Making Everything Easier!™

Spikes Security Special Edition

Malware Isolation

FOR DUMMIES®

A Wiley Brand

Learn to:

- Assess the risks of browser-based malware in your organization
- Recognize the limitations of traditional detection technologies
- Deploy browser isolation technology to restore web security and freedom for users

Brought to you by

SPIKES SECURITY

Mike Chapple, PhD

About Spikes Security

Spikes Security, founded in 2012, is a ventured-backed startup based in Los Gatos, California. The company delivers enterprise-class network security solutions designed to eliminate the primary attack vector used by cyber criminals — advanced malware attacks delivered through the web browser. Spikes Security solves this problem with innovative, patent-pending "AirGap" technology, which effectively isolates the browser and all potentially malicious web content on a secure appliance outside the network. This enables all employees inside the network to safely leverage the power of the web without fear of attack. We invite you to learn more at **www.spikes.com.**

Malware Isolation

FOR DUMMIES®
A Wiley Brand

Spikes Security Special Edition

by Mike Chapple

FOR DUMMIES®
A Wiley Brand

Malware Isolation For Dummies®, Spikes Security Edition

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

ISBN 978-1-119-09865-2 (pbk); ISBN 978-1-119-09881-2 (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:

Development and Copy Editor: Elizabeth Kuball

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Suresh Srinivasan

Special Help: The leadership team at Spikes Security, with special contribution from Branden Spikes, Franklyn Jones, Scott Martin, and Rory Carracher

Introduction

Every modern organization has some form of information security program designed to safeguard information and information systems against external attack. One of the most common threats these programs defend against is malicious software, or *malware.*

Enterprise security teams use antivirus software, intrusion detection systems, firewalls, secure web gateways, and other controls to detect known malware and remove it from infected systems. Unfortunately, most of these controls use a reactive approach that can only defend against previously discovered threats or use a "best guess" approach, and only after an attempted system infection.

Recent advances in malware protection led to the development of a new type of control: malware isolation. This isolation approach prevents any malware — known or unknown — from even reaching the target system.

About This Book

Malware Isolation For Dummies, Spikes Security Special Edition, explains the basic concepts of malware isolation, and shows how you can use it to enhance your organization's information security program.

This book describes the malware risk landscape, including the known types of malware and the controls available to safeguard your organization's computing assets. It specifically introduces the concept of browser isolation, including the various use cases where this technology protects users against malware by eliminating the browser as an attack vector.

Here, you learn how to approach the implementation of a malware isolation system and, once you have a system in place, best practices for management and monitoring of your malware isolation program.

Foolish Assumptions

This book is designed for technology professionals of all backgrounds and does not assume familiarity with malware isolation. That said, I did make a few assumptions in writing this book:

- You have some experience with technology infrastructure and are familiar with servers, networking, and other basic infrastructure components.
- You have a basic familiarity with information security and are interested in enhancing your organization's security program.

Icons Used in This Book

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

When I present something that can save you time and effort, I mark it with the Tip icon.

Info marked with the Remember icon is worth remembering. No need to tattoo it on your forearm or anything. Just keep it in mind.

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

Beyond the Book

This book is designed to get you thinking about malware isolation and set you down the road toward implementing this important control in your organization. When you've finished this book, there are many other resources available to help you learn more about user monitoring.

A great starting point is the Spikes Security website: `www.spikes.com`. You'll find it packed with information about malware isolation, various deployment options, and the business and security benefits associated with this approach.

Chapter 1

Understanding Malware Risks

In This Chapter

- Looking at the growing risks of undetectable browser-based malware
- Identifying the common types of malware risk facing modern enterprises
- Understanding the capabilities and limitations of modern antivirus control mechanisms

Malware poses one of the most significant risks to the security of modern enterprises. Gone are the days of simple viruses and Trojan horses spread from user to user by infected media. The modern malware threat is much more sophisticated and insidious, using techniques to stealthily hide itself from detection and infect systems.

In this chapter, you learn how the reliance of enterprises on web-based applications makes them vulnerable to browser-borne threats and the advanced capabilities that malware uses in an effort to exploit the browser. You also learn about the current state of malware countermeasures and how those controls fall short of protecting the modern enterprise.

Focusing on the Browser

The web browser has become the most strategically important application in business today. It provides customers with access to the organization's websites to place orders, interact with data, and verify service status. Employees use web browsers to access customer relationship management

systems, participate in internal businesses processes, and even manipulate payroll data. These same browsers provide users with access to the broader Internet and allow interaction with computers around the world — activity that is invaluable for both business and personal productivity.

Unfortunately, the broad access that the browser provides also presents a significant risk to the enterprise. More specifically, web communication via the browser also provides a clear, unrestricted path for cyber criminals who use these connections to deposit advanced, often undetectable malware on endpoint devices, and then use those endpoints to launch attacks on internal business resources. Those attacks cost significant time, money, and disruption to the business, and damage the organization's reputation.

The underlying problem is the pervasiveness and complexity of modern malware. In today's Internet-powered global economy, cyber criminals can tap into a black market to buy and sell advanced, continuously updated exploit kits that target the vulnerabilities of specific web browsers, such as Google Chrome, Microsoft Internet Explorer, and Mozilla Firefox. Inevitably, these advanced malware components cross through the browser and infect a target system. They communicate back to a command-and-control network to await further instructions on how they should carry out their attacks.

In an attempt to stay ahead of cyber criminals, browser vendors have made significant improvements to browser security over the past few years. These efforts are quite sincere and continue to this day with the frequent release of security patches. Unfortunately, more patches mean more code, and an increasing codebase adds to the already massive attack surface, providing more opportunities for hackers.

Browser plug-ins and extensions (such as Adobe Flash Player, Adobe Shockwave Player, and Java) are loaded with vulnerabilities that provide additional means of entry for malicious code. These plug-ins are very useful and necessary, but when running on endpoint devices, they offer cyber criminals another point of attack.

How much of a threat does the browser pose? In a 2015 study by Ponemon Institute, organizations reported an average of 51 security breaches over a 12-month period from undetectable

browser malware. Employees unknowingly compromise enterprise security simply by clicking on a link or visiting a malicious website, even if they aren't tricked into downloading software.

Malware that enters through the browser often avoids detection by using trusted communications channels. When it establishes a foothold on even a single employee workstation, it then spreads to other systems on the internal network, increasing its access and potentially discovering and exfiltrating stores of sensitive information.

Browsers protected by traditional detection-based security technologies offer strong defenses against malicious code infections. In fact, they may even provide protection against 99 percent or more of known common malware attacks. There is no way for detection-based technologies to protect against the unknown malware attacks or zero-day attacks. Unfortunately, it only takes one successful breach to compromise enterprise security. Think about the number of employees in your organization who use the web every day and render web content on their endpoints. Is your organization satisfied with a security solution that is only 99 percent effective against known browser malware?

Understanding Malware Risks

IT professionals seeking to protect against malware must understand the techniques used by malware to penetrate organizations. This knowledge allows the design of effective security controls that follow a *defense-in-depth* approach to information security. The defense-in-depth principle states that enterprise security should consist of multiple layers of different types of security products that can work together to defend against various cyber attacks. The idea here is that enterprises following this approach should remain safe even when one of the detection engines fails. In reality, however, it's like putting screen doors on a submarine and hoping the water stays outside!

