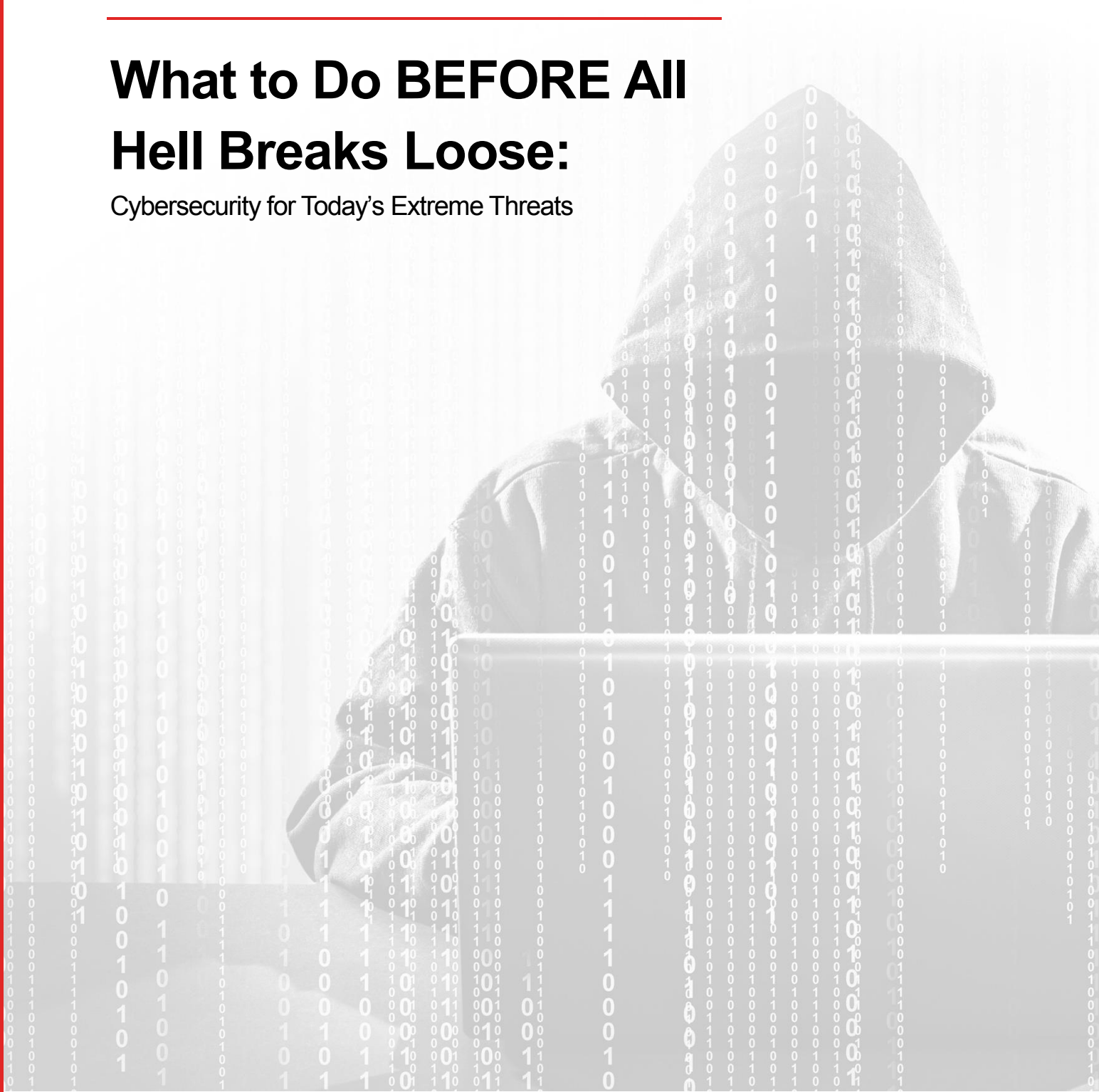
ivanti

What to Do BEFORE All Hell Breaks Loose:

Cybersecurity for Today's Extreme Threats



Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

©2017, Ivanti. All rights reserved. IVI-2028 04/18 AB/BB/DH

Introduction

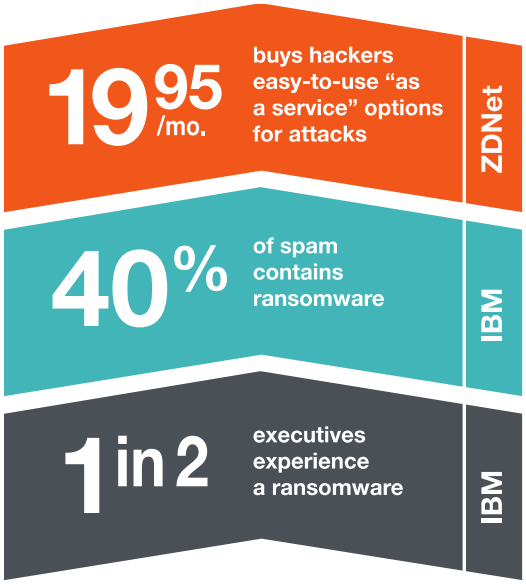
In the U.S. alone there were more than 500 publicly disclosed data breaches in 2016—nearly twice that of the year before.[1] In February 2017, research firm Opinium found that 78 percent of the IT decision makers surveyed across the U.S. and Europe experienced at least one ransomware attack on their organization in the last year. The Shadow Brokers, the hacking group that exposed the vulnerability the now infamous WannaCry exploited, has promised to disclose more of the same. The world has now seen its first publicly disclosed million-dollar ransom payout.[2] NotPetya gave us a taste of the weaponized malware of the future. And then there's Equifax….

How do you stop this freight train? Without a focused security strategy, device sprawl is costly—and out of control. IT teams spend too much time managing these devices. Add to this a major cybersecurity labor shortage that forces companies to optimize their security personnel, and clearly a strategy leveraging tech that's comprehensive, simplifies management, and focuses on security basics that raise the highest barriers against real-world attacks offers a strong advantage over other solutions.

When 93 percent of data breaches compromise organizations in minutes or less,[3] you simply can't afford to make the wrong call when it comes to securing your organization.

Your Security Risk Is Greater Than Ever

All top cybersecurity threats are on the rise.[4] No great surprise there, right? But why, exactly, is this the case?



We won't go down that rabbit hole completely in this paper. Suffice to say, the uptick is in no small part due to how much easier it is to take up the mantle of cyber attacker. Today's exploit kits, for example, simplify cyber attacks for even inexperienced hackers. These malicious toolkits come with pre-written exploit code and require no knowledge of how it works. Often a simple web interface allows licensed users to log in and view active victims and statistics. These kits may even include a support period and updates, much like legal commercial software.

In the same vein, it also has to do with the widespread availability today of sophisticated tools originally intended for cyber espionage and cyber warfare.

Ransomware, for example, has evolved from a simple scary hack to enterprise-grade malware built on stolen U.S. National Security Agency (NSA) tools that holds computers hostage and locks down entire systems. Combine that with the fact that nearly 40 percent of all spam sent in 2016 contained ransomware,[5] and it's clear that at any point an unsuspecting user may click on something they shouldn't and compromise the organization.

IBM X-Force found that one in two executives have experienced a ransomware attack at work. That's potentially half the executives in your organization.[6]

The User: Always Your Weakest Link

The Verizon Data Breach Investigations Report (DBIR) is one of the most respected annual reports in the security industry. Every year, the Verizon Research, Investigations, Solutions and Knowledge (RISK) team, one of the largest IT investigative entities in the world, shares deep insights into the state of cybersecurity for the year, including the largest trends.

In 2017, the team found phishing is used in more than 90 percent of security incidents and breaches.[7]

And at equally alarming rates, users with their many devices are falling victim to ransomware and other malware via these user-targeted attacks. According to Verizon, 30 percent of phishing messages were opened in 2016—up from 23 percent the year before—and in 12 percent of those events users clicked to open the malicious attachment or link.[8]

The Verizon 2016 DBIR highlights the rise of a three-pronged phishing attack:

- The user receives a phishing email with a malicious attachment or a link pointing to a malicious website.
- The user downloads malware, which attackers can use to look for secrets and internal information, steal credentials to multiple applications through key logging, or encrypt files for ransom.
- Attackers can also use stolen credentials for further attacks: for example, to log into third-party websites like banking or retail sites.

