Avecto eBook

C-level guide to defense in depth

Chapter 1: Your relationship with risk

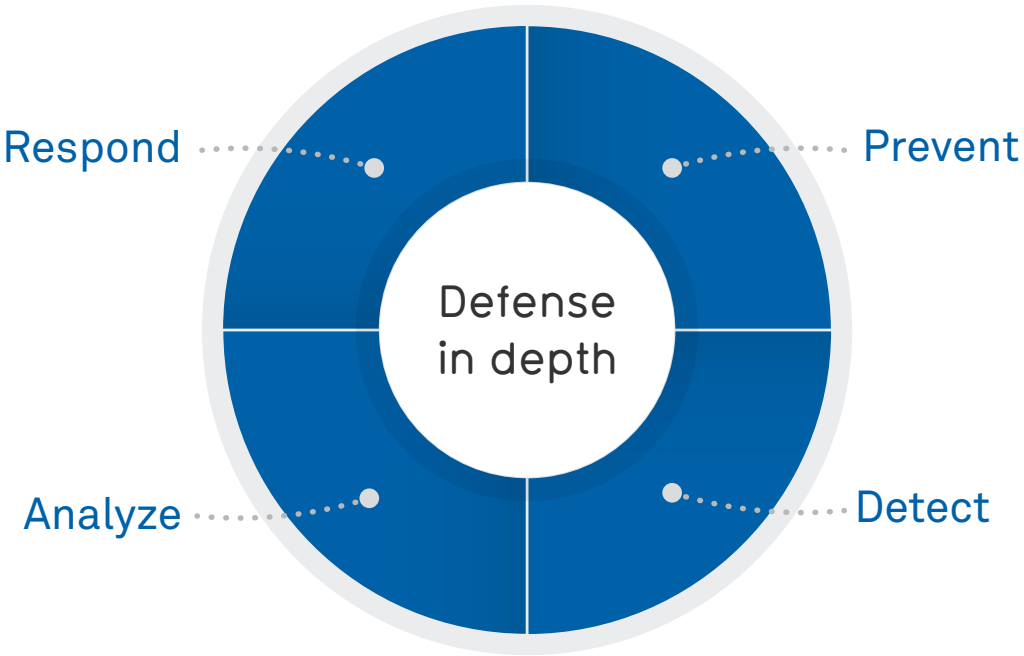
Russell Smith, Windows Security Expert

Contents

Synopsis

In chapter 1 of this ebook, you will learn about the concept of proactive defense in depth and why it is the most effective approach to combat today's advanced threats.

Russell Smith will explore the pros and cons of popular security strategies and make the case that a proactive approach is essential and easily achievable with the right tools in place. With antivirus technologies catching less than half of threats, learn which security strategies should be top of your priority list, providing the least risk with the most gain.



About the author

Russell Smith

Russell Smith specializes in the management and security of Microsoft-based IT systems, with more than 14 years of experience in IT. He has written a book on Windows security, co-authored one for Microsoft's Official Academic Course (MOAC) series, and was a regular contributor at Windows IT Professional magazine. Russell is also a Contributing Editor at the Petri IT Knowledgebase, blogs for Netwrix, and is an instructor at Pluralsight.

Your relationship with risk

> “Infrastructure downtime can cost a business $5,600 a minute on average.”
>
> Gartner

All of us have experienced technical problems with computers at work, sometimes serious enough to result in loss of work and downtime; or performance and operational issues that at best lead to frustration on our part because of the effect on productivity, or otherwise require intervention by IT.