A traditional security architecture (see Figure 1-1) relies on multiple layers of detection-based technologies, each one trying to find and block malicious traffic. This architecture is becoming increasingly ineffective.

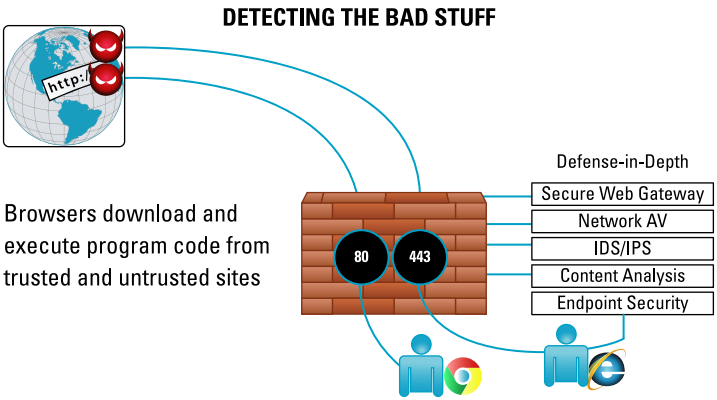

Figure 1-1: A traditional security architecture.

Traditional malware

The history of malware reaches back almost three decades to a dusty village in Pakistan where two brothers wrote a primitive virus named Brain, designed to protect their software from pirates. This virus infected the master boot record (MBR) of computers. This early malware spawned the field of computer security and antivirus protections.

In the early days of malware, IT staff concerned themselves with four major categories of threats:

- **Viruses:** Pieces of malicious code that require some user action to spread from computer to computer. For example, a virus may spread when a user copies data from an infected system onto a USB drive and then brings the infected USB drive to a new system.
- **Worms:** Malicious code objects that spread under their own power. They may exploit a vulnerability in an operating system or server software to gain access to a system. When they do gain access, they begin scanning the local network looking for other systems they may exploit. This allows them to spread very rapidly when they exploit a common vulnerability.
- **Trojan horses:** Malware objects disguised as useful software, such as a game, a utility, or even a security tool. When the user runs the Trojan, it performs the advertised function but also infects the system.

- **Logic bombs:** Malicious code that lies in wait on a system until certain conditions are met. For example, a hacker may program a logic bomb to remain dormant until a certain date and then simultaneously delete data from all infected systems.

These traditional malware threats persist today. They make use of advanced technologies to spread effectively and hide themselves from detection, but they continue to plague system administrators around the world.

Browser-borne malware

One major change in the computing landscape over the past decade is the dominance of the web browser. When malware first appeared on the scene during the 1980s, browsers simply didn't exist. In the decade that followed, the Internet emerged and browsers slowly became more popular. Over the past decade, the browser became the most important piece of software installed on a computer. In fact, many inexpensive low-end computers are now engineered to run nothing other than a web browser!

The widespread deployment of web browsers and the complexity of their underlying software make them a primary target for attackers. They no longer need to wait for users to carry around infected media from system to system in order to spread. Hackers can simply create malicious software and make it accessible over the Internet. If they somehow trick users into visiting an infected website (which can even be a trusted website), they have the means to spread malicious code to thousands of systems around the world quickly and easily.

Browser plug-ins and browser extensions are specialized software add-ins that extend the functionality of the browser. These add-in pieces of software enable third parties to build tools that can be used within the browser environment to affect the display of web pages.

Plug-ins (such as Adobe Flash Player, Apple QuickTime, and Adobe PDF Viewer) can provide significant gains in productivity and functionality by allowing users to view content that the default browser wouldn't be able to display. This makes

common plug-ins a prime target for attackers to exploit as a vector to infect a user's system.

Browser extensions can do even more than plug-ins because they provide third parties with the ability to affect the browser itself. Extensions provide additional functionality to the browser's user interface, such as additional buttons, processing capabilities, or new functionality for the browser user interface. Several extensions are publicly available to install that are known to carry malware and/or spyware.

Because plug-ins and extensions can run with all the capabilities and access of the browser or other installed applications, they can do almost anything to the computer they're running on. Avoid installing plug-ins or extensions whenever possible. This will limit your exposure to browser-borne malware.

The ideal nature of the browser as a vector for malware makes it the most common malware infection approach for modern hackers. Enterprises pay careful attention to browser security and spend countless hours educating users about the importance of safe browsing. Unfortunately, these efforts often fail when users intentionally or accidentally download malicious software through their web browsers.

Drive-by downloads

Hackers know the vulnerability of the browser and take advantage of it in a type of attack known as the *drive-by download.* When launching this type of attack, the hacker does not try to directly infect a targeted system; instead, the hacker places malicious software in a location where the system's authorized user is likely to encounter it. This may include sending a link via an email message or placing it on a trusted, commonly accessed website.

When the user visits the website, the malware may actively ask the user to download and install it. Users who fall victim to this type of attack may not read or fully comprehend the security warning messages that appear on their screen and then authorize the installation. Other drive-by downloads are stealthier and exploit vulnerabilities in the browser and plug-ins to directly install themselves on visiting systems without requiring user interaction or warnings.

Watering-hole attacks

Hackers recognize the significant potential of the drive-by download attack and often use a variant known as the *watering-hole attack* to compromise large numbers of systems. In this attack, the hacker spends significant time and energy compromising a legitimate website that receives thousands or millions of visits every day.

When hackers gain access to the site, they remain stealthy and install malicious software on the site. This software doesn't affect the operation of the site itself; instead, it attempts to infect the systems of visitors to the website. In 2014, Yahoo! was a victim of this type of attack and was unknowingly serving malware and infecting the browsers of millions of visitors.

Watering-hole attacks are highly effective, especially when combined with advanced malware techniques that avoid detection on the victim's system. Hackers often compete with each other to compromise higher-profile sites, priding themselves on the number of systems they infect from a single watering-hole attack.

Polymorphic attacks

As malware has matured, security professionals have developed a set of tools intended to identify and eradicate malicious code on systems. These tools often rely upon a technology called *signature detection.* The signature detection approach to malware identification uses a database containing the telltale signs of thousands of malicious code objects known to exist in the world. They then scan protected systems for the presence of those signatures to identify malware infections.

Malware authors caught on to this technology and realized that signature detection systems are effective only against previously discovered malicious code. In response, Panda Security estimates that professional hackers develop 160,000 new viruses every day and have invented the *polymorphic virus* as a way to counter signature-based defenses. The polymorphic virus rewrites itself slightly differently each time it infects a system. The code still performs the same function,

but it's different enough that it doesn't match an existing signature. Consider, for example, the following two sentences:

> Install this malicious software on the hard drive.
>
> On the computer's main disk, upload this malware.

Software comparing these two sentences would certainly see them as completely different, but the underlying nature of their instructions is identical. Polymorphic viruses use similar techniques to rewrite themselves in such a manner that they're slightly different on each infected system but remain true to their purpose.

Advanced persistent threats

Many of the attacks waged in the early days of malware were launched by a group of attackers known derisively as *script kiddies.* These attackers, who were often children, didn't necessarily understand the technology underlying their attacks. They simply downloaded attack tools (or scripts) from the Internet and ran them against large numbers of systems, compromising any vulnerable system they discovered.

