected and networks breached, despite best efforts to protect them.

When an attack succeeds, early detection and fast, effective response is crucial to minimize damage and fully recover — just as early detection and effective treatment is often crucial to recovery in the case of a major illness. This chapter explores the role of detection and response in endpoint security.

Detecting and Prioritizing Suspicious Activity

Despite the changing *living-off-the-land tactics* increasingly used by attackers (refer to Chapter 1 for more information about these tactics), many organizations continue to rely on signature-based

anti-malware and known indicators of compromise (IOCs) to identify attacks. Unfortunately, these detection methods can't detect new, unknown, or zero-day threats and are unable to identify stolen user accounts or lateral movement. What's needed is a way to expose the unknown and undefined — the anomalous signs of an endpoint compromise that aren't tied to malware.

Uncovering these signs has typically fallen on the shoulders of the incident response (IR) team members. They're the ones responsible for following up on an alert or a tip from law enforcement, a customer, or a partner that something might be wrong. These cyberanalysts are responsible for figuring out what is happening and, if it's an attack, addressing the impact.

However, IR can typically take days, weeks, or even months as the team collects and sifts through mountains of data investigating an incident that may end up being a false alarm and a waste of time. For every digital artifact the team finds, more questions and manual investigations may need to be performed.

To completely remediate an attack, the entire attack sequence needs to be revealed and all potentially impacted systems identified and prioritized. Unfortunately, most of the time, the root cause and full attack timeline can't be found, leaving the organization vulnerable to reinfection. It's like a whack-a-mole strategy: When one thing gets shut down, something else pops up.

What's needed is a way to see the full picture — to see how everything fits together, so that attack activity stands out and is fully understood.

Leveraging Threat Analytics Using Cloud-Based Threat Intelligence

Rather than relying on a single IOC or source of threat intelligence, cloud-based threat intelligence looks at the whole picture from every angle. It uses automated threat analytics to efficiently examine your endpoint environment as a whole. It dynamically baselines what is normal to make it easy to quickly identify software, configuration, and behavioral anomalies that aren't normal or expected. This approach is effective at identifying unknown, zero-day threats because there are no preconceptions about what

to look for and no need to have prior knowledge of trouble spots. It lets the actual activity (data) do the talking.

To effectively leverage threat analytics using cloud-based threat intelligence, organizations should adopt these two phases.

Phase one: Environment assessment

Phase one is a top-down examination of the environment, which ultimately narrows down the scope of what needs to be looked at more carefully to a manageable set of endpoints. During this phase, metadata from endpoints is collected and analyzed to understand usage patterns, statistical outliers, user behavior anomalies, and vulnerabilities. This phase can identify the following:

- **Threat events:** Correlated across multiple control points, including endpoint, network, and email. Correlated events can prioritize which incidents security analysts need to investigate.
- **Adversary intelligence:** Helps identify if an organization is under targeted attack. This type of high-value feed highlights which indicators of targeted attack require the most urgent level of response.
- **Continuous recording:** Endpoint activity, including process starts and stops, module loads and unloads, and user session logon and logoff.
- **User account abuse:** User profiles and logon events that indicate potential account abuse, accounts that have cracked passwords, or pass-the-hash lateral movement behavior.
- **Persistence mechanisms:** Registry, load order, tasks, startup programs, and other methods that enable software to persist on an endpoint, even after a reboot, are examined to identify any threats and establish timestamp information as a starting point for future timeline analysis.
- **Memory and dynamic link library (DLL) injection:** Loaded memory is examined to determine if programs have been injected into other programs, which is a common technique used by remote access tools and malware.
- **Command line and interactive behavior:** Prefetch, superfetch, lnk, shellbags, most recently used (MRU), registry entries, and file timestamps are used to locate suspicious program and user behavior.

- **Perimeter event logs:** Perimeter security device event logs are examined to help identify potential attacks, vulnerable machines, and previous infections.
- **Domain name system (DNS) logs:** DNS logs are examined to help identify at-risk machines.

Phase two: Deep analysis and threat behavior verification

Phase two takes a closer look at high-risk endpoints, identified in phase one, to validate threats and reveal the full extent of the incident's activity. Instead of the traditional, broad analysis of hard drive and memory images, relevant data and digital artifacts needed to validate an attack are collected. These may include master file table records, event logs, registry hives, change journals, memory snapshots, and other sources. The information is automatically normalized, organized, and reconstructed into an attack timeline, so analysts can see the root cause and all the impacted components of the attack. In addition, this phase includes the following:

- **Active threat hunting:** Looking for specific IoCs and searching for specific artifacts across all endpoints, and the ability to search for and acquire files for further endpoint analysis.
- **Sandboxing and payload detonation:** Execution of files in an isolated sandbox environment, and on physical hardware if they are virtual machine-aware.
- **Additional indicators:** Additional queries can be created to quickly and efficiently search the environment as a whole for other known indicators of threats.
- **Network connections and IP reputation:** Network connections from suspicious processes are compared against an IP reputation database.
- **Software usage history:** Event logs are examined to determine if any client-side software has crashed. Crash logs may also be used. This provides a starting point for timeline analysis and helps determine whether a machine has been exploited.