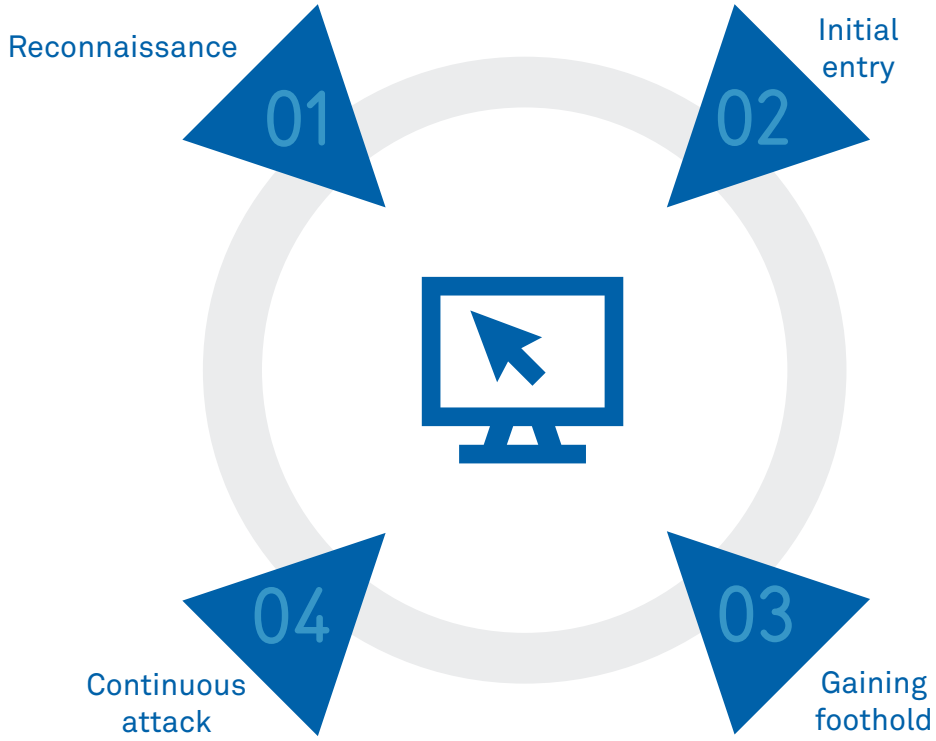
Worst case scenarios lead to complete loss of service for extended periods, or data loss resulting in time-consuming restore operations from backup, reputational damage, and fines from regulatory or governmental bodies. However many organizations accept these risks as part and parcel of utilizing technology, and have a limited reactive strategy to deal with minor and serious incidents.

But it doesn’t have to be like that. Following basic security best practices can go a long way, not only mitigating many of the threats that lead to data loss, leakage or service interruptions, but also preventing the performance and operational issues that users experience daily.

In today's landscape of Advanced Persistent Threats (APTs) and increased technological complexity, using desktop antivirus solutions alone is a low cost but high risk strategy, as signature-based malware detection becomes less effective.

Endpoints without additional defense in depth security protection are left exposed to the performance, operational and business risks described above, and are more likely to be hit by malware. Whatever the impact, there is a cost involved.

Behaviour of an Advanced Persistent Threat



01 Reconnaissance
Gathering information, email addresses, domains, vulnerabilities

02 Initial entry
Weaknesses are exploited and network code is executed. This could be via man-in-the-middle attacks, email phishing, social engineering

03 Gaining foothold
Following initial penetration, hackers look to maximize their hold on the network by seeking privileged accounts to acquire more rights and deep network access

04 Continuous attack
With a presence inside the network the attacker can continue to gather and exploit data, which may continue over weeks, months or years

The psychology of security

Nobody likes being presented with another password to remember, a new security procedure that slows us down or prevents us from moving forward with a task. But on the other hand, we'd all prefer that the technology we use just worked, and that can be evidenced in the popularity of smartphones and tablets, where unless jailbroken by the user, privileged access is never granted and the computing experience is curated through an app store.

Smartphone and tablet operating systems are generally designed from the ground up to balance security and usability in a way that is acceptable to users, while ensuring the OS and data it processes stays protected, with extra controls available to further secure devices if required. But Windows has a different history, and partly what made it so successful is that it was engineered for usability first, in an era where most of us didn't have Internet access.