As information systems became more crucial to businesses, governments, and other critical organizations, more sophisticated attackers came on the scene. Before long, governments, organized crime, and other patient and highly organized attackers discovered the potential of information warfare. They began to develop expansive offensive cyber-warfare capabilities.

These attackers differed from script kiddies in many significant ways. In addition to being highly trained and well funded, they chose their targets differently. Whereas script kiddies simply compromised any vulnerable system they could find, these new attackers had very specific targets in mind that allowed them to achieve their goals. They would then carefully and relentlessly plan their attacks against those targets using sophisticated technologies.

Many of these attackers make use of advanced techniques like *spear phishing* by infecting websites that their targets were known to frequent to ultimately gain access and begin their attack. After the attackers gain their initial access, they set up

a way to quietly exfiltrate the information they want — sometimes taking weeks, months, or even years to slowly gather the data.

These attackers have three defining characteristics:

- They use advanced technologies and methods.
- They're persistent by taking the time needed to minimize the ability to be detected.
- They focus on identifying, attacking, and compromising specific targets.

For this reason, security professionals call these attackers advanced persistent threats (APTs). Security professionals seeking to protect their organizations against an APT must use security controls that are much more sophisticated than those used to protect against script kiddies. The old defenses simply won't cut the mustard in this cut-throat environment.

Zero-day attacks

APT actors enjoy growing success launching *zero-day attacks,* which are vulnerabilities in systems discovered by the attackers but not publicly revealed. Because the security community has no knowledge of the vulnerability, vendors can't create patches or antivirus updates designed to correct the vulnerability. This makes zero-day attacks extremely effective for attackers and extremely dangerous for security professionals.

Security professionals believe that many attackers have research arms dedicated to discovering and cataloging zero-day vulnerabilities. In fact, cyber criminals frequently create stockpiles of fresh zero-day attacks for use in future planned attacks. Their appetite for discovering vulnerabilities is similar to that of research teams at software vendors, with one major difference: When a software vendor's security team discovers a vulnerability, they correct the problem. The attackers' researchers, on the other hand, let the vulnerability remain on systems around the world and place the zero-day exploit in their arsenal for later use. When they later decide to attack a particular system, they search the catalog for unused zero-day attacks that may be effective against that system and then take advantage of a highly precise weapon.

If attackers use a zero-day vulnerability enough, eventually security professionals will discover the attack and prepare a patch to correct it. Therefore, zero-day attackers are normally judicious with their use of these exploits, saving them for situations where other tools won't work effectively.

Malvertising

Malvertising has only recently emerged as a new category of web-based threats. As the name implies, it refers to malware hidden in online ads that appear on websites. Malvertising is particularly insidious because this malware appears as trusted ads on trusted websites, where advertising sales and delivery are typically managed by a third-party advertising network (which can also be highly trusted). In some cases, the ad requires interaction by the end-user to launch the attack. But the other, more frightening method requires only that the end-user visit the website hosting the ad. As soon as that happens, the malware can be delivered to the web browser.

Malware inside SSL

One last issue to be concerned with is malware embedded (and hidden) inside encrypted SSL tunnels. In November 2014, BlueCoat published new research highlighting the growing use of this delivery channel by cyber attackers. Many organizations have privacy policies that prevent them from decrypting and inspecting SSL traffic, so in many cases this malware has a clear, unrestricted path to the endpoint browser. And even in those cases where inspection is permitted, there is no guarantee that embedded malware would be detected.

Traditional Malware Controls

Malware attacks have devastating consequences on the organizations they target. Sophisticated malware can damage systems, steal sensitive information, and disrupt business processes. For this reason, information technologists spend significant time and energy defending the enterprise against malware threats.

Security professionals have a variety of tools at their disposal to assist with this challenge, ranging from traditional antivirus

software to advanced malware analysis engines that target previously unknown zero-day exploits. These tools are typically deployed as part of a multi-layer, defense-in-depth architecture designed to detect and block a broad range of attacks.

Antivirus software

Antivirus software is the primary tool for any information security program. It resides on endpoints and servers and scans those devices for the presence of malicious software. When antivirus software detects an infection, it notifies the system administrator and attempts to automatically remove the infected software from the device.

Antivirus software relies upon the signature detection technology discussed earlier in this chapter. Antivirus vendors, such as Symantec and McAfee, employ large research teams that scour the Internet seeking out new strains of malicious software. When they discover a new virus or worm, they develop a signature that describes its characteristics and update their antivirus software with that new signature.

Vendors issue dozens of new signatures every day. For this reason, it's vital that users of antivirus software maintain current subscriptions and update their signature databases regularly. But even with these continuous updates, signature-based antivirus software is becoming increasingly ineffective as the number of signatures grows exponentially year over year. The harsh reality is that cyber criminals prefer to invest time in the development of complex new threats instead of retreading previous viruses.

Intrusion prevention systems

Whereas antivirus software protects individual systems, *intrusion prevention systems* are designed to protect entire networks. These appliances sit on the network at key strategic chokepoints where they can monitor everything entering or leaving a protected network. They then use signature detection techniques to hopefully identify potentially malicious traffic and stop it before it can reach internal systems.

You may think of intrusion prevention systems as network-based antivirus protection in that it is designed to stop

malware on the network as soon as it's detected. Although it performs a similar function to antivirus, this technology has played an important role in a defense-in-depth approach to signature detection. But as is the case with AV software, its dependency on traditional detection techniques has made it less effective over time.

Secure web gateways

Secure web gateways (SWGs) offer another response to the threat posed by browser vulnerabilities and drive-by downloads. They serve as intermediaries on the network, preventing users from accessing known malicious sites and scrubbing requested content for malicious software.

With an SWG, the user's browser directly reaches out to the web server and requests content. The web server delivers the requested content. Although the SWG acts as a proxy and briefly terminates the connection for content inspection, it still delivers the original web content to the end-user device inside the network. This approach is fraught with risk because, if the SWG fails to identify malicious content, it still allows the external website to provide that content directly to the internal user.

Organizations that use an SWG introduce an appliance that facilitates and moderates this connection. Instead of allowing endpoints to directly reach out to web servers located on the Internet, those endpoints communicate with a web gateway. This gateway checks the request to make sure that it meets the organization's security policy; then the gateway itself reaches out to the web server to retrieve the desired content. After scanning the content for malicious code, the gateway sends the requested web content back to the end-user's system, where it's fully rendered by the local web browser. Unfortunately, like the other security products discussed here, these SWGs also rely on the same detection technologies to guess correctly if content is good or bad.

Malware analysis engines

Antivirus software, intrusion prevention systems, and web gateways all use a current database of known malicious software to analyze potential threats. This reliance upon signature

detection leaves systems vulnerable to zero-day attacks, polymorphic attacks, and other complex targeted attacks. These attacks are unknown to security vendors, so there are no signatures, leaving traditional malware controls defenseless.

Recently, a new tool has emerged in the anti-malware toolkit known as the *malware analysis engine.* These devices watch for any software entering the network and then check it for malicious activity using a technique called a *detonation chamber.* The malware engine copies the suspicious code to an isolated system and "detonates" it by executing it in a safe space where it cannot reach other systems on the network.

The analysis engine then watches the software to see if it tries to perform any unauthorized activity, such as scanning other systems on the network or attempting to communicate with a command-and-control server. Instead of looking for signatures of known malware, the analysis engine watches for patterns of activity that resemble malware actions.

