Making Everything Easier!™

Bit9 + Carbon Black Edition

Endpoint Threat Detection, Response, and Prevention

FOR DUMMIES®

A Wiley Brand

Learn to:

- **Detect advanced attacks in real-time without signatures**
- **Get incident response in seconds with a continuous recorded history**
- **Prevent untrusted software with default-deny**

Brought to you by

Bit9 + Cb CARBON BLACK

Mike Chapple

About Bit9 + Carbon Black

Bit9 and Carbon Black have joined together to offer a complete solution for advanced threat protection for endpoints and servers. The merged company helps organizations protect themselves from advanced threats in two critical ways: by reducing their attack surface through new signature-less forms of prevention and rapidly detecting and responding to threats. They do this by leveraging the powerful combination of Carbon Black's lightweight endpoint sensor, which can be rapidly deployed with no configuration to deliver "incident response in seconds" and Bit9's industry-leading prevention technologies to continuously monitor and record all activity on endpoints and servers and stop cyber threats that evade traditional security defenses. Our lightweight real-time sensor and recorder, cloud-based services, and real-time enforcement engine give organizations immediate visibility into everything running on their endpoints and servers; real-time signature-less detection of and protection against advanced threats; a recorded history of all endpoint and server activity to rapidly respond to alerts and incidents; and real-time integration with network security devices, such as Check Point, FireEye, and Palo Alto Networks. One thousand organizations worldwide — from 25 Fortune 100 companies to small businesses — use Bit9 and Carbon Black to increase security, reduce operational costs, and improve compliance.

Endpoint Threat Detection, Response, and Prevention

FOR DUMMIES®

A Wiley Brand

Bit9 + Carbon Black Edition

by Mike Chapple

FOR DUMMIES®

A Wiley Brand

**Endpoint Threat Detection, Response, and Prevention For Dummies®,
Bit9 + Carbon Black Edition**

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-118-93016-8 (pbk); ISBN: 978-1-118-93030-4 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

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

Project Editor: Carrie A. Johnson

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Production Coordinator: Melissa Cossell

Table of Contents

Introduction

The word *cyberspace* first entered the global lexicon through science-fiction novels in the 1980s. Within cyberspace, the distinctions between governments and corporations were almost nonexistent. Hackers and organized crime and transnational terror organizations broke into systems in pursuit of money, fame, glory, chaos, and — most of all — valuable information. It's amazing how life can imitate art.

In today's real world, cybercrime is occurring at unprecedented levels. Hardly a week goes by that the news doesn't carry a story of a large organization falling victim to information theft, network intrusion, or other forms of cybercrime.

The methods used to defend networks must evolve and change constantly. Many of the methods relied on for years are no longer sufficient. After all, if you keep doing what you've been doing, you'll keep getting what you've been getting!

About This Book

Endpoint Threat Detection, Response, and Prevention For Dummies, Bit9 + Carbon Black Edition, explains how all organizations are targeted in the advanced threat environment. You discover how endpoints, servers, and even special-purpose devices can serve as entry points for adversaries seeking to exploit your network.

You also find out more about the nature of advanced threats and how they follow the cyber kill chain to infiltrate and exploit your organization's information assets. You discover how current endpoint protection strategies are insufficient against these threats, and I explain how you can protect endpoints through a new security life cycle of detecting, responding, and preventing security incidents. Finally, you learn how you can select and deploy an advanced threat protection strategy suitable for your security goals.

Icons Used in This Book

The margins of this book sport several helpful icons that can help guide you through the content:

TIP

When I present something that can save you time and effort, I toss in this icon to highlight it.

TECHNICAL STUFF

This icon offers a little extra info of a technical nature. You don't *have* to read it to follow the book, but it's an interesting aside.

REMEMBER

This bit of info is worth remembering. No need to tattoo it on your forearm or anything, just keep it in mind.

WARNING!

This icon flags information to take note of because it could cause problems.

Chapter 1

Identifying the Risk

In This Chapter

- Understanding how cybercrime impacts organizations
- Looking at the targets for advanced attackers
- Identifying the costs of being prepared

Every enterprise has high-value information vital to its success. As techniques become more sophisticated, this "digital gold" is increasingly vulnerable to exploitation. In this chapter, I examine the high cost of cyber intrusion to organizations, explain how adversaries target computing assets, and identify the costs associated with preparing to respond to security incidents.

Looking at the High Cost of Cybercrime

There is no doubt that breaches exact a costly toll on victims, in terms of both money and time. These stealthy costs often don't appear as line items on financial statements for a number of reasons. First, the costs are often indirect, resulting in wasted resources and missed opportunities. Second, organizations are incentivized to downplay the effects of cybercrime to avoid unwanted attention from the public and media.

From a financial perspective, the average data breach costs U.S. companies nearly $5.4 million. This price tag includes the costs incurred in detecting and responding to a breach, notifying victims, conducting post-response support, and lost business. Clearly, data breaches are financially burdensome on the organizations experiencing them.

In addition to these financial losses, organizations also suffer from lost time. Depending on the type of incident they experience, organizations may lose days, weeks, or even months of time to incident response activities. Figure 1-1 illustrates the average number of days required to respond to attacks in nine major categories.

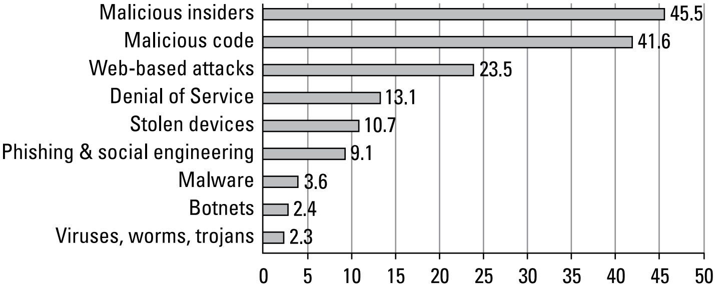


Figure 1-1: The average days required to resolve attacks.

Everyone's a Target

Almost every organization has some "digital gold" that outsiders may want to exploit. This data may include intellectual property, sensitive personal information about customers and employees, confidential business plans, or financial information. Every organization, regardless of industry, is a target for cybercrime, espionage, and state-sponsored attacks.

Retail and consumer

Most retailers have relatively small IT staffs and find themselves struggling to apply those resources to both meet business requirements for 24/7 availability and simultaneously provide the level of security needed to protect sensitive credit card information flowing over their networks. Maintaining security and compliance can be difficult tasks, as well. It's no surprise that retailers find themselves the frequent targets of adversaries.

Law firms

Law firms work with and manage extremely sensitive information on behalf of their corporate clients. This information presents a lucrative target to cybercriminals or espionage actors seeking to attack the client through a third party.

According to the American Bar Association, attackers frequently look at law firms as a secondary path to obtain confidential information about corporate targets while bypassing the client's main security controls.

Healthcare

Many healthcare providers now use electronic medical records (EMRs) to maintain and share sensitive health information about patients. The rise in EMR use prompted the release of updated HIPAA regulations governing the security and privacy of electronic Protected Health Information (ePHI). The electronic availability of this sensitive information about individuals presents an opportunity that's increasingly exploited.

Control systems

Electronic control systems are responsible for ensuring the effective operation of many critical infrastructure services. A wide range of industries, including energy, utilities, transportation, water supply, communications, chemicals, and manufacturing, all depend on industrial control systems (ICS), and these systems are vulnerable to attacks by both nation-states and terrorist organizations.