So, What's the Cost of Modern Cyber Attacks, Really?

According to FBI estimates, criminals collected $209 million in revenue in the first quarter of 2016, with the number expected to have exceeded USD1 billion by year end.[9] Since then, it's only gotten worse. In fact, the world just saw its first million-dollar ransom payout.[10]

But malware today—even ransomware—is about so much more than making money.

In fact, while WannaCry was far less successful at raking in the money (it was at about US$135,000 as of June 28, 2017), it was a huge success in terms of how widespread it was: within a day it had infected more than 230,000 computers in more than 150 countries. And the cost to organizations goes well beyond the ransom payouts that in no way brought them to their knees. There is no guarantee paying the ransom will work and recover lost data; and, regardless, the real damages extend to downtime, damaged data, lost productivity and post-attack disruption to the normal course of business, forensic investigation, and restoration of data and systems—not to mention the huge hit your business's reputation would take with your customers, partners, and the supply chain, or the possibility of fines if you're found to be lax with compliance.

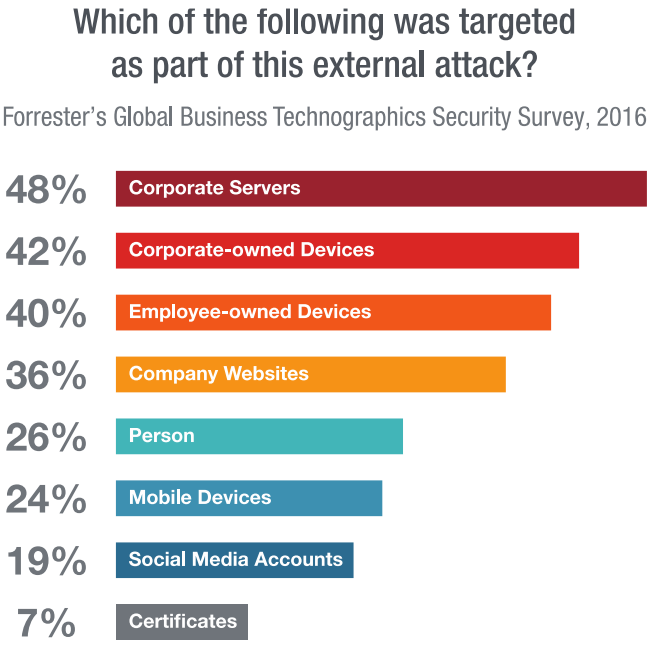
FedEx, pharmaceutical company Merck, and shipping giant Maersk are great examples of this. Each was hit by NotPetya this year, and each has admitted continuing to dig out from under these attacks weeks and even months after they took place. FedEx expected systems to be fully restored at the end of September, three months after the attack, at a cost of USD 300 million.[11] Maersk came up with the same number,[12] and Merck weighed in at USD 200–300 million.[13]

Focus on Your Clients and Servers

So, how is it that even the biggest corporations out there, with what one can only imagine are high-powered security tools in the arsenal, still fall victim to these attacks?

For one thing, many of the tools in place aren't protecting the most vulnerable assets.

For its 2016 Global Business Technographics® Security Survey, Forrester surveyed 192 network security decision-makers whose firms had an external security breach in the past 12 months (1,000+ employees). As part of that survey, they asked respondents which aspects of their infrastructure were targeted in the external attack. The results showed definitively that it's the clients and servers in your network that need to be your primary focus—not the perimeter of your IT environment.



Unfocused Security Strategies? They Lead Only to Expense in Depth

Unfortunately, even if you have the right tools in place to protect against these threats, they're just a few of the many you must configure and manage daily.

Network firewalls, web application firewalls, intrusion prevention systems, vulnerability scanners… oh my! Device sprawl is costly, and IT teams spend too much time managing these devices—time taken away from working with Security to protect against and respond to real threats to the environment.

Patching? Soooo Not a Solved Problem….

Plus, even when you have the right tools in place? They aren't always optimized for success.

Patching, for example, simply isn't a solved problem. WannaCry and NotPetya spread rapidly, using a combination of exploits stolen from the NSA and common weaknesses in Windows software—weaknesses for which there was a patch available.

