5 RISK POINTS TO AVOID IN ENTERPRISE SECURITY

CRASH COURSE

Microsoft

CONTENTS

ADVANCED SECURITY:

WHEN WALLS ARE PENETRABLE.

While many SecOps professionals focus on keeping cyberthreats at bay with breach-prevention, threats to security are constantly evolving around us. Nearly 80% of organizations reported data breaches in 2016, with a third of those reporting more than six breaches.[1] Of that same group, less than one-third anticipated an attack. This optimism doesn't reflect the facts. More and more, attackers are using new tactics to circumvent pre-breach security measures. In fact, one report found that 60% of attacks didn't use malware at all.[2] They now exploit a combination of weaknesses to infiltrate and hide inside operating systems striking from within. And it's working: the average attack in 2016 gave hackers 146 days to act within victims' systems.[3]

In this five-section course, we'll look at what else can be done to stay in front of the evolving threat landscape.

[1] 2017 CyberEdge Cyberthreat Defense Report. Link: https://cyber-edge.com/cdr/

[2] Verizon 2016 Data Breach Investigations Report. Link: http://www.verizonenterprise.com/resources/infographics/ig_understanding-the-real-risk-of-data-breach_en_xg.pdf

[3] Mandiant. The Threat Landscape by The Numbers. Link: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Infographic-mtrends2016.pdf

PRE-BREACH

SHIFTING THREATS. AGILE DEFENSES.

Brute-force malware attacks are still a threat, but the thrust of attacks is shifting to more sophisticated means of entry. Attackers have discovered they can simply go around enterprise anti-malware measures by not using malware at all. In fact, up to 60% of recorded cases have been able to use legitimate operating system (OS) management and pen-testing tools after gaining access through social engineering methods, fooling users into to letting them in with privileges.[4] Once in, they could easily design and insert their zero-days (0-day). Now, looking legitimate, they could breach the network undetected. While effective firewalls continue to be essential, the enemy is also attacking on thousands of fronts, gaining access to systems through hundreds of different devices. From laptops and smartphones to tablets and smart objects—those in addition to social engineering assaults on your vital—and vulnerable—human assets. SecOps need more than improved anti-virus measures. They need next gen approaches such as anti-exploit technology and application control. Siege mentality no longer works. Protecting an enterprise on all those fronts requires more than new tools; it requires new thinking.

[4] Windows Security Center Report: Post Breach: Dealing with Advanced Threats

Risk Point 1
Device Security: Mobile Entrypoints

Mobility in the workplace is a critical factor to employee **creativity, value, productivity and satisfaction**. But a mobile, or BYOD environment comes at additional risk. Malicious apps like **Gooligan** and SnapPea get in through third party apps and allow bad actors to access critical information on mobile devices. Even at the highest levels of government and business, people are fallible. 87% of senior managers admit to regularly uploading work files to a personal email or cloud account.[5] We won't escape from these facts; but by integrating new defenses we can be smart about how we manage them, without over-reliance on end users.

SOLUTIONS

While many enterprises attempt to reduce threats with add-on products, Windows 10 streamlines and integrates these requirements by building them in rather than bolting them on, providing easier management and better coordination:

- **Maintain and verify system integrity:** Trusted Boot ensures devices boot using only software that is known and trusted.
- **Ensure secure app sources:** Device Guard blocks everything but trusted apps and sources.
- **Provide defense at the desktop level:** Windows Defender Antivirus gives you built-in antimalware solution for security and antimalware management for desktops, portable computers, and servers.
- **Automatically separate personal from business data:** Windows 10 includes Windows Information Protection, which separates critical data without changing the work environment or other apps or negatively impacting the user experience.
- **Secure lost or stolen devices:** Bitlocker provides easily provisioned, enterprise grade management, encryption and protection.

[5] Stoz Frieberg, "On The Pulse: Information Security in American Business," 2013