- **Memory artifacts:** Memory snapshots of suspicious processes and modules are examined, including strings and possibly code.

Isolating and Investigating Threats

With the endpoint visibility and analysis that cloud-based threat intelligence provides, IR analysts have what they need to quickly spot, understand, isolate, and shut down threats in your environment. Rather than relying on costly, time-consuming manual IR processes to try to piece together what's happening in your environment, you have the root cause and timeline at your fingertips.

REMEMBER

By arming your IR team with the right digital evidence and contextual information, you can:

- **Understand threats in your environment.** Identify all affected endpoints, expose lateral movement and user account propagation, and document the technical details of a breach.
- **Respond faster.** Plan and execute an effective response that remediates all impacted components of the attack to ensure nothing persists.
- **Reduce risk.** Make configuration changes, based on vulnerabilities identified in the environment, to improve your overall security stance, and establish processes for continuous monitoring of the network to help you get ahead of threats.

Remediation

Given the speed and scale of modern cyberattacks, the size and complexity of the enterprise computing environment, and the limited security resources available in most organizations, remediation must increasingly be automated and orchestrated when possible.

Remediation capabilities should support the following actions:

- Quarantine an endpoint while an investigation is in progress to fortify against the spread of a threat.
- Blacklist files, URLs, and IP addresses that are known to be malicious.
- Delete files and all their associated artifacts that impacted the endpoint.

Investigators should be able to execute these actions across all impacted endpoints with one administrative task or automate remediation actions within playbooks.

Looking at Integration with SOC

Integrating detection and response tools with your security operations center (SOC) provides security analysts with a quick dashboard view of potential threats in the environment. Organizations want to leverage their SOC investments by:

- Extending ticketing and service automation workflow into existing processes with platforms like ServiceNow and Phantom
- Visualizing endpoint detection and response (EDR) data alongside other security information using pre-built apps for security information and event management (SIEM) solutions like Splunk, ArcSight, and IBM QRadar
- Implementing smooth integrations with other security products using open application programming interfaces (APIs) that support data acquisition and security analyst actions like endpoint isolation, file blacklist, and delete

IN THIS CHAPTER

- Recognizing mobile security challenges and limitations of traditional security
- Addressing mobile threat defense with next-generation solutions

Chapter 6
Mobile Threat Defense

This chapter looks at the mobile attack surface, the shortcomings of traditional mobile security approaches, and the requirements for a robust next-generation mobile threat defense solution that leverages pervasive analytics to predictively identify threats and, if necessary, proactively stop attacks without disrupting users' mobile productivity.

Mobile Devices: An Exposed Attack Surface

As the connected world becomes even more connected by the day, cyber threats have been retooled to attack ubiquitous mobile endpoints. Although attack vectors still include physical (device) threats, the focus has shifted more toward exploiting vulnerabilities in networks, mobile apps, mobile operating systems, and mobile user behavior. It follows that next-generation mobile security must be able to holistically protect sensitive data leveraging a multilayered security model that can stay ahead of attackers in all the mobile attack vectors.

Many IT departments have mirrored their mindsets for protecting desktop/laptop computing over to protecting mobile endpoints. The problem that arises is an "apples and oranges" dilemma. Mobile security requires different approaches due to unique characteristics, including:

- **Different resources:** Mobile devices have limited battery life and processing power, so even though desktops and laptops can simultaneously run multiple applications in the background, mobile security solutions must be unified and extremely efficient.
- **Different operating systems:** Due to the design of modern mobile operating systems (that is, *app sandboxing*), apps are limited from monitoring and controlling other apps.
- **Different user behavior:** The bring-your-own-device (BYOD) trend is here to stay. By converging work and personal life into a single mobile device, employees can work more collaboratively and efficiently. However, it can be a challenge to enforce security policies on an employee-owned device. Because these users administer their own devices, they decide what networks to connect to, what apps to install, and when to update to the latest security patches, all of which may add risk to the organization.

Most current mobile security programs are designed to respond reactively to attacks rather than to proactively find intrusions and stop them in their tracks before damage is done. With the evolution of threats on multiple attack vectors, purely reactive security does too little, too late: Reactive measures often only apply policies after sensitive data has already been lost. Targeted, well-planned attacks may not need much of a window to acquire critical data, like enterprise credentials, which may lead to even greater breaches.