The stakes are very high when it comes to protecting ICS systems, particularly the Supervisory Control and Data Acquisition (SCADA) systems that control large-scale processes. These systems, if abused, could trigger explosions, spills, property damage, and even the potential loss of human life.

Not just the primary owner of sensitive information is vulnerable to attack. Networked business associates and partners represent additional avenues of attack for an enterprising adversary seeking a chink in the security armor.

Understanding Targets

After advanced attackers target an organization, they have many potential avenues of infiltration. While servers are likely targets, even the lowliest endpoint's sensitive information may be targeted or the endpoint itself may provide an actor with a toehold on the organization’s network that may be further exploited. Endpoints can then be used as entry points to get to other targets, such as servers, which are more likely to contain larger volumes of sensitive information.

Servers

Servers perform a variety of critical functions for businesses. They run mission-critical business processes and customer-facing applications and host large amounts of sensitive information. Therefore, they have naturally become popular targets for cybercriminals.

More than half of respondents to a Bit9 + Carbon Black survey said that targeted malicious software is their top server security concern. At the same time, 43 percent of respondents either confirmed that they’d been attacked or were uncertain whether they’d been attacked. With these stats in mind, it’s no surprise that servers are huge targets for cybercriminals or that they require significant attention from security professionals seeking to reduce the organization’s exposure to attack.

Endpoints

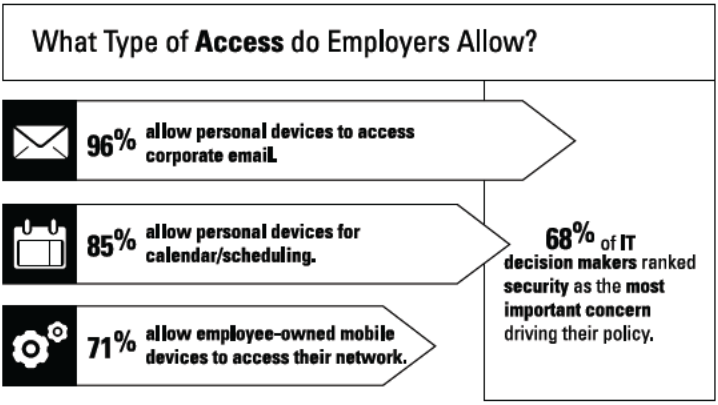
Employees in today’s businesses have access to a tremendous number of devices that enhance their productivity. It’s not unusual for employees to use a desktop in the office, a laptop while traveling, and an array of smartphones and tablets.

Virtual systems are vulnerable

Virtual servers don’t have special automatic security placed around them. The operating systems running in virtualized environments need to be secured in the same manner as those running on physical hardware. In fact, the use of virtual servers introduces a new set of security concerns that enterprises must address. Every virtual environment is governed by a hypervisor — special software that controls the interactions between virtual servers and the physical hardware. Security professionals must ensure that the hypervisor is hardened against attack and that the virtual networks leveraged by virtual servers are appropriately secured.

Each of these devices represents a potential entry point and target for cyber adversaries. IT departments must ensure that they contain appropriate controls to protect the data they contain from loss, theft, and corruption. The widespread use of mobile computing devices means that these controls must apply not only when devices are used on the well-defended corporate network but also extend to use in airports, coffee shops, and hotels.

The Bring Your Own Device (BYOD) trend in corporate computing means that employees also expect the ability to securely interact with corporate computing and information resources from their own devices. Figure 1-2 presents some surprising statistics about the prevalence of personal computing devices in business environments.



What Type of **Access** do Employers Allow?

96% **allow personal devices to access corporate emaiL**

85% **allow personal devices for calendar/scheduling.**

71% **allow employee-owned mobile devices to access their network.**

68% of **IT decision makers** ranked **security** as the **most important concern** driving their policy.

Figure 1-2: Types of personal device use permitted by employers.

Fixed-function devices

Computers are also found in surprising places. It's not unusual to find that retail point-of-sale (POS) systems, automated teller machines (ATMs), and industrial equipment controllers are simply embedded personal computers running specialized software. They commonly run standard operating systems and must be safeguarded against attack like any other system.

POS terminals handle large numbers of credit card transactions and, therefore, are routinely targeted by adversaries. Retailers running these systems often find themselves unable to adequately protect them against advanced threats because of a reliance on legacy security controls.

Scouting the Cost of Being Prepared

When developing a security program, businesses have many costs that they must consider. In addition to considering the direct costs of security controls that you want to purchase, also plan for the costs of incident response. Investing in incident response pays dividends by lowering the cost of security breaches. Each time you respond to a security incident, you expend time and money investigating the compromise, notifying customers, and dealing with the aftermath.

Chapter 2

Understanding Advanced Threats

In This Chapter

- Getting introduced to advanced threats
- Identifying the stages of an advanced attack

Advanced threats have existed in one form or another for at least ten years. Security analysts often have difficulty detecting and identifying these threats as advanced actors because they act in a stealthy manner. Also, there's often not a single analyst with access to all of the diverse information sources necessary to piece together the worldwide activities of an advanced threat.

The threats facing organizations as malicious actors attempt to mine their digital gold are diverse and evolving. Years ago, one of the greatest risks to enterprise security was the so-called "script kiddie" who worked in the wee hours of the morning running primitive attacks written by others. Today, the script kiddie has grown up and become more mature. He now has a job and is working with other hackers in an organized fashion with clear objectives. This is the era of the advanced threat.

In this chapter, I explore the world of advanced threats and explain how these expert attackers leverage the cyber kill chain to infiltrate and exploit their targets.

Introducing Advanced Threats

Advanced threats are organized, well-resourced, and determined to achieve the objectives set out by their leadership. Unlike the script kiddie or casual hacker of decades past, the advanced threat is a formidable adversary seeking out a specific target for exploitation.

As an IT professional, you should have a strong knowledge of the characteristics of an advanced threat. By understanding the motivations, tools, and objectives of your adversary, you can better prepare your defense-in-depth approach to securing your organization's digital gold. The defining characteristics of the advanced threat include

- **Range of technical tools:** Advanced threats make use of a wide variety of technical tools. Instead of having a single piece of malware, the advanced threat often develops its own exploits. The code used by advanced attackers often makes use of otherwise undisclosed zero-day attacks for which the target may have no defense (see the sidebar "Zero-day attacks" for more information).
- **Tactical sophistication:** Advanced threats have experience on their side. They have had time to develop a playbook for breaking into organizations. Out of their expansive toolset, they use the least sophisticated assets necessary to achieve success and still have the ability to adjust to the victim's defensive posture.
- **Integration with human threats:** Advanced threats don't limit their domain to technically sophisticated exploits. They understand and integrate the use of social threats as well, often leveraging phishing, social engineering, and traditional intelligence gathering activities to amplify the effectiveness of their technical tools. The key here is that it's a human on the other end. You need to make tactical decisions, be creative in the face of a roadblock, and so on.
- **Targeted at specific objectives:** The targets of advanced threats are carefully determined and align with the objectives of their sponsors. They aren't opportunistic but, instead, seek out the systems or individuals that are very likely to contribute to their objectives. Advanced threats conduct targeting analysis and understand their adversary before engaging in an attack.

When most people think about the objectives of advanced threats, they naturally think about the military and political objectives of nations and think that they don’t have resources that fit these objectives. Remember, however, that organized crime and political activists are also advanced threat sponsors. If you have money or a public-facing website, you’re a legitimate target!