Despite its history, Windows today provides a relatively secure experience, and stands up well against other desktop OSes, such as Redhat Linux or Ubuntu, which have traditionally been seen as mainstays of security, even if you needed to be a robot to use them. Every new version of Windows is a more secure platform, and the free upgrade to Windows 10 for Windows 7 users is something organizations should consider from a security point-of-view alone.

Open Windows

IT departments often shy away from following security best practices in Windows, partly because traditionally it has been difficult to use and manage unless left completely open. Removing privileges from Windows users is a more realistic proposition in Windows 7, where granting employees standard user accounts should be sufficient for performing most daily work-related tasks. Microsoft also provides a way for consumers to elevate privileges via User Account Control (UAC), which might always be a requirement for tapping into the deep recesses of the operating system to utilize its full potential. However UAC has been criticized for its lack of flexibility and customization, which often leads to a poor user experience.

The politics of Privilege Management

As working with standard user privileges hasn't traditionally been the norm in most organizations, the cultural shift to using restricted privileges isn't just a technical issue, but also political. Some employees see it as a matter of status that they should be given free reign over their desktop, and others may demand it on genuine or bogus technical grounds. Often it becomes easier for IT to grant users their wishes, and deal with the technical fallout later, even if that means putting the company's IT systems at much greater risk. After all, it only takes one compromised machine to bring down an entire network like dominoes, and another fact employees regularly fail to apprehend is that devices are interconnected.

It is also important not to forget that even if an organization is not considered to be at particular risk from hackers, attacks are often opportunistic and almost always automated. Little effort is required to distribute exploits far and wide, with exploits indiscriminately targeting devices to see what information or weak points exist to gain entry.

Security strategies

Neither Windows, Apple OS X nor Ubuntu desktop operating systems provide the security and user experience of Windows Phone or iOS out-of-the-box. The more proactive tablet/smartphone security model has proven to be an effective approach that doesn't impact usability, which is in stark contrast to the reactive line that many organizations take with desktop security.

But gone are the days where antivirus and endpoint firewalls provided enough protection to deliver an acceptably low level of risk, as antivirus by itself is only capable of blocking around fifty percent of threats. APTs have increased in sophistication and number, being more difficult to detect and harder to eradicate than traditional viruses.

Multi-layered security strategy

A comprehensive defense in depth security strategy is known to be effective, and this can be evidenced in Microsoft's approach to security in Windows. Privilege Management in the form of User Account Control (UAC) has significantly reduced malware infection rates for consumers, as shown in Microsoft's quarterly Security Intelligence Report; along with other mechanisms such as the

SmartScreen filter, which uses application reputation to determine if downloaded executables are trustworthy, and Protected View in Office 2013, which disables editing and interactive features until the user explicitly enables them, for content originating from the Internet. Finally, Windows Store apps in Windows 8 are sandboxed to a limited extent, a feature that doesn't apply to desktop programs out-of-the-box.

Implementing the following three pillars of defense in depth security together provides the best investment to risk reduction ratio, and is substantially more effective than using antivirus alone. And even though there's no panacea in computer security, the three complimentary pillars of defense in depth security provide a significant level of damage limitation should your systems be successfully infiltrated.

> "88% of insider threat actions can be attributed to privilege abuse."
>
> Verizon

Privilege Management

The principle of least privilege, a security best practice where users are granted only the permissions required to perform the task at hand, is key in establishing a secure baseline for all Windows systems. Not only that, but it is also a requirement to meet IT regulatory compliance standards.

Privilege Management is a critical component of any proactive security strategy, protecting important system configuration from malicious processes, and intentional or accidental changes users might make that can have a negative impact on performance, increase the attack surface and cause operational issues that require support from the helpdesk.

Privilege Management technologies provide the additional flexibility that is often lacking in Windows alone, empowering users to run effectively with a standard user account, no matter what their role requirements.