Traditionally, enterprise mobile security has been based on mobile device management (MDM) and containerization as part of reactive strategies, or proactive but intrusive approaches, like persistent VPN tunneling to remediate threats and attacks:

- **MDM:** Although MDM can ensure that basic security and compliance policies are set on mobile devices, it lacks active

threat detection. It can only passively enforce mobile security best practices without the ability to proactively seek, identify, and defend against device, app, and network-level attacks, threats, and intrusions.

- **Containerization:** *Containerization* doesn't provide complete device security. It's a passive approach that offers no proactive threat defense to identify attacks and vulnerabilities outside of containers, and when a device is compromised, the containers provide no protection at all. Containerization also puts limitations on user enablement and mobile productivity. Thus, it isn't user-friendly and makes work on the device more cumbersome, often causing mobile users to adopt what's referred to as *shadow IT practices* to work around containerization. Finally, many of the most important security features of containerization, such as password-protected access to enterprise apps, are now offered natively by the latest versions of mobile operating systems.

REMEMBER

Shadow IT is a cultural trend, largely driven by BYOD and the consumerization of IT, in which end users largely bypass corporate IT resources to procure, install, and support IT devices, applications, and services on their own.

- **VPN tunneling:** Although this approach may work well for desktops and laptops, it fails mobile users on multiple levels:
  - **Disrupted privacy and enablement:** Running VPN tunneling 24/7 results in an unacceptable drain on device battery life. Most BYOD users also won't adopt tunneling because they don't wish to have their personal activity tunneled and monitored by their employer or a third-party solution.
  - **Lack of seamless continuity:** VPN tunneling can cause significant latency problems affecting productivity and workflow. Although adding proxy servers can mitigate latency, doing so comes with a hefty price tag. Regardless of the numbers of VPN servers available to route traffic, any connectivity issue on a proxy server can kill all data (personal and business) communications on a device.
  - **Incomplete security:** Communications within an internal network don't use tunneling.

Although each of these three approaches does offer some value, none of them is a complete security solution, and combining them still doesn't offer the proactive defense essential to protecting both corporate data and end-user experience.

Mobile devices are exposed to orders of magnitude more threats than laptops and desktops, with attackers actively seeking to breach devices via multiple mobile attack vectors. Staying ahead of this new breed of attacks requires a revolutionary approach to mobile security that goes beyond simply detecting attacks and sending notifications. Only by predicting attacks based on multilayered, crowd-based risk assessment, detecting actual attacks, and proactively protecting sensitive data on the device and in connected systems can mobile truly be secure.

Protecting against Network, Device, OS, and Application Vulnerabilities

Predictive intelligence and analytics that can instantly extract insights from big data have been pivotal to business success in the connected world. Enterprises can leverage the same powerful capabilities to upgrade their mobile security into a stronger breed of defense. Proactive mobile threat defense maintains intelligent security thresholds 24/7, ensuring business continuity by predicting, detecting, and preventing attacks along the full range of mobile attack vectors: physical (device-level), mobile apps, mobile operating system, networks, and mobile user behavior.

According to Statista, more than half of all global web traffic was from mobile devices in 2017. The November 2017 *Ericsson Mobility Report* estimates that total mobile data traffic (which includes web browsing, file sharing, software downloads, audio, video, and social networking) will increase from 14 exabytes per month worldwide in 2017 to 110 exabytes per month worldwide in 2023. Thus, attackers will increasingly target mobile platforms and enterprises that continue to use legacy IT solutions originally designed for desktop-based assets, making them easy prey.

Mobile workers often join public networks (such as Wi-Fi hotspots) when cell tower bandwidth is limited or cellular

coverage is poor, or to limit their use of expensive cellular data plans. Next-generation mobile threat defense should be able to recognize public locations that are suspicious by correlating millions of data points, gathered from public networks via crowd wisdom and performing anomaly detection. Crowd wisdom and instant socializing of detected threats from other mobile devices can infuse next-generation mobile threat defense with the real-time social proofing to accurately and efficiently flag suspicious public hotspots. A similar social-proofing threat detection can be applied to mobile app downloads.

WARNING

Though more complicated and costly, attackers can launch attacks via cellular interfaces — even when users turn off their devices' Wi-Fi connection.

Finally, mobile threat defense must encourage users to take appropriate actions and not leave themselves more vulnerable to attacks. Ideally, next-generation mobile threat defense should continuously educate and garner the trust of end users by showing relevant, timely, and actionable alerts. Several important ways of gaining employee trust and ensuring rapid adoption include providing:

- **Non-invasive experiences:** Most employees, contractors, and partners prefer mobile security to work in the background without infringing on their privacy or productivity.
- **Minimal footprint:** To maintain mobile security thresholds 24/7, the mobile threat defense solution should constantly run in the background, which is only possible by minimizing the solution's footprint regarding battery and bandwidth utilization.
- **Ease of use:** If a mobile security solution disrupts the familiar mobile experiences of employees, it may cause adoption churn and poor overall compliance.
- **Accurate alerts:** Non-adoption of mobile security can also result from alert fatigue caused by too many false positives. When this happens, mobile users will quickly start ignoring alerts.