- **Well resourced:** Governments, organized crime, terrorist groups, and other well-funded organizations are behind advanced threats. The sponsors of these groups provide them with financial means, technical talent, and intelligence gathering capabilities that enable their success.
- **High degree of organization:** Advanced threats operate more like military units than hacking clubs. They have well-defined leadership structures and operate very efficiently. They’re organized around their mission.

Zero-day attacks

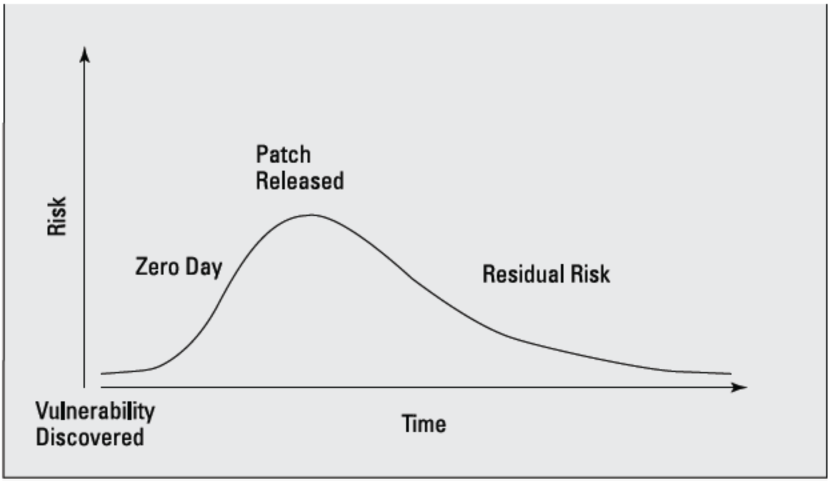
One of the most potent weapons wielded by advanced threat entities is the zero-day attack. These attacks exploit software vulnerabilities discovered by the attacker that allow the attacker to bypass security controls. Instead of disclosing the vulnerability to the security community, the attacker develops an exploit and adds the exploit tool to its arsenal for use at a strategic moment.

The danger behind zero-day attacks is that there is no patch that target organizations may apply to prevent systems on their network from falling victim. The sidebar figure shows the “window of vulnerability” — notice that the risk increases from the time of discovery until the point when a patch or signature update is released and then diminishes as system administrators apply the patch. Many companies fail to patch quickly, which further increases the window of opportunity for the attackers.

Defending against zero-day attacks requires the use of security technologies that leverage techniques other than blacklisting. When defending against a novel attack, security professionals must rely on a defense-in-depth strategy that uses real-time, signature-less detection to proactively act on potential threats.

(continued)

(continued)



The bottom line is that the advanced threat is unlike any information security risk faced by previous generations of security professionals. Organizations and individuals targeted by advanced threats are at the receiving end of a military or paramilitary attack and must organize their defenses accordingly.

Attacker Motivations

There are many different types of advanced threat actors and each has different motivations. Three common driving forces behind advanced attacks include the following:

- **Cybercrime:** Many advanced attackers simply seek financial gain. They seek to steal money, obtain information, or hijack computing resources in an attempt to achieve a windfall.
- **Hacktivism:** Other advanced attackers seek to use their hacking skills to advance a political agenda. They typically engage in denial of service attacks and website defacements designed to embarrass or disrupt their target.
- **Cyber espionage:** Attackers in this category seek to steal information to gain a political, economic, or military advantage, which can often be funded and directed by nation-state governments.

- **Insiders:** Advanced attackers aren't necessarily limited to outsiders. For example, consider a disgruntled employee looking to steal information and sell it to a competitor, or perform some type of sabotage.

The types of attackers targeting a specific organization depend on that organization's mission and its global reputation.

Looking at the Stages of an Advanced Attack

When an advanced attacker seeks to infiltrate an organization, it follows a sophisticated, well-defined process that allows it to leverage its skills effectively and avoid detection. Lockheed Martin researchers Eric Hutchins, Mike Cloppert, and Rohan Amin, developed a model known as the Cyber Kill Chain to help security professionals understand this process. Figure 2-1 illustrates the steps in the Cyber Kill Chain.

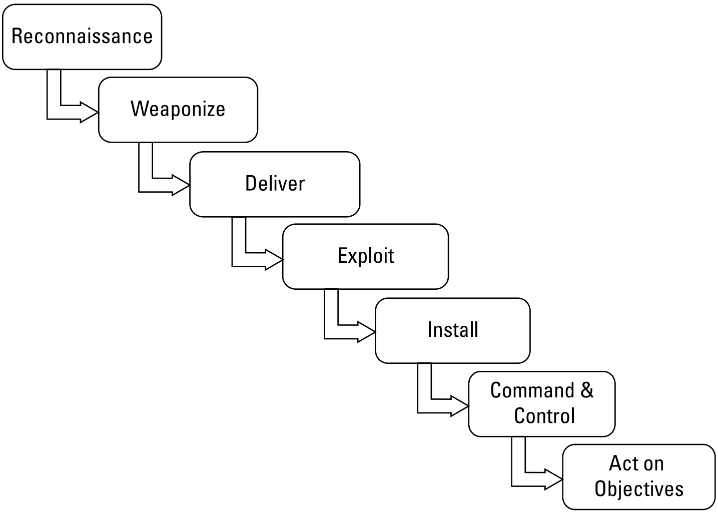


Figure 2-1: Stages of an attack, using the Lockheed Martin Cyber Kill Chain.

Lockheed suggests that organizations understand the Cyber Kill Chain in order to get inside the minds of advanced threats and engage in intelligence-driven network defense. In this section, I briefly describe each of the steps in the Cyber Kill Chain.

The Cyber Kill Chain process is an effective way of understanding the highly organized, technically sophisticated activities of advanced threats. IT staffers seeking to build secure enterprises may use this model to understand the nature and methodologies of their adversaries.

Reconnaissance

Smart military planners never act without knowledge of the enemy's defenses and tactics. This is just as true in the domain of cyber warfare as it is in the realm of air, land, and naval combat. Advanced threats understand this and conduct careful research before launching a cyberattack.

The first step of reconnaissance is to identify appropriate targets that, if compromised, would meet the attacker's objectives. For example, an attacker seeking to infiltrate a hospital's medical records system may target the system administrator as a likely way to gain access.

After they've selected a target, the attackers then gather as much intelligence as possible to inform the next stages of their attack. This can include gleaning information from public websites, social networking, media reports, and other sources. The attackers seek to learn as much as possible about their target before launching any form of attack.

Weaponize

After attackers have identified and researched an appropriate target, they then develop a weapon custom-tailored to their target. They analyze the information systems used by the attacker and select an exploit that affects an operating system or application known to be used by the intended victim. This may include the use of a zero-day exploit if both required by the technical sophistication of the target and justified by the target's value to the attacker.

Attackers are reluctant to use zero-day vulnerabilities against all but the most valuable target. Each time they launch a zero-day exploit, they run the risk of the attack being detected and made known to the security community. After this occurs, the zero-day attack loses its effectiveness as a weapon.

When an exploit is selected, it must be embedded in a delivery mechanism appropriate to the exploit and target. For example, the attacker may embed code exploiting a vulnerability in Adobe Reader in a PDF file. Java exploits then may be coded into a website that uses Java technology.