Although malware analysis engines do provide an added level of protection over traditional antivirus controls, they also carry risks:

- **The algorithms used in malware detonation are not foolproof.** What if malware is designed to lay dormant for a long period of time before showing signs of malicious activity?
- **Malware analysis engines requires execution of potentially malicious software within your environment.** What if the malware manages to compromise the analysis engine itself and use that to gain a foothold on your network.

Again, any security products that depend upon detection techniques to block malware will have inherent limitations that prevent them from being fully effective. These controls must always make decisions about what's legitimate and what's malicious. Sometimes those decisions will be right, and sometimes they'll be wrong. When they're wrong, the results can be disastrous.

Chapter 2

Introducing Browser Isolation

In This Chapter

- Understanding how the principles of isolation can facilitate secure web browsing for employees
- Identifying the components of a browser isolation system
- Seeing how browser isolation systems fulfill business requirements and bring security benefits to the organization

If you read Chapter 1, you should have a solid understanding of the malware threat environment and the limitations of detection-based anti-malware controls. Anti-malware systems that depend upon signatures are only as good as the most recent virus definitions released by the vendor. When a zero-day exploit strikes, the system is powerless to defend against it until the vendor analyzes the new malware and releases a signature update. Likewise, advanced detection technologies based on heuristics, content analysis, or predictive behavior also have limited value because they ultimately rely on a best guess to determine whether web content is safe. If that guess is wrong, the hacker wins and you lose.

In this chapter, you discover an alternative approach to malware prevention that embraces the principle of isolation to prevent malicious software from ever reaching endpoints on your network. Specifically, you learn about browser isolation systems that create a safe environment for employees to visit any website without exposing their computers and mobile devices to the malware threat.

Understanding Isolation Principles

Security professionals have long understood the value of isolation in designing highly secure systems. One of the strongest ways to protect a system from a threat environment is to completely disconnect that system from any network capable of delivering malicious web content to endpoint devices.

The military practices this idea by building isolated networks for classified computing systems. Those networks allow classified systems to communicate with each other but do not permit connections to unclassified systems or the Internet. This prevents the accidental leak of classified information and eliminates the risk that malware will spread from the Internet onto the classified network.

Security professionals refer to the concept of separating secure systems from insecure networks as an *air gap.* In this case, the gap is the physical disconnect and separation between the two networks. Any data crossing between the secure and insecure systems must pass through an intermediary that is designed to review and transport the required data to the other network. This may take the form of an IT staffer with a USB drive or an automated gateway device that enforces the organization's security policy.

Isolating the Browser

Until recently, very few organizations outside of the military-industrial complex implemented isolation due to the technical complexity and costs associated with operating separate networks. Recent advances in technology have created a new approach to isolation: *browser isolation*. Instead of creating completely separate networks, browser isolation systems are being deployed in response to three critical issues:

- The web browser is the most strategically important — and most vulnerable — application on endpoint devices.

- The web browser is the only application allowed to fully render third-party code directly on the endpoint device.
- As a result, the web browser is now the most significant attack vector for cyber criminals.

Browser isolation systems work by combining the core functionality of web gateways with virtual desktop technology to isolate the user from direct access to web content. Users of browser isolation systems instead connect to a specialized appliance located outside the organization's secure network. This appliance contains a full browser and the ability to create isolated virtual sessions for each user requesting access to web content. The isolated web-browsing appliance performs all interaction with external websites on behalf of the user, transforms the content into a benign format, and delivers all audio, video, text, and graphics content back to the endpoint device. Users can view the content using a dedicated client viewer or through specialized integration into their existing browsers. (Components of the system are discussed in the next section.)

With this browser isolation architecture, all original web content — and any malware associated with it — remains isolated in the virtual machine (VM) created for each web session and is further isolated on the appliance. It has no ability to escape the appliance and enter the network. When the session is over, the VM is destroyed along with any possible malware.

Components of a Browser Isolation System

Browser isolation systems have three major components: a client web viewer, a web-browsing appliance, and a control center. These components isolate the user from the web browser, as shown in Figure 2-1.

Viewing web content

The viewer is the user's link to the Internet and the browser isolation system. The viewer's design mimics a traditional

web browser. It could be deployed as a lightweight client viewer or could be seamlessly integrated as a tab (or tabs) into any existing commercial browser. In either case, most users probably wouldn't recognize much of a difference in their web experience. All normal browser functionality would still be there, but the browser no longer connects directly to websites. Instead, it connects to the isolated web-browsing appliance, which processes and renders all web content requests. The client browser then views the results of those web requests.

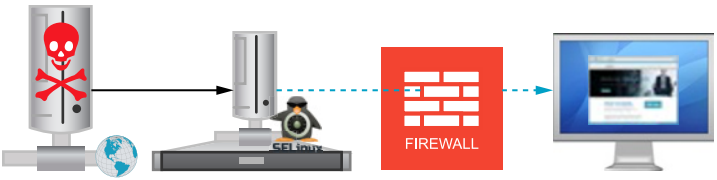

Figure 2-1: Browser isolation systems involve using specialized appliances outside the firewall that interact directly with requested websites and render all content on behalf of internal users.

The important principle at work here is that the web viewer never interacts with systems on the Internet that may contain malicious code. Instead, it interacts only with the trusted intermediary browsing appliance, which is carefully designed to never pass any executable content along to the viewer. The rendered web content is first transformed into a benign format that cannot be subverted for malicious purposes and then safely transmitted to the client viewer.

As noted earlier, some organizations may want to leverage their existing web browsers (for example, Google Chrome or Microsoft Internet Explorer) and still gain the benefit of browser isolation. In that case, the current browser can be redirected to connect to the appliance instead of the web. The appliance would still retrieve and process all web content, and then deliver the transformed content to a separate tab in the endpoint browser. In this deployment model, policies could be set so that the existing browser could still be used to access specific systems and applications on the corporate intranet, for example.

Browser isolation appliance

The web-browsing appliance is the bastion host responsible for interacting directly with potentially malicious websites. As shown in Figure 2-1, technologists should place the appliance *outside* the organization's internal environment to prevent potentially malicious content from entering the secure network.

The appliance contains a full web browser along with virtualization technology. Each time a user makes a web request, the appliance creates a dedicated VM for that web session and uses it to isolate the web session from the end-user, as well as other web sessions. The appliance retrieves web content that answers the user's request and then fully renders it within the isolated VM. But the actual content, which may include undetectable malware, is never delivered into the secure network. Instead, the appliance transforms the website's text, audio, video, and graphics and delivers that as continuously updated content to the end-user.

At the conclusion of the web session, the appliance destroys the virtual machine, and any malware sent by the web server gets destroyed along with the virtual machine. This process assures that no malware persists on the appliance and ensures a safe and secure browsing experience for all users.

These innovative appliances are typically designed to provision a specific number of concurrent web sessions without any degradation of performance or user experience. Just as important, these appliances can scale linearly to support virtually any number of users (or locations) within an organization.

Management console

System administrators benefit from the use of a centralized management console — essentially a control center — for the browser isolation system. This control center provides a consolidated view into the configuration, management and reporting functionality of the browser isolation system. Large enterprises can use a single control center to manage multiple sites simultaneously.

You can find out more about the management and reporting features of browser isolation systems in Chapter 4.