REAL-TIME PROTECTIONS ARE ESSENTIAL TO MOBILE SECURITY

Detecting active threats and recognizing risky situations are clearly a first step in being able to secure mobile devices. But what happens then? It isn't enough to simply identify an incident if your end goal is to protect your sensitive data that either resides on, or may be accessed by, mobile devices. A common remediation approach is to integrate with an MDM solution that has policy enforcement capabilities and will respond to a device that is flagged as noncompliant by removing enterprise access privileges. Unfortunately, this can take time and is often too little, too late.

Mobile Threat Defense must be able to respond on-device, instantly, and independently of other solutions, because it can take less than a second for a hacker to steal corporate credentials and other sensitive information. Look for a solution that has real-time protections that activate automatically in response to any elevated risk and return to full function the moment the risk is removed.

The most powerful of these features is Mobile Network Access Control (mNAC), which allows the mobile app to protect data in a variety of ways. mNAC should be able to block communication with your sensitive servers and services to prevent a hacker from capturing credentials and data. mNAC should also have information about known malicious command and control servers so those can be blocked, regardless of the attack vector — SMS, email, malware, and so on. Other real-time protection mechanisms to look for include on-demand VPN for when an unsafe Wi-Fi is identified, or blocking the installation of malware, or terminating a malicious process operating with elevated privileges.

Almost as important as it is to take immediate protective actions, it's also highly desirable for mobile threat defense to return the device to full function and access in real time, as soon as a threat is removed, to optimize end-user productivity. Aside from the obvious gain in productivity that comes from rapid remediation, there is a less tangible benefit of usability and user satisfaction when security interruptions are minimized. The more seamless this process is, the happier users will be and the higher overall compliance will be, leading to a more secure mobile infrastructure.

IN THIS CHAPTER

- Recognizing the reality of software vulnerabilities
- Taking control of your endpoints with full visibility

Chapter 7
Good Endpoint Hygiene with Patch Management

An effective and comprehensive patch management strategy is an essential part of securing and protecting your organization. The vast majority of vulnerabilities being exploited are ones for which a fix has already been available from the software vendor such as the WannaCry ransomware attack that took place two months after the patch had been released by Microsoft. This chapter discusses vulnerabilities, exploits, and the critical role of patch management in endpoint security.

The Continuing Issues with Vulnerabilities

Security vulnerabilities in operating systems and application software are a fact of life. Continuous delivery (CD) and continuous integration (CI) models for application development are a double-edged blade with regard to vulnerabilities. On the one side, patches can be quickly released and efficiently delivered as soon as a vulnerability is discovered. On the other side, a vulnerability is more likely to exist in software that is rushed to market on accelerated timelines. This may explain the recent increase in

the number of vulnerabilities detected in software applications and operating systems. For example, according to CVE Details, the number of vulnerabilities discovered between 2017 and 2018 increased 128 percent.

Thus, effective patch management is — and will always be — essential to good endpoint security. Unfortunately, too many organizations lack full visibility and control of all their endpoints — desktop and laptop PCs, tablets, mobile phones, and other devices — to ensure vulnerabilities are fully patched in a timely and effective manner.


TIP

The initial release of Windows 10 marked a fundamental shift to a Windows-as-a-service paradigm for updating the operating system. A short time later, Microsoft adopted a similar model for keeping Windows 7 and 8.1 up-to-date. The move to a Windows-as-a-service model wasn't unprecedented because Microsoft had been using a similar model for keeping Office 365 updated. Along with the shift to a service-based paradigm, Microsoft introduced significant changes to the manner in which updates are packaged, distributed, and installed. However, enterprises must still test Windows updates and ensure they're installed promptly and correctly on all their Windows-based devices. These Microsoft updates can be quite large and so the option to use other deployment methods such as a multicasting or peer-to-peer package downloading capabilities can be a great alternative, especially for remote sites where downloading large files from the WAN is undesirable.

Full Endpoint Estate Visibility — Inside and Outside the Network

The modern threat landscape includes worms, malware, and ransomware targeting and exploiting known vulnerabilities in unpatched and/or underpatched operating systems and applications, resulting in costly, unproductive downtime and, in some cases, enormous damage to a company's reputation.

In addition, most organizations today have remote or mobile workers who may seldom connect to the corporate network. These roaming endpoints may go weeks or even months without connecting to the network and as a result can fall behind in

receiving the latest software updates and security patches. This combined with the increased number of vulnerabilities and the associated patches that are needed to be deployed further complicates this challenge. Organizations must be able to deploy software updates and patches regardless of where these endpoints are located and how often they connect to the network. It only takes one unpatched system to wreak havoc in an environment.