Deliver

After carefully selecting a target and weapon, the advanced threat must then deliver the weapon to the intended target. Common delivery mechanisms include the following:

- Sending a carefully designed spear phishing message that tricks the target into clicking a link
- Placing an infected file on a USB drive and getting it into the target's hands as a gift or leave-behind
- Storing the infected file on a website known to be frequented by the target
- Sharing an infected file with the target through a cloud-based file sharing mechanism
- SQL-injection attacks, where users try to send malformed data to database and backend-systems via websites and online forms to try to gain access or retrieve data

Unlike the phishing messages some attackers send to large numbers of individuals seeking to find a couple of unwitting victims, the spear phishing messages used by advanced threats are carefully designed to look like legitimate email sent directly to the intended victim. They make use of information that the attacker gathered during the reconnaissance phase to increase the likelihood that the target will act on the message.

Exploit

After the weapon is delivered to the target system, the weapon engages the selected exploit mechanism to gain control of the system. The exploit gives the weapon the ability to manipulate the target system with administrative privileges. This level of access enables the weapon to configure system settings, install software, and perform other actions normally limited to system administrators.

Install

After the weapon gains this all-important foothold on the system, it then has free reign to perform whatever actions it likes. The objective of an advanced threat is often to gain long-term access to the system for monitoring purposes. To facilitate this access, weapons often immediately install a remote access Trojan (RAT) on the target system. RATs, also often just called *implants* or *rootkits,* can hide malicious file, network, and process activity to allow the attacker to have continued access to the system, even after the weapon is no longer running.

With a RAT installed, the attacker now has more permanent access to the system. While a system reboot may annihilate the weapon if it is only resident in memory, the RAT is permanently installed software that will simply restart when the system comes back online. Through the use of RATs, the advanced threat may retain access to the target system for weeks, months, or even years.

Command and control

After a system is compromised by an advanced threat, the RAT normally establishes an outbound connection to a command-and-control server. This command link provides attackers with a way to communicate with the software on their victim systems without establishing a direct inbound connection.

The connections made to command-and-control servers often use standard HTTPS connections to emulate normal web browsing activity. Because the connections are encrypted, they're indistinguishable from any other HTTPS connection, other than the fact that their destination isn't a normal website. This approach allows RATs to limit the likelihood of their detection by intrusion detection systems monitoring traffic on the victim organization's network.

In addition to bypassing intrusion detection systems, the command-and-control connection is also designed to evade firewall controls on the victim network. While most network firewalls are set to block unsolicited inbound connections from the Internet, they often allow unrestricted or minimally restricted access to Internet sites when a system on the internal network initiates the connection. The attacker may then use this command-and-control connection to deliver instructions to the compromised system

Act on objectives

After establishing a command-and-control link between the victim system and servers run by the advanced threat, the Cyber Kill Chain reaches its final stages. At this point, the attacker has gained full control of the target system and may now manipulate it to achieve their objectives.

In many cases, the objective is to steal data from the system and return it to the advanced threat's sponsors. This may include stealing files from a targeted system, monitoring network communications, or logging all of the keyboard activity of the system's end-user. The organization collecting this data may receive a treasure trove of valuable intelligence providing advanced insight into the actions, thoughts and plans of the victim.

While the objectives of advanced threats often target information assets, attackers also may seek to cause physical damage to a target by manipulating information systems. In 2010, malware known as Stuxnet infiltrated the Natanz uranium enrichment facility, a critical component of the Iranian nuclear infrastructure. The worm caused the centrifuges used to enrich uranium to spin rapidly at speeds exceeding the manufacturer's safety specifications. This rapid rotation irreparably damaged the equipment, causing a major setback to the Iranian program.

In some cases, the victim system may only be an intermediate objective itself. If the ultimate target of an attack resides on a protected network and the advanced threat can't find a suitable delivery mechanism that would allow delivery of an exploit directly to the ultimate target, they may use an intermediate system as a jumping-off point for a final attack. After establishing the command-and-control link to the intermediary system, the advanced threat then begins the Cyber Kill Chain again, this time attempting to infiltrate the final target from the intermediary victim.

Chapter 3

Recognizing Current Limitations in Traditional Endpoint Protection

In This Chapter

- Seeing the limitations of antivirus software and intrusion prevention
- Understanding how incident response services can assist
- Identifying the capabilities required to respond to emerging threats

Technology professionals have a variety of tools in their belts designed to protect endpoints and servers against security threats. Many of these tools, however, aren't effective against the attacks waged by advanced threats. In this chapter, I explain the limitations of existing tools and discuss the capabilities required to respond effectively to an advanced attack.

Antivirus Software Limitations

Antivirus software has a long history in the security field, dating back to the 1980s. This software is designed to protect against a wide variety of malicious software, including viruses, worms, Trojan horses, logic bombs, and other threats. Antivirus packages are capable of detecting, blocking, and removing malicious software on a system.

WARNING!

Because of their reliance on signatures, antivirus packages are an effective way to protect against known threats, often called *nuisance threats,* and are installed on virtually every endpoint in a well-managed enterprise. While they're extremely effective against the threat posed by widely distributed malware, current antivirus technology doesn't provide effective defense against advanced threats, where a signature is typically not provided. Antivirus software can be used effectively against common malware but not against yet unknown or targeted threats. It really doesn't make sense to invest in "for fee" signature-based antivirus solutions when there are many "for free" alternatives.

Signature-based scanning

The major limitation of antivirus software is its dependence on signature-based scanning. Antivirus packages rely on constantly updated databases that contain digital fingerprints of all known malware. Antivirus firms employ large teams of security researchers who discover, catalog, and create fingerprints for millions of malware variants each year. They release signature updates daily and provide software installed on systems around the world with the most recent threat information available.

Antivirus software scans systems, email messages, and file downloads for the presence of these malware signatures. Any file or message suspected to contain malware may be deleted, quarantined, or repaired to prevent system infection. The issue with this approach is that advanced attackers often leverage zero-day attacks for which there's no signature available. Attacks that are previously unknown to the security community will be able to slip right past a signature-based detection system. Additionally, malware authors can make very minor changes to their code that prevents it from matching existing signatures, rendering it undetectable by signature engines.

Performance impact

Antivirus software must analyze each and every bit stored on a system's storage devices and memory, looking for the presence of malware signatures. This scanning is resource-intensive, requiring the use of disk bandwidth, memory, and CPU capacity. When a malware scan runs on a system, the scanning software may have a noticeable performance impact on user activity.

Specifically, scanners must check every file on the system, not just those that are likely to be threats. The scanner must check the entire contents of each file, looking for signs of malware. Administrators typically configure scans to take place on a scheduled basis, which may have a significant impact on the end-user if she's trying to use the system when a scheduled scan takes place. When users experience these issues, they're more likely to attempt to disable or circumvent the security control that's interfering with their work.

Point-in-time scanning

One of the techniques used by antivirus software is point-in-time scanning of a system. Due to the performance impact of antivirus software conducting full system scans, these scans are usually scheduled to occur daily or weekly. Administrators often schedule these scans to take place during the evening hours when the scan won't impact normal user activity. This provides a threat window where malware may run uninhibited between scans.

Host Intrusion Prevention

Some administrators lean on host intrusion prevention systems to supplement the protection provided by antivirus software. These packages, also known as *behavioral host intrusion prevention systems* (BHIPS), monitor activity on a system for potentially malicious actions. Unlike antivirus software, BHIPS don't rely on a database of all known malicious software and then watch for signs of known bad activities. Instead, they monitor the system over time, developing a model of normal activity and then flag deviations from normal behavior for administrator review.