Containerizing the browser

Some organizations approach browser isolation through a different mechanism. Instead of using a dedicated browsing appliance outside the firewall, they build a virtualized browser container on each endpoint. In this scenario, the original content requested from the web server (including any hidden malware) is permitted to enter the network and is fully rendered by the browser on each endpoint device. To help prevent successful malware attacks, the browser processes all content inside an endpoint container that remains isolated from the rest of the system. The theory is that malicious content reaching the system will remain trapped in the virtualized container, unable to interact with the rest of the system.

Although this approach does isolate the browser, it can increase cost and complexity while still posing security risks. For example, deploying this containerization on every endpoint in a large organization requires testing and compatibility with multiple applications already deployed on the endpoint. It may also require upgrading endpoint performance to handle additional processing requirements. But the major problem with containerized browsers is that it allows potentially malicious content to reach the endpoint. If the virtualization technology fails or the malware understands how to escape a VM container, the malicious software may be able to interact with the underlying host operating system. This approach represents a false hope in the goal of effective malware isolation.

Meeting Business Requirements

Organizations seeking to adopt a browser isolation system should evaluate that system to ensure that it meets business requirements. Specifically, any candidate system should provide strong security and robust performance, and allow scaling to meet the organization's needs.

Security

The isolation technology used by the system should use multiple levels of protection to ensure that the end-user remains isolated from potentially malicious content. This includes the use of physical isolation through a web-browsing appliance and virtualized isolation to protect web sessions from each other.

In addition, it means transformation of all web content into a benign format that is completely safe to allow inside the network. Just as important, this transformed content can be delivered over specific ports, so that ports 80 and 443 (the primary access ports to the Internet) can be shut down between the internal client and the external appliance — thus eliminating a primary command and control (C&C) channel for malware. Shutting down the C&C connection is also valuable if the existing endpoint system had already been infected through previous web sessions before isolation was deployed.

Performance

Web browsing is critical to users and business processes throughout the enterprise. The browser isolation system must not be perceived as a burden or performance bottleneck, or users will be discouraged from using it. In fact, users shouldn't detect a significant difference between using a standard web browser and the isolation system's viewer. Ensure that the browser isolation system you choose maintains the highest-quality frame rate and responsiveness, even for high-bandwidth applications, such as audio and video streaming. When browsing is offloaded from endpoints to the browser isolation system, you'll likely find endpoints run much faster as the resource-hungry browsers are no longer choking these endpoints of available memory and CPU resources.

Scalability

Your browser isolation system must be able to meet the needs of your entire organization, regardless of the size or number of your locations. Ensure that the system's infrastructure allows you to easily add appliances, users, and scale capacity based upon your needs.

Scalability must extend to users off-premises as well. That means the browser isolation system should support a cloud deployment architecture, so that users anywhere can safely leverage the power of the web by connecting to isolation through the cloud.

To ensure nonstop performance of secure web browsing, appliances should also be deployed in fault-tolerant N+1 configurations, ensuring high availability even if a single appliance or component fails.

Benefits to the Organization

Browser isolation systems play a key role in enterprise security programs and deliver strong benefits to organizations choosing to deploy them. In this section, I show you the five key benefits provided by browser isolation systems that may assist you in building a business case for deploying this technology in your environment.

Preventing all browser-borne malware

Browser isolation systems (as the name implies) isolate the user from the web browser, eliminating the top threat vector for malware attacks on the enterprise. This game-changing architecture turns the tables on cyber criminals because there is no longer any reason to try to detect browser-borne malware or determine if the requested web content is good or bad. With a browser isolation system, you essentially assume all web content is potentially bad and isolate it all on a secure appliance outside the network. The result is complete protection against all known and unknown web malware, including zero-day threats, advanced targeted attacks, drive-by malware, polymorphic threats, and more.

Simplifying endpoint security management

IT staffers dislike endpoint security management tasks. The work of maintaining stable system configurations is tedious and challenging, especially when users visit websites containing drive-by downloads of malicious software. Browser isolation systems reduce the complexity of maintaining endpoint security management by eliminating the possibility that any type of downloaded browser malware will infect users.

This provides great value to the organization. Administrators don't need to waste money on AV software or worry about deploying complex browser containerization solutions on each endpoint. They also don't need to worry about managing browser versions or controlling the deployment of dangerous

plug-ins, such as Adobe Flash Player and Apple QuickTime. The browser isolation system renders all this content on behalf of the end-user and displays it through the lightweight viewer.

Reducing risk of business disruption

Isolating the web browser significantly reduces the risk of infection or a successful cyber attack on your business by shutting down the main attack vector that hackers use to gain a foothold in your organization. The net result is that you remain much safer from attacks by cyber criminals that want to harm your business.

This reduced attack risk means that you are less vulnerable to harmful events, such as:

- Disruptions in business operations
- Lost user productivity
- Theft of confidential information
- Damage to your brand reputation

This risk mitigation provides clear value to the business and allows you to focus on the value you provide to your customers.

Saving money on forensics and remediation

Browser isolation systems prevent malware from reaching the endpoint and reduce the overall risk of system infection. This is a big deal from a financial perspective, because cleaning up after malware infections can be quite costly. Consider these statistics from industry analysts:

- A 2015 survey by the Ponemon Institute revealed that most companies believed that they had been breached by browser malware at least five times in the past 12 months.
- Gartner estimates that each time a laptop becomes infected with malware, the IT department incurs $653 in costs remediating that infection.

- The Ponemon Institute also estimates that U.S. organizations suffering data breaches spend $5.4 million, on average, remediating the breach.

These are significant costs. If your browser isolation system prevents even a *single* data breach, it will pay for itself many times over. You simply can't afford *not* to deploy browser isolation technology.

Three hidden costs of not using isolation

In addition to the benefits inherent in deploying browser isolation systems, organizations should recognize that *failing* to deploy browser isolation bears hidden costs. Although these costs may not show up directly on an organization's bottom line, they reflect the opportunity cost of time spent by IT staffers and contractors performing unnecessary functions.

Here are three hidden costs of *not* using browser isolation:

- **The cost of deploying alternative solutions that don't work effectively:** Antivirus software and intrusion prevention systems are expensive. So are whitelisting and URL filtering. Browser containerization is difficult and time-consuming to install and maintain. All of these approaches can consume a significant portion of the IT budget, without effectively solving the web malware problem.
- **The cost of forensic analysis of infected systems:** One Symantec study revealed it can take nearly a year to discover a breach from a zero-day attack. When these advanced malware attacks infect a network containing sensitive information, businesses call in expensive consultants to assess the damage. Organizations using browser isolation avoid these costs by never allowing the execution of browser-based code on the endpoint.
- **The cost of recovering lost business data:** Security breaches often result in lost business information. Stolen credit card data is regularly bought and sold on the black market, costing businesses millions each year. IT staff must spend time and energy recovering data from backups and may need to call in consultants to reconstruct compromised systems. This consumes IT staff time and causes downtime for the rest of the business while staff reconstruct needed data.

Empowering employees with real web freedom

Web-browsing habits serve as a constant source of tension between employees and IT departments. Employees want to be free to surf the web for both business and personal use. They can't stand the policies and controls that IT puts in place to restrict web browsing to approved websites.

Employees routinely ignore IT staff's appeals to practice safe web browsing. In fact, most employees probably don't have a very clear idea of what "safe browsing" actually means! They only know that when their systems are inevitably infected, an IT staffer will show up with a "you should have known better" attitude and clean things up.