Another common challenge for many organizations is the expanded use of non-Microsoft operating systems and applications. Many organizations are using a mix of MacOS, Unix, and Linux along with many third-party applications (Adobe, Google, Java, Oracle, and so on). The ability to patch these operating systems and applications is critical. In fact, also according to CVE Details, recent data shows that 76 percent of the top 50 vulnerabilities found were from non-Microsoft applications and operating systems and therefore require careful attention. Using a single tool to test, deploy, and manage all the patches is highly recommended to centralize and simplify what can otherwise be a complex and time-consuming process.

EFFECTIVE PATCH MANAGEMENT

To address enterprise needs for effective patch management in all devices and applications — both on and off the network — a robust patch management solution should include

- Broad coverage across operating systems such as Windows, MacOS, Linux (for example, Red Hat, CentOS, and SUSE), as well as Android and Apple iOS
- Broad support for applications such as Office 365, Adobe, SQL, and Oracle
- Appropriate prioritization of updates (don't set higher than necessary) to minimize cost and service disruption
- Automation and optimization of the patching process
- Support for on-premises, peer-to-peer, and cloud-based patch distribution
- Grouping of assets for patch deployment — for example, to test the impact on a system or application or to distribute critical patches to specific higher risk user groups

Further fueling the need for effective, timely management of patch updates, fixes, and remediation is an increasing concern around governance and regulatory compliance, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS), and many others. Regulatory compliance mandates have forced enterprises to implement better control and oversight of their software and devices.

IN THIS CHAPTER

- Looking at web and email gateways
- Correlating security information
- Integrating with orchestration

Chapter 8
Integrating Endpoint Security with the Rest of Your Security Infrastructure

Endpoint security is just one of the defense layers, albeit an important one. Organizations already invest in network security such as web and email gateways, IT ticketing systems, and Security Operations Center (SOC) infrastructure. However, in most cases, all these investments work in silo leading to gaps in security that attackers try to exploit, high operational complexity, and high total cost of operations, as this chapter discusses.

The Need for Integrated Cyber Defense

Today's security infrastructure fragmentation is largely a result of organic, well-meaning reactions to rapid technology shifts. Cobbled-together collections of isolated point products simply

can't protect your organization, no matter how good they are individually. The only viable, long-term answer is an integrated, platform approach where all your security technologies, services, and threat intelligence work together to safeguard your people and information. Figure 8-1 shows the anatomy of an Integrated Cyber Defense platform architecture.

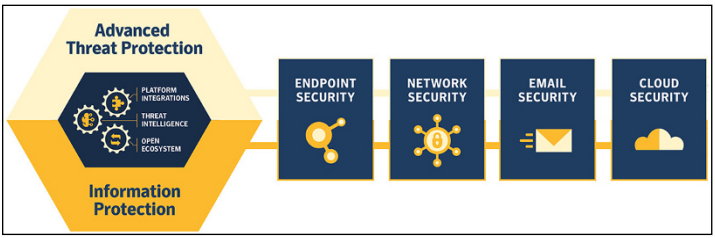


FIGURE 8-1: Anatomy of an Integrated Cyber Defense platform.

Web and Email Gateways

To strengthen security across the network, endpoint protection ought to be integrated with secure web gateways (web proxies) and email gateways. So how should this integration work? The network gateways (web or email) are your first line of defense. They use technologies such as advanced machine learning, heuristics, threat intelligence, sandboxing, and more to identify malicious content.

These detections should be pushed down to the endpoint protection agent to orchestrate rapid remediation (for example, blacklisting, undo actions, and more) to prevent lateral spread. In addition, the endpoint detections should also be shared with the network gateways to strengthen network security. Overall, the integration increases security efficacy for both the network and endpoints.

Security Information and Event Managers (SIEM)

SIEM integration should allow customers to stream or export threat events to a SIEM directly via a connector or app that can replicate event data generated by Endpoint Protection solutions

and Endpoint Detection and Response tools. These integrations should help SOC teams correlate and prioritize threat data with other critical events collected by the SIEM, providing broader visibility into the customer environment. The improved visibility and correlation should reduce the number of alerts SOC teams chase and ensure the focus is on urgent investigative tasks. The SOC team should also have the ability to drill down from dashboard views in the SIEM to get enriched details for a specific event or incident.

In addition, the SIEM integration should allow incident responders to blacklist and delete malicious files and isolate compromised endpoints directly from the SIEM console, initiating these actions that get executed by the endpoint agent.