WARNING! In theory, BHIPS are the ideal supplement to antivirus software because they have the potential to detect advanced threats. However, in practice these systems require an excessive investment of administrator time to tune and maintain. They also have very high false positive rates, triggering alerts on non-malicious activity. The combination of these two limitations often results in administrators disabling BHIPS capabilities because of the time spent maintaining them and responding to false alarms.

In addition, the information provided by BHIPS is often too shallow for useful analysis. It doesn't tell where unknown executable files were spawned. BHIPS often doesn't provide historical data that facilitates the time-based analysis required by security analysts. The model used by behavioral systems also is not capable of incorporating external information containing the latest threat intelligence. Furthermore, stand-alone host-based systems can't assess network effects or correlate multiple reports received from systems across the network.

Looking for Incident Response Services

When organizations find that they've fallen victim to a sophisticated cyberattack, they often retain the services of a firm that specializes in security incident response. These firms bring together teams of experts in a variety of security disciplines to quickly assess a security incident, contain the damage, and restore the organization to secure working order as quickly as possible.

While these services are often invaluable when responding to a security incident, they're also quite expensive and available only for a limited duration of time. After the incident is resolved, the expert team leaves, and maintaining system security is once again incumbent on the organization's information technology team. In this section, I explain some of the limitations involved with relying upon incident response services.

Limited data availability

Information systems generate massive amounts of data and are capable of logging extremely detailed records about their activity. These logs often contain critical information necessary to reconstruct the events that took place during a security incident. Responders depend on the availability of a detailed audit trail to identify how an intruder gained access to a network, the scope of their activities, and the data that they may have stolen.

One of the major limitations of incident response services is it's more than just collecting data — it's about collecting the *right* data and having a suite of tools available that allows you to understand it in context. When an incident occurs, the response is hampered by the lack of visibility into system events that took place while the attack was underway. Responders want to be able to quickly understand the relationships between systems and trace the spread of malicious files within the enterprise. Without purpose-specific tools in place before a breach, gathering all the data necessary for an effective incident response could take weeks or months.

Limited scope

When an incident response team arrives at an organization, they have a clearly defined scope of services. This is normally limited to identifying the circumstances surrounding a particular security incident and remediating the vulnerabilities that contributed to that incident.

Incident response teams often use sophisticated analysis and response tools that are licensed to the incident response firm. They don't leave these tools behind for the organization to use on an ongoing basis. In cases where the tools are open source or the organization opts to purchase a license, the incident response firm doesn't normally integrate them into the client's normal operations.

Home-grown tools

Many companies, and even some incident response firms, rely on the use of custom-developed tools that have been handed down through the ranks of incident responders. While they may be effective, they're the IT equivalent of duct tape and chicken wire.

Expertise required

Incident response is a specialty skill and experienced professionals are highly sought after and very well compensated. Only the largest organizations are able to maintain a full-time incident response staff, making it difficult to maintain incident response tools on an ongoing basis.

Non-continuous approach

Traditional incident response activities are targeted at a very specific activity instead of designing the type of continuous monitoring program that's essential to maintaining security in the age of advanced attacks. The alternative is to implement a solution that allows for real-time continuous recording of endpoint and server activity.

Matching New Threats with New Capabilities

Organizations seeking to maintain secure IT operations in this risk-laden threat environment must maintain a set of security controls designed to meet today's threats instead of those that were adequate for years past.

Responding quickly

Conventional security defenses are too slow. No matter how dedicated and talented they are, security staff simply can't keep up with the volume of data flowing through the enterprise architecture. Security systems such as intrusion prevention systems, firewalls, security information, event management systems, and antivirus software generate large amounts of information that adds to the data overload. Many businesses experience hundreds, or even thousands, of alerts each day and simply don't have the staff to respond to them all. They require the ability to triage alerts to a manageable level.

Not only must organizations find a way to respond to this information overload, they must also do so in a rapid manner. It's true that a cybercriminal may take months to identify targets, develop specialized malware that exploits specific vulnerabilities in targeted systems, and install command-and-control capabilities on targeted systems. Despite this, most advanced attacks aren't detected or stopped in time to prevent theft or damage.

After an attacker successfully infiltrates a system, the actual theft of data can take place rapidly. Massive amounts of information can be stolen in mere minutes or seconds. Security systems must be capable of quickly identifying an attack in progress and taking automated action to prevent damage.

In addition to reducing the delay in initiating a response, security systems should increase the efficiency of response staff. In some cases, enterprises implementing next generation security tools have been able to achieve significant time savings. With the new technology, one guy in one hour can get what it used to take ten guys ten days to get.

Detecting potential threats automatically

The modern threat operates faster than any incident response team can analyze and react to information. Security technologies that are configured to require administrator intervention before a response occurs are ineffective because the time taken by the administrator to analyze the attack may be longer than the short duration of the attack itself.

Effective security controls must be capable of autonomous operation. This doesn't mean that you don't need trained security staff; it simply means that they should be spending their time installing, maintaining, and monitoring automated response controls instead of conducting security response manually. Even the best security tools must be custom-tailored to the unique operating environment of your organization and that's where security professionals can lend valuable expertise.

Stopping malware execution

Embedding automated detection techniques in your environment is the first barrier to advanced threats, but successfully protecting your organization's security requires actually *blocking* and preventing suspicious software execution until the issue is resolved.

Chapter 4

Protecting Endpoints and Servers through a Continuous Security Life Cycle

In This Chapter

- Managing the security life cycle
- Understanding integrations between multiple security products and platforms
- Identifying strategies for protecting off-network devices

If the limitations of legacy security solutions make them insufficient for modern threats, how can organizations ensure they have adequate defenses in place? In this chapter, I explore how you can implement a life cycle approach to security that hardens your endpoints by establishing real-time visibility, detecting attacks without signatures, responding rapidly to attacks, and containing attacks by blocking and prevention solutions.

Defining the Continuous Security Life Cycle for Endpoints and Servers

Modern security strategies must reflect the reality that the threat landscape has evolved to the point where you can't count on creating an impenetrable perimeter. This means preparing the battlefield by deploying sensors on endpoints and servers that can detect and block in real time but also continuously record events in your environment that allow you to proactive respond to attacks as they happen. After an event occurs, a continuous recording allows you to "rewind the tape" and understand if a file moved laterally around your network, deleted itself, or performed other actions. Based off the information that these sensors deliver, you can incrementally strengthen your prevention technologies to improve your security posture moving forward.

In this section, I examine the three major elements of a continuous life cycle approach to security. I explain how you can build a defense-in-depth approach to security that accomplishes each of these three goals.

Detect

Despite the best of intentions, every security strategy has its weaknesses, and it's likely that determined attackers will eventually discover and exploit those vulnerabilities. Organizations with well-rounded security strategies are prepared to detect those incidents and share several common characteristics:

- **They monitor in real-time.** Advanced threats require rapid response. If you're going to detect attacks in time to respond appropriately, you must conduct real-time monitoring of endpoints, servers, and networks. Until recently, standard practice among system administrators has been to monitor and record network traffic but endpoints remained a blind spot.
- **They conduct behavior analysis.** Signature analysis is insufficient to detect zero-day attacks emanating from advanced threats. You must select technologies that integrate behavior analysis techniques to identify abnormal activity.
- **They use signature-less technology to predict attacks.** Performing exposure analysis is an important step toward preventing attacks, but it can also contribute to effective attack detection. When you perform your analysis, identify those risks that you were unable to successfully harden and use that information to predict how successful attacks may take place. This information can then assist you in detecting successful penetrations of your security controls.
- **They focus on the unusual.** These tools are effective because they develop baselines of normal activity in an

environment and then help administrators identify what's unusual and different. They can correlate reports of unusual activity across multiple systems, processes, and actions.