Risk Point 2
User Identities:
The people problem

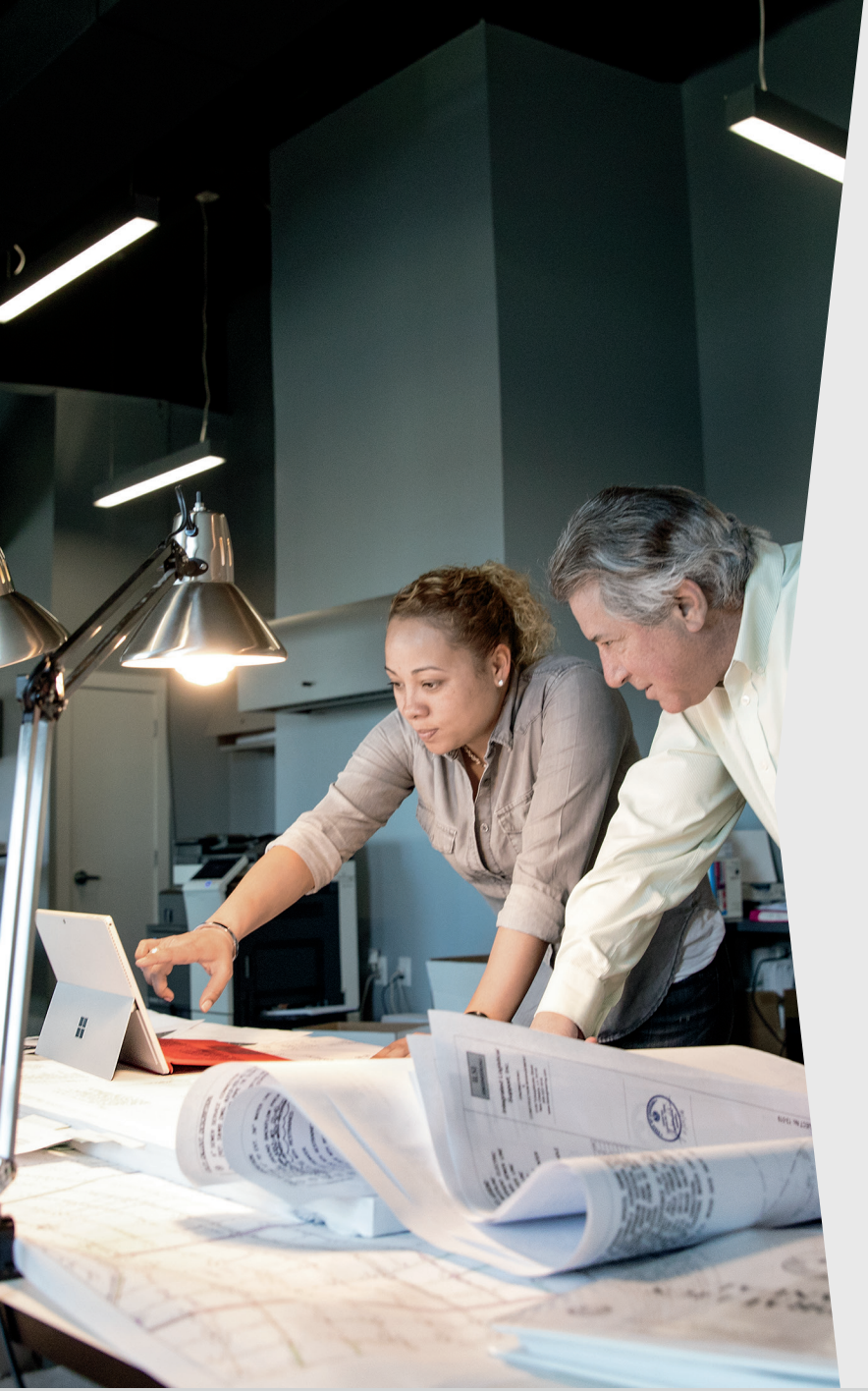
Securing machines is difficult enough. Securing the user identities that access them can be just as hard. Passwords are a weak point. With 75% of individuals using only three or four passwords across all their accounts, security risks can be huge. And beyond simple password security, the underlying tokens we use after we authenticate and use for single sign-in (e.g: NTLM) can be stolen and used instead of our passwords and other multi-factor authentication solutions to impersonate the user. These approaches leave your assets open to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket.

SOLUTIONS

- **Reduce reliance on user-generated passwords:** Windows Hello, included in Windows 10, gives you enterprise-grade security based on fingerprint, facial or iris recognition. It provides a multi factor password alternative that works on any device using a PIN or biometric options.

- **Protect identities from full system compromise:** Credential Guard provides hardware-based virtualization to isolate and protect NTLM and Kerberos credentials. This prevents malware running in the operating system with administrative privileges from extracting protected secrets.

[6] Security Week. Link: http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email



POST-BREACH

THREATS FROM THE INSIDE

While pre-breach defenses continue to be essential, they can be defeated; and they are being defeating more often. Once attackers gain access and are inside the system, the security situation changes. They are carrying out malicious actions more at will—performing reconnaissance, hiding and moving across the network to locate high-value assets, and executing information extraction. This is a huge concern with 82% of C-level IT executives voicing the need for better end-point analytics to identify and chase down these threats. This kind of threat calls for Windows Defender Advanced Threat Protection (ATP), capable of monitoring security events on the endpoint, using large scale correlation and anomaly detection algorithms to pinpoint evidence of attacks while they happen—and alarm you before they do more damage. Another focus of Windows Defender ATP is to report on built-in pre-breach threat protection technologies and revealing the signals missed before the attackers got inside.