For example, a security analyst should be able to view on the SIEM dashboard the top ten suspicious files, then drill down to see if there's any particular file hash related to the specific event or incident along with telemetry and analytics available. If required, the analyst should be able to quarantine the impacted endpoints during the investigation and then blacklist and delete files, all within the SIEM console.

Security Orchestration, Automation, and Response (SOAR)

Security Orchestration, Automation, and Response (SOAR) integration should allow customers to collect disparate security and threat data from a variety of different sources and enable automated and standardized incident response workflows (also assisted by human investigators). The integration should streamline the definition and execution of incident analysis and response procedures via automated playbooks (built-in and customized by the organization).

SOC teams should rely on SOAR integrations to orchestrate security and nonsecurity products so that the resulting data flows can be used for automation tasks that human investigators would otherwise need to perform.

SOAR integrations should bring together events from endpoint protection, detection and response, data loss prevention, and

network proxies to enable end-to-end management of incidents from initiation to closure.

Ticketing

Ticketing integration should allow customers to leverage their existing support notification and routing rules. Management should be able to monitor the progress of critical requests and report on incident performance metrics. This integration should ensure that each organizational function gets notified if an incident impacts their operations. Automated workflows that integrate incident data and associated events should support timely response and, if necessary, escalation.

IN THIS CHAPTER

- Keeping your end users safe
- Hardening endpoints
- Deploying honeypots
- Taking security to the cloud and integrating your security ecosystem
- Preventing software exploits

Chapter 9
Ten Tips for Effective Endpoint Security

This chapter gives you ten tips for effective endpoint security in your organization:

- **Conduct end-user security awareness training.** All the best security technologies and processes won't protect your endpoints if a user unwittingly reveals her password to an attacker. Cybercriminals target the weakest link in your security chain. Don't let your end users be that link. Conduct short, frequent, focused, relevant, and engaging security awareness training for your end users in a variety of formats such as in-person classes, short videos, one-on-one sessions, apps and gamification, email newsletters, and more.
- **Harden your endpoints with application isolation and control.** Whitelist known good applications, blacklist known bad applications, and isolate potentially good, but risky applications to prevent exploitation.
- **Be deceptive.** Honeypots and honeynets allow the good guys to turn the tables on the bad guys by misdirecting attacks to fake targets and data while simultaneously

revealing an attacker's presence on the network and his tactics and techniques.

- **Use personal firewalls and host-based intrusion prevention systems (HIPS).** Extend network security to the endpoint with personal firewalls and HIPS to block or drop malicious traffic at the endpoint.
- **Install a data loss prevention (DLP) solution.** Whether accidental or intentional, data loss can cause serious damage to an organization. DLP technologies can scan outgoing emails and file transfers for sensitive data (such as Social Security numbers and credit card information), and restrict transmission based on policy as well as prevent users from copying sensitive data onto removable media, such as USB thumb drives.
- **Enable disk encryption.** Encrypting storage on your endpoint devices protects sensitive data in the event a device is lost or stolen. Many data privacy laws have safe harbor provisions for encrypted drives.
- **Protect mobile devices.** Mobile devices drastically expand your attack surface. Mobile users don't think twice about connecting their BYOD smartphone to a public Wi-Fi hotspot. Enable security features on your users' mobile devices, including malware protection, and install mobile device management (MDM) and mobile application management (MAM) solutions.
- **Leverage cloud-based threat intelligence.** Cloud-based threat intelligence provides real-time threat information that helps protect your endpoints from zero-day threats and extends your security resources by leveraging security expertise from your vendor.
- **Integrate endpoint security with the rest of your security ecosystem.** Enable effective correlation of events by operating all of your security solutions as part of a comprehensive security strategy that provides a single pane-of-glass view into your environment.
- **Patch vulnerabilities.** Attackers exploit unpatched vulnerabilities in software and operating systems to infect endpoints with malware and pivot their attacks to other targets on the network. Installing and verifying patches in a timely manner is crucial to effective endpoint security.

Glossary

ActiveX: A software framework created by Microsoft that adapts its earlier COM and OLE technologies for content downloaded from a network, such as the Internet. *See also* Component Object Model (COM) and Object Linking and Embedding (OLE).

artificial intelligence (AI): The ability of a computer to interact with and learn from its environment, and then automatically perform actions without being explicitly programmed.

BITSAdmin: A command-line tool used to create and monitor the progress of downloads and uploads.

bring your own device (BYOD): A mobile device policy that permits employees to use their personal mobile devices in the workplace for work-related and personal business.

business email compromise (BEC): An exploit in which the attacker gains unauthorized access to a corporate email account and spoofs the email account owner's identity to defraud the company and/or its employees, customers, and partners.