- **They confirm and prioritize risks.** You have a large number of systems and applications running in your environment. Developing catalogs of those assets and assigning them priority scores based on the likelihood and impact of compromise can help focus your attack detection efforts. Your highest value assets should receive the largest share of your attention.
- **They integrate threat intelligence.** There's a wide world of security professionals out there who are detecting attacks every day. Don't work in isolation. Leverage their knowledge by incorporating a threat intelligence product that incorporates signature feeds, malicious IP address information, and other community-sourced threat intelligence. You can build from community knowledge when stopping *known* threats and then use threat indicators to stop *unknown* threats.

Detecting attacks promptly is an important component of an information security strategy. While no one wants to be in the news because his organization suffered a security breach, you certainly don't want the added injury of a headline that reads "Firm Unaware of Security Breach for Five Years!"

Respond

In the unfortunate event of an attack against your organization, you want to be prepared to respond swiftly and appropriately in a manner that limits the damage and restores working order as quickly as possible. Ideally, your incident response capabilities allow you to react while an attack is in progress before it becomes a successful breach that steals your data.

To ensure that your organization properly responds to security incidents, try these five activities:

1. **Continuous recording.**

   A critical component of being able to rapidly respond is ensuring that you have an up-to-date continuous recording of all your endpoints and servers. It's also important to understand the relationships of those endpoints and servers to determine whether an advanced attack moved from endpoint-to-endpoint or deleted itself during an attack.

2. **Contain threats.**

   When you do detect a potential security incident, your first priority should be to contain the threat. Prevent it from exfiltrating data and/or expanding to other areas of your network. This is often accomplished by isolating the infected system, application, or file.

3. **Investigate and conduct forensic analysis.**

   After taking immediate steps to contain the damage, incident responders should turn to an investigation and forensic analysis of the attack. These activities are targeted at answering the following questions:

   - **How** did this start?
   - **What** did it do?
   - **How many** machines are infected?
   - **What** do we do about it?

   The answers to these questions are vital inputs to the next two stages of response.

4. **Design and test change.**

   With information in hand about the attack that took place, you should now turn your attention to designing and testing updated security controls that prevent a recurrence of the attack.

5. **Remediate and make change.**

   After you're satisfied that the proposed changes adequately address the security issues at hand with minimal side effects, roll them out to production and rest easy that you won't fall victim to the same attack in the future.

REMEMBER

By leveraging a continuous recorded history and understanding the entire attack process, you should be able to take what you learn with an incident and use it to improve your prevention in the future when performing a proactive exposure analysis.

Prevent

The primary objective of a sound security defense strategy should be to prevent attacks from occurring in the first place. The more attacks you can block before they occur, the lower the risk to your information assets. To prevent cyberattacks from penetrating your defenses, you can use these strategies:

1. **Perform proactive exposure analysis**.

   Periodically gather a team of subject matter experts from your organization that can assist with proactively identifying risks that require remediation. This analysis should include the use of technical tools that provide visibility into the security status of endpoints, servers, and networks and identify and prioritize potential vulnerabilities. This proactive analysis provides you with important information that an attacker would gather during the reconnaissance phase of the Cyber Kill Chain (see Chapter 3 for more info). You're much better off if that information is in your hands first.

2. **Establish trust in environment.**

   Establish trust in your environment by leveraging prevention solutions that can define what's approved software and what is not (default-deny). This is essential for critical systems such as servers, point-of-sale systems, and other fixed-function devices that should only be running trusted software. Using a trust-based default-deny solution is the best way to reduce your surface area to attack by preventing both known and unknown threats from executing in your environment. After defining trust and locking down these endpoints and servers, you should then look to roll out a trust-based prevention solution to remaining endpoints.

3. **Harden and isolate systems.**

   Follow a remediation plan designed to harden them against potential threats. You may also want to take systems that contain particularly sensitive information and/or unavoidable security vulnerabilities and isolate them from areas of the network where they may be exposed to external attack.

4. **Divert attackers.**

   It's inevitable that attackers will place your organization in their crosshairs at some point. Why not give them a juicy target to occupy their time while you detect and respond to their activity? The use of *honeypots* (decoy systems containing false but tantalizing clues of digital gold) is a time-tested technique to divert attackers from truly valuable assets.

5. **Prevent incidents through minimization.**

   Hardening systems and creating decoys can help prevent incidents. However, the best way to prevent an incident from occurring is to remove the target entirely. Reducing the sensitive information contained on your systems to the bare minimum necessary to transact business makes successful attacks less likely and, when they occur, less damaging.

6. **Engage end-users.**

   Make sure that everyone in the organization is actively engaged in security activities and understands their role. Remember, not all attacks are technical. Hardening your systems won't help protect you against phishing attacks.

These strategies can help you prevent successful attacks against your organization's systems and networks. Building a solid defense-in-depth approach to enterprise security will reduce your exposure to security threats. Following this process forces more security maturity and moves the organization toward a security baseline that's trusted and well-managed. Simplifying endpoints and reducing the amount of change leads to dramatic improvements in security.

Leveraging a Unified Platform

Perhaps the most successful strategy used in advanced threats takes advantage of the silos typical of IT organizations by deploying a variety of techniques that cross network and endpoint boundaries. Many security solutions are designed to monitor a single or discrete number of attack paths and vectors. A single security solution may detect and eradicate a single exploit, providing the illusion that an attack has been prevented or stopped successfully when in fact it has only addressed the tip of the iceberg. The siloed nature of tools makes it almost impossible for IT to achieve a holistic view of an advanced attack in progress or provide adequate forensics to trace all the steps and paths of the attack, assess all the damage, and address it comprehensively.

New generation security tools employ an integrated approach that spans the network and its thousands of server, desktop and mobile device endpoints to track and analyze the entire scope of the attack and its impact. Instead of a deluge of disjointed, disconnected information from multiple displays, logs, and consoles, IT gets a single view of the advanced threat and its entire impact, allowing technology staffers to coordinate a strategic response that addresses all of the attack components before the damage is done.

Integrating with Security Products

Many organizations use Security Information and Event Management (SIEM) systems to correlate the many sources of security information across the enterprise, looking for signs of attack. When choosing components of your security infrastructure, you should select products that fully integrate with your SIEM and allow the use of correlation rules.

Of course, every organization is unique, so the correlation rules that you use must be specific to your data sources and should include endpoint security information. A correlation rule that works with events from a Snort intrusion detection system may or may not be effective with information gathered from a similar NetWitness product.

When designing correlation rules, organizations should ask these questions:

- What types of threats do we want to monitor?
- What are the typical attack patterns for such threats?
- What are the sources and types of events currently being tracked within the SIEM?
- Which of these events are used most often in monitoring for potential threats?
- How often do investigations resulting from those events result in false positives?
- When investigating an event, what types of additional information does the analyst need?
- Are we collecting the right data to make incident response quick and conclusive?

Using these questions to guide event correlation across a variety of security products enhances your ability to successfully detect and respond to security incidents.

Supporting Multiple Platforms

The modern enterprise is a hybrid environment consisting of computers and mobile devices running a variety of operating systems. You need to select endpoint security products with monitoring, detection, response, and prevention capabilities that match the platforms in use in your environment.