IT staffers, on the other hand, view employee web browsing as one of the riskiest activities taking place in the organization every day — and rightfully so. It is believed that the 2014 breach of JPMorgan Chase began with an employee clicking on a bad web link. So, IT remains frustrated at its lack of ability to control web browsing and spend countless hours cleaning up after browser-borne malware.

Browser isolation systems offer a solution to this dilemma. By placing the web browser in a secure container outside the organization's firewall, employees can surf the web with complete freedom while remaining protected from any malware on sites they visit. The content never reaches the endpoint and, therefore, can't infect the system.

IT staff only need to maintain the browser isolation system and never have to worry about user behavior or endpoint browser controls. The isolation system does the heavy lifting. Best of all, IT staff can end the "safe-browsing habits" lectures that they hate delivering and users hate hearing!

Chapter 3

Understanding Browser Isolation Use Cases

In This Chapter

- Learning how browser isolation systems fit into the standard enterprise-computing environment
- Identifying common use cases where browser isolation can bolster enterprise security
- Understanding the risks associated with web browsing by internal and external users

Browser isolation systems play an important role in an enterprise information security program. They provide an organization's security team with the ability to protect users, information, and computing systems from browser-borne malware.

Understanding the Browsing Environment

Before diving into the use cases, you must have a good understanding of the various components of the web-browsing environment. Figure 3-1 provides an illustration of a typical environment that includes different types of endpoints, different categories of websites, and the browser isolation system moderating the connections between endpoints and websites.

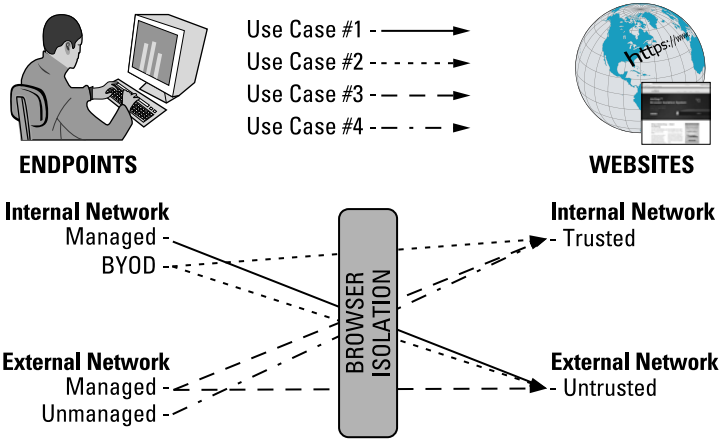

Figure 3-1: The typical web-browsing environment includes endpoints connected to both internal and external networks, accessing both internal and external websites. In each case, the user is isolated from all browser malware.

Endpoints are the devices used by employees and customers to access websites. Those devices may be connected either to an internal corporate network or to an external network, such as a hotel, coffee shop, or home wireless network.

Endpoints may be either managed or unmanaged:

- **Managed endpoints:** Managed endpoints are owned by the company and connected to enterprise configuration management systems. Generally, the security risks associated with managed endpoints is low because IT staff use policy settings to control the system configuration and maintain it in a secure state.
- **Unmanaged endpoints:** Ideally, an organization should minimize the use of unmanaged endpoints to ensure greater control and network security. But the growing "bring your own device" (BYOD) trend is the new reality in today's corporate network, even though it means a loss of endpoint control by IT. In this scenario, it's especially important to provide an elegant way of isolating BYOD browsers from potential cyber attacks, without the need to configure and manage each device.

Websites fit into two categories based upon the location of the site:

- **Internal websites:** Internal websites, located on the corporate network, host business applications that are developed and/or maintained by the company's IT staff. These applications are safe and trusted because trusted employees manage their security.
- **External websites:** External websites run on Internet-connected networks, and the company's IT staff may not even know their true location. In some cases, such as a software-as-a-service (SaaS) vendor, the company has a formal relationship with the vendor and IT staff trust the website more than those located on the general Internet. Most external websites, however, should be considered untrusted because any site can unknowingly serve malware.

Use Case 1: Internal Managed Systems Visiting External Websites

In the most common use case for browser isolation systems, employees using managed systems on the internal network require access to external websites for business or personal reasons. IT staff may have varying degrees of trust in those external websites and, therefore, should deploy browser isolation to protect users from malicious content.

There are two main risks associated with this use case:

- **Trusted managed computers often contain large amounts of sensitive information.** If a user accesses a website containing malware, the malware may infect the system and compromise that sensitive information.
- **An infected corporate computer provides intruders with a foothold on the corporate network.** They may then use this system as a launching point for more sophisticated attacks against the target company.

Browser isolation systems prevent external website data from directly reaching a corporate endpoint, eliminating the risk of browser-borne malware infection.

Use Case 2: BYOD Users Visiting Internal and External Websites

BYOD devices typically don't contain much sensitive business information. At first glance, this may seem like it reduces the risk they pose to the enterprise, but this couldn't be farther from the truth.

The main challenge with BYOD devices is that IT staff can't maintain their configuration in a known safe state. This makes BYOD systems more vulnerable to malware infections that may spread to internal systems or websites. For this reason, browser isolation systems play a critical role in reducing the likelihood that a BYOD device will become infected and protecting internal web applications from infections carried by BYOD devices.

Use Case 3: External Managed Systems Visiting Internal and External Websites

IT staff must also consider the risk posed to managed systems when they travel off the corporate network. Users may take their laptops home or on business trips and access both internal and external websites.

When managed systems leave the enterprise network, they also leave behind the security controls of that network. The enterprise firewall and web gateway no longer help protect them, and they're more prone to malware infections. They may then spread this infection to internal websites they visit. Also, when they reconnect to the corporate network, they may be used as a springboard for advanced attacks.

IT staff seeking to reduce the risk of this use case must extend the protections of the isolated corporate network to traveling users. They may accomplish this either by configuring the managed devices to access the company's browser isolation appliance even while disconnected from the corporate network or by leveraging a cloud-based browser isolation system for mobile users. In either case, employees would be protected from all browser malware, regardless of where they are working.

Use Case 4: External Users Visiting Internal Websites

Users outside your corporate network may need to access your internal websites for two reasons:

- Employees using their home computers may need to access business-related applications when they're away from the office.
- Customers, vendors, and other partners may need to access your internal systems to participate in your business processes.

In addition to the risks discussed in the "Use Case 2" section earlier in this chapter, there is an additional risk in this use case: If your website inadvertently contains malware, you may cause an infection of the external user's system. This infection may compromise the user's account on your website and may also cause reputational damage if the user believes the company was responsible for the damage.

To mitigate this risk, some organizations deploy browser isolation systems in "reverse" fashion. Instead of protecting access to external systems, the system isolates the internal application and servers from external users. Using this approach, malware can't spread from the internal application to the browsers of external users. Nor can malware on an external endpoint infect an internal website or server.

The cost of browser-based malware infections

A 2015 study of 645 enterprise organizations conducted by the Ponemon Institute and sponsored by Spikes Security found that these organizations experienced an average of 51 successful browser malware attacks during the previous 12 months — each costing about $62,000 to the business. So, collectively, browser-borne malware attacks cost U.S. companies an average of $3.2 million per year. These attacks were successful despite the fact that all companies surveyed had deployed a multilayer defense-in-depth security architecture based on traditional detection technologies.