Component Object Model (COM): A platform-independent, object-oriented system for creating binary software components that can interact. COM is the foundation technology for Microsoft OLE and ActiveX. *See also* Object Linking and Embedding and ActiveX.

cryptocurrency: A form of digital currency, such as Bitcoin, that uses encryption to control the creation of currency and verify the transfer of funds, independent of a central bank or authority.

deceptor: Bait, such as fake database credentials or files, used in deception technologies to lure attackers into revealing their presence.

domain name system (DNS): A hierarchical, decentralized directory service database that converts domain names to IP addresses.

dynamic link library (DLL): A type of file used in Microsoft operating systems that enables multiple programs to share programming instructions contained in a single file to perform specific functions.

ECMAScript: A scripting-language specification standardized by Ecma International in ECMA-262 and ISO/IEC 16262.

endpoint: A desktop or laptop computer or mobile device.

General Data Protection Regulation (GDPR): European regulation containing provisions that strengthens data protection for European Union (EU) citizens and addresses the export of personal data outside the EU.

Health Insurance Portability and Accountability Act (HIPAA): U.S. regulation that protects confidentiality and data privacy of PHI. *See also* protected health information (PHI).

honeynet: Also referred to as a *honeyfarm*, a large deployment of honeypots. *See also* honeypot.

honeypot: Computing resource used to detect, deflect, or otherwise disrupt a cyberattack.

Hypertext Transfer Protocol (HTTP): An application protocol for transmitting distributed and collaborative information.

indicators of compromise (IOCs): An artifact observed on a network or in an operating system that is likely to be associated with a breach attempt.

Internet Relay Chat (IRC): An application layer protocol that facilitates communication in text form using a client-server network.

JavaScript: A high-level, dynamic, lightweight interpreted programming language used to make webpages interactive and provide online programs.

JScript: Microsoft's dialect of the ECMAScript standard that is used in Microsoft's Internet Explorer. *See also* ECMAScript.

keystroke logger: A malware program that records keystrokes for illicit purposes, such as acquiring user IDs, passwords, and other confidential information. *See also* malware.

logic bomb: A program designed to perform some malicious function when a predetermined circumstance occurs. *See also* malware.

machine learning (ML): A method of data analysis that enables computers to analyze a dataset and automatically perform actions based on the results without being explicitly programmed.

malware: Malicious software or firmware that typically damages, takes control of, or collects information from a computer, including viruses, worms, Trojan horses (including remote access Trojans, or RATs), logic bombs, keystroke loggers, ransomware, and spyware. *See also* virus, worm, Trojan horse, remote access Trojan (RAT), logic bomb, keystroke logger, ransomware, and spyware.

master boot record (MBR): The most important data structure on a storage drive, containing the master boot code, disk signature, and partition table for the drive.

master file table (MFT): A database file that contains information about every file and directory on an NTFS volume. *See also* New Technology File System (NTFS).

metamorphism: A technique used in a virus to change its appearance in host programs without necessarily depending on encryption. The difference in appearance comes from changes made by the virus to its own body. *See also* polymorphism.

mobile device management (MDM): Software used to manage the administration of mobile devices.

network address translation (NAT): A technique used to convert internal, privately used IP addresses to external, public IP addresses.

New Technology File System (NTFS): A file system developed by Microsoft to store and retrieve files on a hard drive.

Object Linking and Embedding (OLE): A technology developed by Microsoft that allows embedding and linking to documents and other objects.

Payment Card Industry Data Security Standard (PCI DSS): Technology standard implemented to protect personal data related to credit, debit, and cash card transactions.

Personal Information Protection and Electronic Documents Act (PIPEDA): Canadian regulation that protects the privacy of personal information for Canadian citizens.

phishing: A social-engineering cyberattack technique widely used in identity theft crimes in which an email, purportedly from a known legitimate business (typically, financial institutions, online auctions, retail stores, and so on), requests the recipient to verify personal information online at a forged or hijacked website.

polymorphism: A technique used in a virus to change its appearance in host programs. For instance, it encrypts its body with a different key each time and prepends a decryption routine to itself. The decryption routine (known as the *decryptor*) is mutated randomly across virus instances, so as to be not easily recognizable. *See also* metamorphism.

PowerShell: A task-based command-line shell and scripting language built on the Microsoft .NET framework.

protected health information (PHI): Special type of information under U.S. law that includes any information about a health status, provisioning of health care, or payment for health care collected by a covered entity (such as a healthcare provider or insurance company) that can be linked to a specific individual.