The growing use of Apple devices in enterprises, either through corporate purchases or Bring Your Own Device (BYOD) programs means that a Windows-centric security model is no longer sufficient. Organizations should seek security products that function equally well on Mac and Windows platforms. Furthermore, a lot of organizations utilize Linux servers and therefore require coverage on Linux as well.

Protecting Off-Network Devices

Another thing that you should remember when considering endpoint protection is that endpoints move. More so than ever before, users are mobile and take their endpoints with them. The perimeter security defenses that provide them with secure networks in offices may be undermined when users remove devices from that secure perimeter and use them to connect to networks in hotels, coffee shops, and airports.

Unless you're able to convince your entire workforce to stop traveling (good luck with that!), you need to design a security strategy that extends protection to devices located outside of your secure networks. Controls should continue to defend systems when they're located on a potentially hostile network.

Chapter 5

Deploying Endpoint Threat Detection, Response, and Prevention

In This Chapter

- Incorporating the security maturity model into your enterprise security strategy
- Understanding the role of smart policies
- Deploying endpoint threat detection, response, and prevention consistent with your business needs

In this chapter, I explain how you can apply the security maturity model to your organization and deploy endpoint threat detection, response, and prevention with smart policies designed to protect your systems against emerging threats.

Security Maturity Model

As you prepare to select and deploy endpoint threat detection, response, and prevention, it's a good opportunity to assess the state of your organization's current security program on four dimensions:

- Oversight
- Technology
- Process
- People

For each area, you answer a series of questions that are compiled into functional area ratings and then overall ratings for each category. The maturity of your organization on each dimension is then assigned one of the following ratings:

- Nonexistent (0)
- Ad hoc (1)
- Repeatable (2)
- Defined (3)
- Measured (4)
- Optimized (5)

Performing this self-assessment provides you with an idea of the current state of your security controls and can assist you in defining the requirements for your endpoint threat detection, response, and prevention program. The products and vendors you choose should be able to work within your technical environment and culture, bringing you value wherever you lie on this spectrum.

Managing Smart Policies

Signature-based detection is simply not effective against advanced threats. While some people say that the alternative — whitelisting or application control — is too hard, they're not correct. These people think of whitelisting as a long list of appropriate files.

Smart policies aren't lists. They're covering mechanisms that catalog metadata, patterns, and system information. They then impart trust to each of those items. Simply put, smart policies are a short list of observations and actions that describe a system state as positive, negative, or neutral. Smart policies distill application control and attack detection into an understandable and manageable task.

Do you trust all of the applications contained within your main software repository? If so, you can express that trust using a single smart policy item. Do you automatically mistrust anything downloaded within a web browser? You can express that distrust in a smart policy as well. If you receive threat intelligence reports that rate a given binary file as "middling" and requiring further investigation, a smart policy can also handle that situation.

Smart policies can overlap, with multiple smart polices applying to a single file. Endpoint threat detection, response, and prevention systems allow this to occur and come to conclusions taking all of the trust ratings into account. Next generation security products allow you to express policies as imparting trust on a spectrum.

This section covers three major strategies that endpoint threat detection, response, and prevention products may take when evaluating software. You should seek to identify a product that provides a flexible deployment methodology. The ideal product lets you select from a set of available policies and choose the ones most appropriate for your computing environment.

Detonate and deny

Next generation technologies from some vendors can "detonate" a suspect binary inside an isolated virtual machine (or even several in different virtual machines with different configurations). *Detonate and deny* technology observes the behavior of that binary — from file writes to memory access to registry changes to network access — and records all of it for analysis.

After recording this behavior, the security product assigns a threat rating to the binary based on the sum total of observed behaviors. The application may seem mildly suspicious, may be clearly attempting to hijack a system, or may map exactly to a specific known threat. The software may install other attack tools, "phone home" over the Internet, or even begin exfiltrating information. Detonation technologies can catalog these behaviors and make them available to other security systems to take action.

You may configure detonate and deny technology to target certain file types that you consider suspicious. For example, you may route all binaries created by browsers, PDF readers, and MS Office applications to a detonator. Or you may choose to route binaries that lack a digital signature from a trusted publisher or are unknown to your security product.

This process may be highly automated through the use of event-based rules within your existing security products. For example, one rule may look for the creation of previously unknown files on your endpoints. When it detects a new file on an endpoint, the rule automatically submits the file to a sandboxed environment to "detonate" the file for analysis.

If the detonation returns suspicious results, another event-based rule may trigger a ban for that file on the affected endpoint. In addition, the tool may simultaneously create a policy blocking that file on the organization's next generation firewall, preventing it from entering the network in the future. This process results in a powerful feedback loop that allows threats identified on an endpoint to drive network-wide security policy.

The bottom line is that the detonation approach allows you to take a file from anywhere, detonate it, and then take action anywhere else. The ideal product allows a workflow from an arbitrary file source to an arbitrary action destination. This approach allows you to quickly evolve your enterprise-wide defenses in the presence of a new threat.

Detect and deny

Next generation endpoint security technologies also use signatureless detection technologies to identify both suspicious behaviors and novel attacks, especially targeted ones. For example, products in this category can flag binary files executing from unusual locations such as the Windows Recycle Bin, or files attempting to tamper with core operating system settings. This approach is known as *detect and deny.*

Think of detect and deny technology as a set of surveillance cameras that collect large amounts of information about your computing environment. They can correlate events within machines and across long periods of time. For example, the product may identify that the combination of four mildly suspicious activities on a single machine in a short period of time represents a threat when looked at together. The system then takes automatic action based on these circumstances.

Human operators may then quickly assess the information collected by detect and deny strategies. Products often allow them to drill down to investigate infected systems and processes further. After a quick investigation, the operator may take remediation action, such as banning files or locking down a system, all within minutes or hours, instead of days or weeks.

A detect and deny strategy focuses on smart surveillance and quick reaction, with capabilities to maximize the human element of detection and enforcement technologies that make positive reaction instantaneous.

Default deny

In the most restrictive security strategy, known as *default deny,* no software is allowed to run unless you have explicitly trusted it. The default is to deny execution to any binaries that haven't been deliberately trusted. Many organizations aspire to this goal because they want to be able to provide end-users with the software they need but otherwise lock down the environment, reducing both the number of successful attacks and suspicious alerts that require administrator investigation.

Of course, system administrators don't have enough time to create and maintain an accurate list of all software that may be allowed within an organization. For this reason, successful default deny strategies provide a variety of automated mechanisms to impart trust. These may combine characteristics of trust imparted by local IT groups with those gleaned from cloud repositories:

- Trusting all software contained in enterprise software repositories
- Trusting any software installed by a trusted configuration agent
- Allowing software execution if the software bears a trusted digital signature
- Imparting trust on software listed in a cloud-based reputation service
- Allowing end-users to make better trust decisions by supplementing their knowledge of the situation with threat information and security checkpoints

In addition, strong default deny policies include efficient and effective ways to manage exceptions. These allow you to match your company's particular cultural and operational needs, while still providing a high level of security. For example, you may choose a lower enforcement level that allows users to make approval decisions or a more stringent level of control requiring IT approvals.

Deployment Flexibility Matters

When it comes to enterprise security, one size does not fit all. Your operations may be more staff-centric or more automation-centric or somewhere in the middle. Your software deployment strategy may depend upon trusted repositories and configuration agents, or be nonexistent.