Chapter 4

Implementing Browser Isolation

In This Chapter

- Building a browser isolation system suitable for your environment
- Identifying the five principles of isolation
- Managing and monitoring browser isolation systems deployed in your enterprise

When you've decided to deploy browser isolation to protect your organization against malware, it's time to begin the implementation process. You'll need to build your solution, implement isolation in your environment, manage the change with your end-users, and implement an ongoing monitoring and management program.

A Browser Isolation Solution

The underlying architecture of various browser isolation systems may vary slightly. In this case, I'm presenting a three-step deployment process based on client-server architecture, where the server is typically a purpose-built security appliance. This architecture represents best practices to ensure the most secure web browsing without fear of malware attacks.

1. **Install the appliance on your network.**

The appliance should reside in the DMZ *outside* of your network. This provides added protection against malware infection by keeping executable code completely out of your internal network. The number and

capacity of the appliances will be determined based on the size of your organization and estimated number of concurrent web users. Also, it's important to deploy in pairs if possible, to ensure reliable, high-availability web access.

2. **Ensure secure web viewing for employees.**

   Because internal employees will be connected to the isolation appliance rather than the web, the preferred desktop viewing experience must be determined. Organizations can install a lightweight dedicated viewer client to replace the traditional browser; or the viewing experience can be integrated into existing desktop browsers. In either case, the viewer transmits data between the employee system and the browser isolation appliance using an encrypted connection. Once it's configured, employees should test the viewer to ensure they can browse the web securely through the appliance.

3. **Block direct web access.**

   When you're certain that the system is in place and fully tested, you should modify your network firewall configuration to block direct web access — both port 80 and port 443 — from employee systems. This is particularly important if you decide to integrate the isolated web viewer into an existing commercial browser. This will prevent employees from directly connecting to potentially malicious websites. Instead, all web access will require use of the browser isolation appliance.

Deploying browser isolation isn't very difficult. Following a planned process ensures that you minimize the impact on your organization and deploy the solution in a secure, efficient manner.

Isolation Architecture

Browser isolation products use several layers of isolation technology to protect end-users from malicious web content. These include physical isolation, resource isolation, session isolation, content isolation, and attacker isolation. Each component of a browser isolation architecture works together to

prevent browser-borne malware and provide end-users with a safe and secure browsing experience.

Physical isolation

Browser isolation should be based upon physical separation and isolation. How does this work? End-users are located inside the corporate network, but the web browser is located on the appliance outside the network (or sometimes in the cloud). When end-users want to visit a website, they no longer reach out directly to the remote web server. Instead, the viewer passes the request to the isolation appliance. The isolation appliance then processes the web request, retrieves data from the remote server, and renders the original content for the end-user. This creates physical separation and isolation between the appliance (which may process malicious code) and the corporate network.

In contrast, an endpoint isolation architecture uses VMs and sandbox technology to isolate browser content and potential malware within containers on each endpoint device. With this architecture, there is no physical isolation between end-users and malware. Instead, there is coexistence, which significantly increases security risks.

Resource isolation

Browser isolation solutions achieve resource isolation by separating malware from sensitive resources on the end-user's system, such as the operating system, applications, and confidential files. In addition, this isolation extends to vulnerable tools like browser plug-ins, Adobe Flash, and Java. Malware sequestered on the browsing appliance simply can't reach these resources and, therefore, may not exploit the vulnerabilities they may contain. Unpatched Java isn't a problem if malicious code can't reach it!

What about the resources on the browsing appliance itself? The appliance is a locked-down, highly secured browser that runs a minimal operating system and contains no personal or confidential data. You may think of the browser as an empty room with no doors, no information, and no opportunity for malware to access the network and infect the organization.

Session isolation

When an end-user initiates an external web session, the browser isolation appliance automatically creates and launches a private web session contained within a virtual machine dedicated to that purpose. These virtual machines isolate all user sessions from each other, preventing the spread of malicious activity and cross-contamination between user sessions. Just as important, session isolation includes the isolation and protection of personally identifiable information (PII), thus preventing hackers from gaining access to any content that could compromise a user's identity.

When the user finishes browsing, the appliance completely destroys the virtual machine associated with that session. Any session data, cookies, or other information associated with the session is irrevocably wiped. This approach ensures that each user always enjoys a clean, secure, and fast browsing experience every time they launch a web session.

Content isolation

Browser isolation solutions isolate content in two ways:

- They transform all web content to benign virtual content.
- They isolate the transportation of the transformed web content.

When the solution renders the original web content inside a virtual machine, it's possible that the content contains malware. The appliance protects the endpoint against this possible malware by actively and continuously transforming all web content — including graphics, text, audio, and video — into benign multimedia streams. As a result, this content transformation makes it impossible for cyber criminals to inject malicious commands into the content.

From a content transportation perspective, the data streams carrying the user's requested content take advantage of strong encryption. The encryption keys used to protect this content are secret between the client and the appliance, preventing other users from eavesdropping on the web-browsing activity. And all of this happens over specified ports, because connectivity through ports 80 and 443 is not available.

Attacker isolation

Even with browser isolation's complete, end-to-end focus on security through isolation, enterprises must prepare to isolate any suspicious traffic that targets the browsing appliance itself. For this reason, the isolation appliance uses active monitoring that instantly identifies, isolates, and destroys any malicious traffic.

If the appliance detects any unauthorized activity, nonstandard system state, or blocked processes within a browsing virtual machine, it immediately destroys that virtual machine, along with any malware it may contain.

Managing Change

Any changes you make to your computing environment may prompt anxiety among end-users. People don't like change, and users who may already find IT intimidating may be fearful of any change in their computing routines.

The best way to handle this is with an aggressive, well-planned change management campaign. You should communicate early and often about the purpose of the browser isolation technology, highlighting the security benefits to the organization and the minimal impact it will have on their daily computer use.

Here are a few ideas for effectively communicating with users about your browser isolation deployment:

- Send regular emails beginning well in advance of the change and continuing throughout the deployment, updating users on the project status.
- Provide managers with talking points to help them answer questions about the technology and its impact on user activity.
- Tackle the question of privacy honestly and head-on. Explain that the encryption technology used by the browser isolation solution offers enhanced privacy over traditional web browsing.

- Host demonstration sessions on a drop-in basis where users may stop by a break room or other common area and see the technology in action.
- Provide hands-on training opportunities that allow users to try out the software before it appears on their own computers.

Don't underestimate the importance of these change management issues. Failure to address the "soft side" of change is one of the leading causes of technology project failures.

Managing and Monitoring Browser Isolation Solutions

After your browser isolation solution is in place, you have to turn your attention to the ongoing monitoring and management of your new technology.

If you have a service desk or other Tier 1 support infrastructure, they will likely handle most user questions and concerns. The security and systems administration teams will, however, retain repsonsibility for operating the system and ensuring that it continues to effectively protect the organization against browser-borne malware.

Reporting

One of the most important capabilities of any security system is its built-in reporting functionality. The reports provided by your browser isolation solution offer you insight into the system's effectiveness and may point to other security issues that you must address.

There are three primary reporting capabilities that you should incorporate into your security operations processes:

- **Dashboards:** Dashboards provide at-a-glance insight into system operation. You see key statistics about the number of security incidents, performance of the isolation appliance, number of connected users, and other critical metrics. Be sure to customize the dashboard to meet your organization's reporting requirements and

then display it live on a monitor visible to members of your security team.