PsExec: A server utility that lets you execute Microsoft Windows Server processes on a remote system and redirect output to the local system without installing client software.

ransomware: Malware that encrypts files on an infected server or endpoint and demands a ransom payment, usually cryptocurrency, to retrieve the decryption key. *See also* malware *and* cryptocurrency.

remote access Trojan (RAT): Malware that controls a system via a remote network connection for criminal, malicious, or unauthorized purposes. *See also* malware.

remote desktop protocol (RDP): A Microsoft protocol used to connect to another computer over a network connection.

script kiddie: An individual who doesn't have any programming or hacking skills, but instead uses scripts, malware, exploits, and other hacking tools developed by others to attack an endpoint or network.

security information and event management (SIEM): Provides real-time analysis of network and application security alerts.

security operation center (SOC): A facility that provides information security monitoring, assessment, defense, and remediation for compute and network resources both on premises and in the cloud.

server message block (SMB): A client-server communications protocol used to share files, printers, and other resources on a network.

spear phishing: A targeted phishing attack, for example, against a particular organization or part of an organization. *See also* phishing.

spyware: Malware that's installed on an endpoint (such as a user's computer), often for the purpose of collecting information about the user's Internet usage or for taking control of the user's device. *See also* malware.

tactics, techniques, and procedures (TTPs): A cyberthreat intelligence approach that analyzes the patterns and methods of a threat actor or group of threat actors to develop more effective security responses.

Trojan horse: Malware that purports to perform a given function, but that actually performs some other (usually malicious) function. *See also* malware.

update sequence number (USN): A 64-bit number in Active Directory that increments as changes occur in the directory.

virtual network computing (VNC): A desktop sharing application used to remotely control another computer.

virtual private network (VPN): A private network that uses encryption and encapsulation to communicate securely over public networks.

virus: A set of computer instructions that embeds itself within another computer program in order to replicate itself. *See also* malware.

Visual Basic Script (VBScript): An Active Scripting language developed by Microsoft and modeled on Visual Basic.

Web-Based Enterprise Management (WBEM): An industry initiative to develop a standard technology for accessing management information in an enterprise environment.

Windows Management Instrumentation (WMI): The Microsoft implementation of WBEM that provides the infrastructure for management data and operations on Windows-based operating systems. *See also* Web-Based Enterprise Management (WBEM).

Windows Script Host (WSH): An automation technology for the Windows operating system that provides scripting abilities comparable to batch files but with a wider range of supported features.

Windows Scriptlet (SCT): A script used to create a COM object that may be written in VBScript, JavaScript, or Jscript, and runs in Windows if WSH is installed. *See also* Component Object Model (COM), VBScript, JavaScript, Jscript, and Windows Script Host (WSH).

worm: Malware that usually has the capability to replicate itself from computer to computer without human interaction. *See also* malware.

WScript: A Windows service that allows you to execute VBScript files. *See also* VBScript.

Notes

Notes

Simplify with Symantec Endpoint Security.

Only Symantec provides single agent endpoint security with no gaps.

Endpoints protected
175,000,000

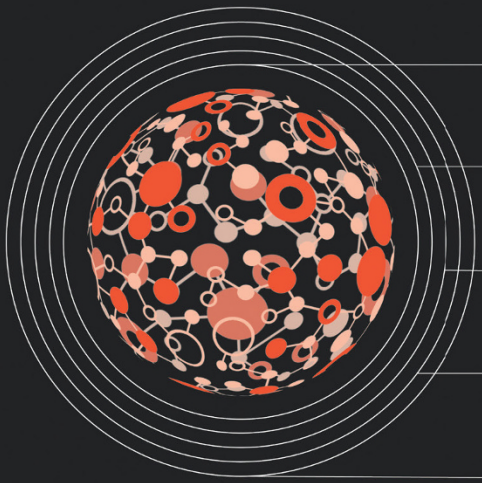
Malicious emails stopped annually
1,000,000,000+

Web attacks blocked annually
40,000,000,000+

1 Billion and counting
Wannacry infection attempts blocked

Over 730 Billion
Emails scanned annually

The most advanced, multilayered endpoint security.



- **Endpoint Protection**
- **Mobile Threat Defense**
- **Deception**
- **Endpoint Detection & Response (EDR)**
- **Application Isolation & Control**

Symantec™

Learn more about Symantec endpoint security.
Visit https://www.symantec.com/products/endpoint or contact your Symantec representative.

Secure all your devices with a single agent to reduce complexity and cost

Are you worried about ransomware holding you hostage or stealthy attacks stealing your data, but you're confused by buzz terms like machine learning? Then this book is for you. New techniques have vastly improved response to evolving attacks. *Advanced Endpoint Security For Dummies,* Symantec Special Edition explains how these technologies work and sets forth an integrated framework for endpoint security that covers it all: Windows, MacOS, servers, cloud workloads, and mobile. This handy guide also presents Symantec solutions that will give you the security you need while reducing costs and complexity.

Inside...

- Take a look at the framework approach
- Master new technologies like application isolation, deception, EDR, and mobile threat defense
- Analyze the role of threat intelligence
- Keep your systems and data safe
- Investigate and remediate incidents

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!


Also available as an e-book

ISBN: 978-1-119-48792-0

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.