- **Software is inherently vulnerable.** Hundreds of thousands of lines of code, all written by humans. What could go wrong, right? Nobody writes software that's completely free of errors and immune to potential attackers.
- **The older your software gets, the more vulnerabilities get exposed.** At Ivanti, we like to use spoiled milk as a metaphor for this one. The longer milk is left on the shelf, the older it gets. Eventually? It spoils. Similarly, the longer software is out there in the world, the more its inherent vulnerabilities get uncovered, exposed, and exploited.
- **Legacy software doesn't get patched.** This one isn't a hard-and-fast rule. For example, after WannaCry hit, Microsoft decided to go ahead and release patches for its unsupported operating systems, given the widespread nature of the threat. But by and large, you can't count on updating vulnerable legacy software.
- **Newer software isn't patched properly.** Patches were available for supported Windows operating systems prior to WannaCry, and as noted, for unsupported systems after that attack. Yet, even with all those patches available and the threat of WannaCry so recently passed, organizations still fell victim to NotPetya a month later. Maybe they didn't have the tools in place to patch comprehensively

across the environment. Maybe their limited resources were working as quickly as they could, but just hadn't been able to get the job done in time. Whatever the reason, patches simply being available doesn't mean they're being implemented as they should be.

- **And finally? Not everything can be patched.** Patching won't protect against zero-day exploits. And if you can't patch—because you're running legacy systems, for example, or you have concerns that patching will break something in your environment? You need to block the applications that don't get patched with tools like application whitelisting and privilege management. Regardless of how or where a user accesses their desktop, it's essential they receive only the authorized apps they need to be productive, and can't introduce unauthorized apps that could reduce desktop stability, impact security, breach licensing compliance, lead to user downtime, and increase desktop management costs.

Other Problems We Hear from Our Customers

There's more to the cybersecurity puzzle than this, certainly. But simply put, IT and Security are working so hard, but they're set up for failure.

The patchwork of cybersecurity point solutions they've got in place? It doesn't function well as a whole, and it doesn't provide a complete, integrated view of the risks to the environment. According to the Cisco 2017 Annual Cybersecurity Report, 55 percent of security professionals use at least six security vendors.

That's compounded by the well-publicized cybersecurity resource shortage. Without the talent—or tools—to determine which alerts are critical and why they're occurring, security professionals are often forced to skip the investigation of alerts altogether. In fact, according to the same report, nearly half of alerts go uninvestigated.

Imagine what these uninvestigated threats could do to productivity, customer satisfaction, and trust in your organization.

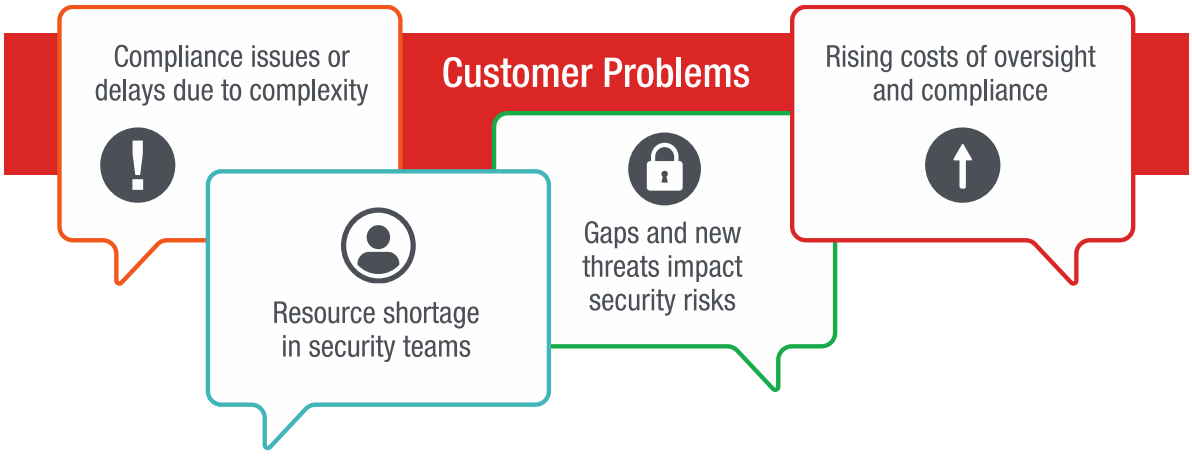
Now consider this: juggling solutions and platforms from many vendors actually creates gaps where attacks can be launched, compounding risk and cost, putting that much more pressure on already overworked teams and IT governance.