> “57% of workers install personal software on corporate machines.”
>
> Microsoft

Application Control

Ensuring that users are only able to execute trusted code is also paramount. Removing administrative privileges from users doesn’t in any way guarantee that they are not able to install applications, drivers or run scripts not approved by IT, as many applications can still run or execute with standard user rights.

Without a set of policies designed to restrict what can be executed, not only can users decide what applications can be trusted, but malicious processes running under the context of a user’s login

account can execute without detection.
While app stores provide a certain amount of additional security, as applications are vetted before users can install them, in theory considerably reducing the risk of malicious activity, Application Control provides organizations with ultimate control over the approved desktop programs and Windows Store apps that users can install and run.

> “More than 15 million new suspect URLs were discovered in Q4 2014.”
>
> McAfee

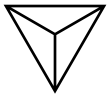
Sandboxing

Even the applications we trust can suffer from zero-day exploits, previously unknown security vulnerabilities that are used by hackers. Application sandboxing until recently has relied on complex virtualization technologies, meaning that it hasn’t always been practical to implement due to the technical requirements and interruptions to users’ workflow.

However, recent developments in these technologies have changed the game. Defendpoint from Avecto provides a sandboxing solution that uses Windows built-in NTFS access controls, a tried and trusted technology of some twenty years, with low overhead and a workflow that integrates naturally into the user’s computing experience.

Defendpoint treats content as untrusted so that it cannot interact with other processes and data unless the user explicitly allows it, providing an important additional layer of protection against vulnerabilities in trusted applications.

Defendpoint



While it may seem complicated to implement the three measures above to achieve a robust defense in depth security solution, Defendpoint deploys a single agent to clients, and uses policy-based configuration on the backend that can be managed using Windows Active Directory or McAfee ePolicy Orchestrator.

Unlike the free and in-built privilege management and application control tools from Microsoft, Defendpoint helps administrators quickly create policy baselines by auditing privilege use, and out-of-the-box templates for common configuration scenarios, taking out much of the guess work that might otherwise make deploying security defenses a process of trial and error.

Improving performance, operational reliability and security is a choice. While many organizations struggle to manage the day-to-day issues of supporting IT systems because of their reactive strategies, another path is available where a complete proactive security strategy not only diminishes the risk of major malware outbreaks, but also reduces the workload of the IT helpdesk and improves employee productivity, leaving staff to get on with the business of doing business.

Summary

The temptation exists for IT and security professionals to deploy the easiest and most familiar technologies first. Yet in the modern age of cyber threats, this is not the most effective use of resources and businesses should invest in those measures known to provide the most control against the riskiest threat vectors.

Achieving effective defense in depth relies on prioritizing key strategies such as patching, Privilege Management, Application Control and Sandboxing. This greatly reduces risk, both externally and internally, and reduces the potential for privilege escalation if an account is compromised.

About Avecto

Avecto is a global software company specializing in endpoint security. Its revolutionary Defendpoint software offers proactive protection against advanced threats. Uniquely combining the technologies of Privilege Management, Application Control and Sandboxing in an integrated suite, you achieve security strength and depth without compromising user experience. This mantra of security + freedom underpins Avecto's philosophy to unite IT departments and their end users.

Avecto's experience is proven, with implementations of over 5 million endpoints at many of the world's most recognizable brands. Established in 2008, Avecto is headquartered in Manchester (UK) with offices in Boston, (US) and Melbourne, (Australia).

Contact

Avecto
@avecto
+Avecto

avecto.com
info@avecto.com

UK

Hobart House
Cheadle Royal Business Park, Cheadle, Cheshire, SK8 3SR

Phone
+44 (0)845 519 0114
Fax
+44 (0)845 519 0115

Americas

125 Cambridge Park Drive
Suite 301, Cambridge, MA 02140
USA

Phone
978-703-4169
Fax
978 910 0448

Australia

Level 8
350 Collins Street, Melbourne, Victoria 3000, Australia

Phone
+613 8605 4822
Fax
+613 8601 1180