- **Alerts:** Alerts offer real-time insight into critical situations. If the system identifies a security violation, experiences a performance bottleneck, or suffers a failure, alerts delivered via email or SMS attract immediate attention from administrators allowing the prompt restoration of normal operations.

  Excessive alerting can train your responders to ignore valid security violations. Be sure to fine-tune your alerts to minimize the number of false alarms.

- **Reports:** Reports allow the analysis of security trends over time. You find out if your awareness efforts are effective by seeing the number of times users browse to malicious sites, identifying trends in web-browsing activity, and gaining other valuable insights. Your browser isolation system should offer a variety of interesting built-in reports, as well as allow you to create customized reports that meet your needs.

Browser isolation in the security ecosystem

Browser isolation systems can replace other browser protection technologies to provide the most effective approach to browser malware protection. The use of this technology also renders web access control systems unnecessary.

The majority of untrusted file downloads happen through the web browser and email attachments. By centralizing control of the web browser, isolation systems can restore centralized control of this function to the IT organization. Thus, if the company uses web-based email or an email system with download controls, security teams may not need to implement endpoint-based download controls.

Downloading any file from a third-party resource involves some level of risk. By restoring centralized IT control of that decision, organizations can determine their own risk tolerance and set up appropriate policies for permissions, file types, and scanning tools.

Likewise, a browser isolation system also prevents employees from leaking sensitive files outside the organization. Again, IT can centralize control and policies related to this process to further strengthen their data loss prevention strategy.

Together, these reporting capabilities provide you with the tactical and strategic information you need to manage your organization's information security program.

System performance management

Security operations teams use the browser isolation system's reporting capabilities to manage system performance. This includes the identification of necessary upgrades if usage begins to increase beyond the capabilities of existing hardware.

Administrators must also ensure that when a new user joins the organization, the account provisioning process automatically informs the browser isolation system of the new employee.

Centralized management and control

Large enterprises require scalable security tools. If you're responsible for managing security across a number of geographically distant sites, the browser isolation console should allow you to manage them all seamlessly.

Need to make a change to a security policy? You should be able to log in to the centralized console, design the policy, and automatically deploy it across the entire organization with a single click.

Although centralized management is important, it also requires the ability to customize configurations where necessary. The system should facilitate easily updating policies across the enterprise and allow you to take granular control of the system where necessary.

For example, an organization may set a policy that prohibits all users from uploading files to the web. Members of the human resources (HR) benefits group, however, may need an exception to this policy to upload information to a website run by an insurance company. The management tool should allow you to easily create the enterprise-wide policy and then efficiently make an exception to that policy where business needs dictate.

Chapter 5

Seven Questions to Consider When Selecting a Malware Isolation Solution

In This Chapter

- Identifying the best architecture in a malware prevention solution
- Considering the cost and complexity of malware prevention solutions
- Understanding how malware prevention solutions must scale to cover multisite deployments

Selecting a malware prevention solution is an extremely important decision for an enterprise information security program. Here are seven important questions you should ask to help you select the product that will best protect your organization against the evolving malware threat:

- **Will the system prevent all browser malware from entering the network?** An effective isolation system will ensure that all browser malware remains safely outside the network, with no ability to escape the appliance or find a path into the network. For that reason, it's important that connections to the appliance are encrypted and secure, and that all web content is completely transformed before delivering to end-users over secure channels.

- **Will the system add more complexity to the security architecture?** When isolation technology is deployed on each individual endpoint device, it can add a significant complexity and management burden for IT organizations (especially in large-scale deployments). However, when isolation technology is deployed in one location — on an appliance outside the network — there is essentially one point of configuration, control, management, and maintenance. This greatly minimizes any potential complexity. It may actually reduce complexity by minimizing the need for other less effective products (AV, URL filtering, whitelisting, and so on).
- **Will the system save any money for my IT organization?** It should! By stopping web malware, you stop successful breaches, which means you save money by avoiding the time and cost required with lengthy forensics, remediation, and business disruption. According to a 2015 report from Ponemon Institute, organizations spend an average of $3.2 million on every breach resulting from failed malware detection. Effective browser isolation can help keep that money in your pocket.
- **Will browser isolation impact employees' browsing experience?** When deploying isolation outside the network, the virtual browsing function is launched on internal endpoint devices as usual. This can be done via a dedicated client viewer or through integration with an existing desktop browser. In either case, employees are empowered with normal browser features, plus the ability to leverage the full power of the web without fear of any malware attack.
- **How can a browser isolation system help reduce the risks of browser file downloads?** In a typical enterprise network, employees have direct access to web content and often have complete freedom to download any file from any location. Potentially malicious files pose a second security risk in addition to browser malware. With a browser isolation system, IT can regain control of all file download requests, and establish appropriate files, tools, and processes to minimize the risk of allowing unapproved and potentially malicious content into their network.

- **How can a browser isolation system handle potentially malicious SSL traffic?** In a typical enterprise, IT organizations are reluctant to decrypt and inspect SSL traffic for fear of violating employee privacy. Unfortunately, cyber criminals know this and increasingly use encrypted SSL tunnels to carry targeted malware. So, what's the solution? With browser isolation, all traffic — including encrypted SSL traffic — is terminated on the appliance outside the network. There is no need to inspect it because all traffic is transformed into a benign format and delivered over a secure, proprietary channel to internal endpoint devices.
- **Can a browser isolation system scale and adapt to the needs of my business?** Browser isolation appliances are designed to scale linearly — simply add more capacity and more locations as your needs evolve. In addition, because the system supports a cloud-based delivery model, remote and roaming users can enjoy the same level of malware protection as if they were working on premise.

READY TO
ELIMINATE
ALL BROWSER-BORNE
MALWARE
IN YOUR
ORGANIZATION?

Spikes Security can help you eliminate the primary attack vector used by cyber criminals. When it's convenient for you, we are happy to schedule a demo or arrange for a 30-day on-site trial of our browser isolation system.

To learn more visit www.spikes.com

SPIKES SECURITY

Protect your organization from all browser-borne malware with browser isolation technology

Web browsers are a primary vector for malware attacks that jeopardize network security. These attacks threaten the confidentiality, integrity, and availability of sensitive information. Browser isolation technology mitigates the risk of malware infection by separating the browser from the user and creating a safe browsing environment.

- ***Understand the limits of detection technologies* — *learn how traditional defense-in-depth security architectures, based on various detection technologies, are becoming increasingly ineffective.***
- ***Identify how browser isolation reduces risk* — *See how browser isolation technology separates the user from the browser, preventing malware from entering your network and infecting endpoint devices.***
- ***Create a browser isolation deployment plan* — *Every organization has unique web communication requirements. Discover use cases where browser isolation can secure your business.***

Open the book and find:

- **Clear descriptions of browser isolation technology**
- **Discussion of where existing malware controls fall short**
- **Use cases describing typical browser isolation deployment scenarios**
- **Best practices for deploying browser isolation technology**
- **Management practices to maintain your deployment**

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

Mike Chapple, PhD, is Senior Director for IT Service Delivery at the University of Notre Dame. He is the author of 20 books, including the *CISSP Study Guide*. Follow him on Twitter at @mchapple.

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-09881-2
Not for resale