Risk Point 3
Behavior-Based detection: Seeing the invisible

The first challenge in any post-breach scenario is distinguishing the legitimate actions of your authorized users from those that could be malicious. If the attackers are smart (and the dangerous ones are) they will disguise their actions well as normal movement and storage of data, and it would seem impossible to find them. That 146 days average attack duration we talked about above bears this out. So how do you see the invisible?

SOLUTIONS

Windows 10 provides enterprises with **advanced attack detection.** The functions built into the platform—not bolted on—mitigate the risks of attack while increasing ease of operation:

- **Maximize on strong security analytics:** To identify anomalies and threats from a wide variety of sources, Windows Defender ATP uses advanced behavioral analytics and Machine Learning to alert you on attacks and zero days.
- **Leverage the largest data sets:** Windows Defender Advanced Threat Protection (ATP) uses the Microsoft Security Intelligence Graph to combine signals from our email, communications, browser and malware protection, identity protection, web search services, and our operating system - above and beyond what others can offer. Using these signals, Windows Defender ATP applies state of the art machine learning and analytics to power high quality detection and investigation capabilities.

Risk Point 4
Security management: Controlling the situation

Even if SecOps have an effective post-breach detection system, setting up a manageable, coordinated defense without having to expend too many valuable resources is enormously complex. Ongoing security will require that you maintain a record of attacker footprints and actions across the network, create and maintain a database risk sources. Detected alterations in your systems will then require quick adjustments to your policies. And these are just the beginning. Controlled response is key.

SOLUTIONS

The Windows 10 portal gives SecOps tools and capabilities for **Investigation and Response** to threats on their endpoints throughout the enterprise, without unduly tying up resources:

- **Single pane of glass for windows security:** Explore 6 months of rich machine timeline that unifies security events from Windows Defender ATP, Windows Defender Antivirus and Device Guard.
- **Customize policies on the fly:** Windows 10 also enables efficient alteration of policies based on the changing threat environment such as additional or upgraded hardware.
- **Apply activity filters:** IT can look for the location of a user, device type, IP address or if someone is granted admin rights to identify suspicious logins and behaviors.
- **Create custom alerts:** IT can be immediately notified of events by email or simply looking at their console.
- **Capitalize on extensive investigative resources:** Windows 10 allows SecOps to perform forensics on specific machines, get a detailed file footprint across your organization, or submit a file for deep analysis.

Risk Point 5
Advanced information: Staying ahead of threats

Heartbleed. Strontium. Wannacry. No one knows how the next generation of attackers will exploit kinks in enterprise defenses. Forrester predicts that during this year "we will see a Fortune 1000 company disappear — through bankruptcy, acquisition, or regulatory enforcement — because of a cyberattack."[7] The enterprises less likely to suffer that fate will be those that identify new threat trends and how those trends are likely to collide with their own vulnerabilities. This requires good intelligence on emerging and possible threats.

SOLUTIONS

Threat Intelligence will be a major determinant of winners and losers in the battle against cyberattack. Windows 10 gives enterprise access to resources to help stay informed of the latest threats.

- **Access internal and external reports:** Windows Defender Advanced Threat Protection provides your enterprise with reports and indicators for known attackers and prominent attacks that could be risks.
- **Find out if threats have been validated by security black belts and third party feeds:** With these additional resources, Windows 10 facilitates access to a wider base of expertise on evolving dangers.
- **Focus on the right threats:** Within Windows Advanced Threat Protection, you can upload your own threat intelligence, then define alerts unique to your environment based on your definitions.

[7] Forrester Report—Predictions 2017: Cybersecurity Risks Intensify. By Amy DeMartine, Jeff Pollard, Joseph Blankenship, Andras Cser, Heidi Shey, Christopher McClean. November 1, 2016. Link: https://www.forrester.com/report/Predictions+2017+Cybersecurity+Risks+Intensify/-/E-RES127867

SECURITY ASSESSMENT

IDENTIFY YOUR INITIAL LEVEL OF RISK

Of course, your entire enterprise security profile can't be established in these six questions. But they can tell you if you need to look deeper. The answers to the questions below will help you shine a light on opportunities to improve your security with Windows Defender Advanced Threat Protection (ATP). If you answer yes to any of them, register for the free trial.

1. Is your enterprise fostering a mobile or BYOD culture?
2. Do you still rely on password user authentication alone?
3. Do you have a behavioral-based detection solution in place to identify possible post-breach risks?
4. Does your SecOps resource have agile security and detection policies that can respond quickly to new threats?
5. Do you have a dedicated resource for the identification of emerging cyberthreats?
6. Is your current security solution built in to your OS for both mobile and desktop devices?

If you answered "yes" to any of these questions, consider Windows Defender ATP.

Register for the Windows Defender ATP trial now

Go to https://www.microsoft.com/en-us/windowsforbusiness/windows-atp