At the same time, your company culture may be open and permissive or more traditional and controlled. On top of that, you may want to focus more on detection — finding the bad guys — or more on prevention and the default deny strategy. You don't want a product or vendor that tells you what to do and how to deploy; you want one that looks at your requirements and environment and then works with your to develop the right approach.

REMEMBER

You need to be able to fit multiple solutions into the various parts of your ecosystems, and you need product knobs and dials that custom configure each one. And depending on how daunting this sounds, you need a services partner that can guide you efficiently and effectively.

Mobile Devices and BYOD

Almost every organization is either allowing some degree of Bring Your Own Device (BYOD) computing for mobile phones and tablets or plans to do so in the near future. It is no longer a matter of *if* organizations will allow personally owned devices in the workplace but *when* they will allow this use. BYOD provides great convenience to employees and allows companies to avoid the expenses of acquiring and managing mobile devices.

That said, BYOD comes with many security implications and consequences. Companies need to protect corporate data that resides on personally owned devices by preventing leakage from the device to external sources. To achieve this while remaining sensitive to the privacy of personal data on employee-owned devices, some companies are turning to mobile device management solutions that include *containerization* technology.

TECHNICAL STUFF

Containerization approaches isolate corporate data on personal devices and wrap it in a layer of protection. This includes encrypting data stored on the device, providing secure transmission of data and allowing secure communications channels between applications within the container and back-end servers.

The use of sensitive information on BYOD devices makes them a tempting target for advanced threats. Your endpoint threat detection, response, and prevention strategy should include policy and technical mechanisms designed to preserve the trust environment created on mobile devices.

Defining Your Requirements

As you move toward selecting an endpoint threat detection, response, and prevention product, you should identify the requirements that are most important to your organization. If you choose to conduct a request for proposal (RFP), you'll need to define these requirements well to solicit useful proposals from vendors. Even if you don't go the RFP route, it's helpful to know what you're seeking before you begin evaluating products. As you set out on your product selection journey, consider these key requirements:

- **Visibility:** Choose a product that allows you to record your environment continuously in real-time. This real-time visibility fuels detection, response, and prevention components of. The more items of relevance — memory operations, parent processes, registry access — the better.
- **Detonation capabilities:** Choose a product that doesn't lock you in to a single vendor. If you want to integrate with an existing detonation or next-generation firewall product, make sure that the threat protection vendor has experience with that integration. Look for products that both take in information from detonators and can also push data out to those detonators.
- **Enforcement capabilities:** Your endpoint protection solution should provide you with a wide range of possible responses to a threat, including banning files by name or hash value and/or extracting suspect files from the endpoint.
- **Lightweight agent:** Users don't want a heavy agent installed on their endpoints. Your goal should be to find a product with a lightweight agent that helps you identify issues and respond to them appropriately. Defense without business/productivity disruption is a fundamental goal.

- **Phased approach to default deny:** Flexible endpoint threat detection, response, and prevention solutions allow you to work your way toward a default deny approach in a manner consistent with the culture and operating environment of your organization by allowing
  - Your other chosen strategies to naturally impart trust
  - To help you see how far that gets you in terms of measuring risk and assessing operational impact
  - You to target low-hanging fruit that gets you one step closer
- **Signature-less detection:** Your chosen solution should use a wide variety of data sources and detection approaches when evaluating suspicious files. You want to avoid signature-based approaches that are vulnerable to zero-day attacks. Ideally the product has a rules engine or API that lets you and your expert staff participate in the creation of new detection mechanisms. A vendor may even enable the sharing of security knowledge within its customer base and facilitate turning that into rules and policies.
- **Efficient, high-value reporting and administration:** The solution should provide you with standard templates and practices for getting information and actionable items, and allow you to build out your own approaches as well.
- **Professional services with proven expertise in deploying protection:** Most deployments of endpoint threat detection, response, and prevention software take place with a professional services engagement. Make sure you choose a product backed by a team of professionals with experience deploying security software in organizations similar to yours.

Next generation security makes the effort affordable, but it's also new and may require changes in perspective. Choose a vendor who can guide you efficiently and effectively.

In the end, you need to choose an endpoint threat detection, response, and prevention product that best meets the security needs of your organization and can function within your existing culture. This list of potential issues should help you develop the specific requirements that will guide your product selection process to a successful conclusion.

Chapter 6

Ten Things to Look for in Endpoint Threat Detection, Response, and Prevention

In This Chapter

- Recognizing ten key requirements
- Understanding what to look for when selecting solution

Selecting an endpoint threat detection, response, and prevention solution can be a daunting task. A variety of products exist on the market and all offer different capabilities. Here, I give you ten (okay, 11) things that you should consider when selecting a solution:

1. **Minimal user impact**

   Advanced security solutions should be hassle-free for the end-user. They should be transparent during normal operation. Reducing disruption is key.

2. **Continuous monitoring and recording**

   On-demand or scheduled scanning creates a window of vulnerability. Continuous, real-time monitoring and recording is essential. Choose technologies that don't rely on sweeps or scheduled scans.

3. **Centralized storage**

   Endpoint agents should send results to a central server that can correlate events across systems and over time. Having the data already centralized is crucial when seconds count during an incident.

4. **Full attack and incident context**

   The product you choose should be able to provide you with a detailed look at a suspected security incident from all angles. This should include the ability to aggregate many sources of information into summary data as well as drilling deep into existing data sources. Each security analyst should be able to work her way through the data in a manner suiting her own style toward the needed answer.

5. **Threat intelligence**

   The best products leverage the knowledge of the community by incorporating external threat intelligence information from a broad variety of sources, both hierarchical and communal.

6. **Prevent untrusted software**

   You should use an endpoint threat detection, response, and prevention solution that allows you to establish and define trusted software within your environment. This allows you to fully secure systems by making it easier to prevent untrusted software from executing in your environment such as advanced and targeted threats.

7. **Open API**

   Products with open APIs allow integration with other security and analysis tools by facilitating the sharing of information between products. APIs also allow one product to trigger actions by another security or system management tool. Technical staff can write their own applications or "scripts" to customize the product to their exact needs.

8. **Speed of alert response**

   Effective products should facilitate rapid response to security incidents by providing automated responses and clear, concise alerts to administrators, along with an intuitive console that allows any human element to be executed rapidly and efficiently.

9. **Complements existing security ecosystem**

   You have a set of security tools in your enterprise now — make sure your advanced security product integrates with them.

10. **Platform coverage**

    Endpoint threat detection, response, and prevention solutions must cover all the platforms that exist in your environment, including Linux servers and Mac workstations.

Get rapid response capabilities in seconds

Traditional signature-based endpoint protection solutions struggle to protect against today's advanced threats and zero-day attacks. Enterprises need to detect and respond based on real-time monitoring and a continuous recorded history to reduce the attack surface with leading default-deny prevention solutions.

- ***Discover what real-time visibility and recorded history is — how it drives emerging detection, response, and prevention solutions***
- ***Detect attacks without signatures — respond earlier in the kill chain***
- ***Rapidly respond to attacks in motion — perform pre-breach incident response in seconds before data exfiltration***
- ***Reduce your attack surface with default-deny — only allow trusted software to run***

Open the book and find:

- How every enterprise is a target
- Why traditional endpoint security solutions can't protect your environment from advanced threats
- How endpoint threat detection, response, and prevention solutions stand apart from traditional security solutions
- What capabilities you need to protect your enterprise

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

FOR DUMMIES
A Wiley Brand

ISBN 978-1-118-93016-8
Not for resale