The Future? It's Weaponized Malware

Without question, hackers today can have a major impact on critical infrastructure worldwide—hospitals, banking systems, the power grid—especially when they're partnered with aging, vulnerable technology like legacy software. And they appear to be more and more intent on making that happen.

That's a nightmarish scenario. But cyber attacks are growing in sophistication, and evolving in intent—in no small part because sophisticated tools originally intended for cyber espionage and warfare are now readily available to any cyber criminal.

WannaCry ransomware crippled computers at hospitals, banks, and businesses around the world. Hospitals in the UK had to turn patients away while they grappled with computers held hostage. NotPetya affected hospitals too—leading to canceled surgeries—and other major organizations like airlines, banks, the Chernobyl nuclear power plant, and a global shipping company, which was forced to shut down container terminals in ports from Los Angeles to Mumbai.



How can security and IT pros protect their organizations from the perils of these kinds of sophisticated, nefarious attacks that are designed to have such a critical impact?

Focused Security Strategies? They Lead to IT Success

There are many parts to a successful security strategy. The most effective use a layered approach that provides multiple defensive options for any given situation. Get rid of the gaps.

Provide Defense-in-Depth

- ***Discover the full breadth of risk***
- ***Reduce the attack surface***
- ***Detect malicious activity***
- ***Take action to solve problems***
- ***Analyze data for insight into issues***

Simplify and automate security to improve response time

- Provide a complete picture of what is going on in your environment, because you can't protect (or defend against) anything you don't know is out there.
- Reduce the attack surface—prevent malware and exploits from executing to give your security capabilities and team a fighting chance to hunt down threats that make it through.
- Detect malicious activity post-execution.
- Respond to and contain malicious activity and potential vulnerabilities.
- And underscore your efforts with rich data that informs your security posture and compliance.

You also need simpler, streamlined tools that automate security processes. Automation can help remove the burden of detection and investigation from your already swamped resources.

And finally, you should look for threat mitigation that protects and even boosts user productivity. Because users who can't get their work done WILL call the help desk more, and even go around IT with "shadow IT" workarounds, introducing risk into the environment.

Balance Security with User Needs

- ***Learn about users and discover their needs***
- ***Provide security without interfering with jobs***
- ***Silently provide service through upgrades and risk evasion***
- ***Increase productivity with the right tools***

Get from Here to There with the CIS

The best way to make this vision a reality is through a strong security framework. When Security and IT Operations teams work together to promote a focused security solution built on common processes and a prioritized set of actions, costs can go down and responsiveness increase.

Cyber watchdogs like the Center for Internet Security (CIS) agree, and are contributing their knowledge and expertise to identify, validate, promote, and sustain the adoption of cybersecurity best practices. Derived from practices forged from actual experiences at the NSA, the CIS Critical Security Controls both support and reflect many of the other leading sources of cybersecurity guidance.

And their ultimate goal? They're designed to help you rapidly define the starting point for your defenses, direct your scarce resources to actions with an immediate and high-value payoff, and then focus on additional risks unique to your business.

- Prioritized list of actions
- Immediate and high-value payoff
- Comply with regulations
- Based on actual attack experience

Using a proven framework and finding single-vendor solutions that can address the majority of the requirements across your enterprise, then filling in with point solutions where you see specific need, will help you reduce costs while getting the defense-in-depth, effective strategy you desire.

Research and case studies from the CIS show that configuring IT systems in compliance with CIS benchmarks can eliminate 80 to 95 percent of known security vulnerabilities.

Take Security to the Next Level Rapidly with the CSC Top 5

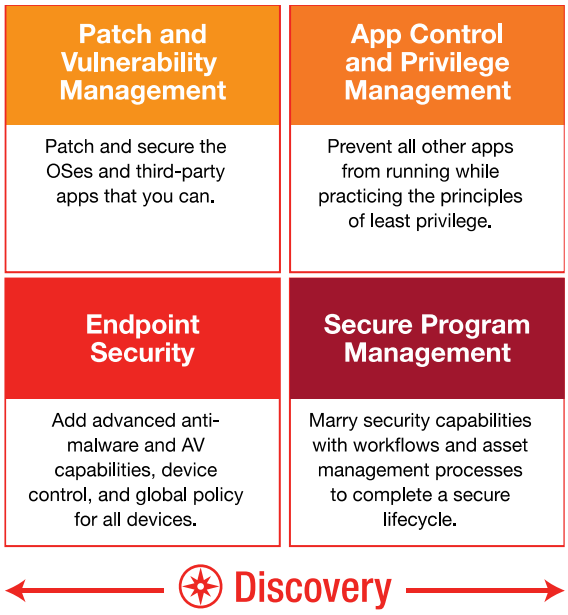
In particular, the Top 5 CIS Critical Security Controls establish a solid foundation for radically improving an organization's security posture. That's why they refer to these as "Foundational Cyber Hygiene."

1. **Inventory and Control of Hardware Assets**
   As per the CIS itself:[14] "Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access."
2. **Inventory and Control of Software Assets**
   As above, but for software: "Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."
3. **Continuous Vulnerability Management**
   "Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers."
4. **Controlled Use of Administrative Privileges**
   "The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise." Provide processes and tools "to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications."
5. **Secure Configuration for Hardware and Software**
   "Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. (As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use—not security.)"

Our Defense-in-Depth Solutions

The takeaway is this: with each business-critical asset in your organization, you should compare your existing security controls against the CIS Critical Security Controls. Pinpoint exactly which sub-controls within those you already meet and those you do not. Then, based on identified gaps and specific business risks and concerns, take immediate steps to implement the Top 5 Controls and develop a strategic plan to implement the others.

We can help. Ivanti provides a comprehensive, targeted portfolio that addresses the Top 5 and other CSC controls, aligning IT Operations and Security to best meet customer cybersecurity needs.



Automated capabilities such as discovery, patch management, application and device control, administrative privilege management, and secure configuration—essential elements of the Top 5 CIS Controls—power Ivanti solutions. What's more, Ivanti helps customers implement those Controls successfully, economically, and easily, with minimal impact on user productivity. Users don't need to call the service desk every five minutes for access rights. Unauthorized, insecure, "shadow IT" workarounds are eliminated. Business still gets done at speed.

We Can Also Help You Know Your Results.

Since you have no real defense without real insight into your environment, Ivanti Xtraction turns reporting into a checkbox, with data on demand and the ability to easily

create new dashboards and reports to get the right data into the hands of executives, directors, and line-of-business (LOB) and application owners.

Pre-built connectors for nearly every tool you use (service desks, monitoring and ITAM toolsets, phone systems, etc.) mean no coding, business intelligence gurus, or spreadsheets—and no data silos. And Xtraction can be customized to connect to even more, so everyone can view their data enterprise-wide in context—cutting through the mass of information to the critical insights that matter—to make smarter, faster decisions with ease.

The Bottom Line

Don't throw good money after bad, or leave your Security and IT teams pulling out their hair as they try to deliver what your organization needs to be protected without the resources and expertise to get it done. Implement a strong cybersecurity program, so you can focus on what matters most to move the needle. Then choose the solutions designed to meet those core security needs and help defend your environment from today's sophisticated, widespread cyber threats.

www.ivanti.com

1.800.982.2130

sales@ivanti.com

1 Privacy Rights Clearinghouse

2 **https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/**

3 Verizon 2016 Data Breach Investigations Report (DBIR)

4 EY's Global Information Security Survey 2016-17

5 2016 IBM X-Force research, **http://www-03.ibm.com/press/us/en/pressrelease/51230.wss**

6 Op. cit.

7 Verizon 2017 DBIR

8 Verizon 2016 DBIR

9 **http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/**

10 **https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/**

11 **https://www.infosecurity-magazine.com/news/fedex-notpetya-cost-us-300-million/**

12 **http://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html**

13 **http://files.shareholder.com/downloads/ABEA-3GG91Y/5005768664x0x954059/3E9E6E5C-7732-4401-8AFE-F37F7104E2F7/Maersk_Interim_Report_Q2_2017.pdf**

14 **https://www.cisecurity.org/controls/**