Multi-Layered Security Made Easy

Cyber attacks are on the rise. We've all heard it, time and again, right? There's a reason for that. In the U.S. alone there were more than 500 publicly disclosed data breaches in 2016—nearly twice that of the year before.[i] 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 on a regular basis, via a "Wine of the Month Club" model. The world has now seen its first publicly disclosed million-dollar ransom payout.[ii] And Petya just gave us a taste of the weaponized malware of the future.

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

It Starts with Patching

The thing is, many existing vulnerabilities already have patches available. There was a patch back in March 2017 for the WannaCry vulnerability for supported Microsoft operating systems (and Microsoft has since released a patch even for legacy OSes). Many existing vulnerabilities like this one remain open primarily because security patches that have long been available were never implemented. In 2015 the Verizon RISK team found that many of those vulnerabilities could be traced to 2007.[iv] And the top 10 known vulnerabilities? They account for 85 percent of successful exploits.[v]

How do you keep track of, remediate, and report on all your vulnerabilities—without breaking the bank or creating headaches for IT? You must be able to research, evaluate, test, and apply patches across the organization with ease. And with the majority of vulnerabilities affecting third-party applications, patching and updating operating systems just isn't enough.

Save time and money and stay focused on supporting core business initiatives. In minutes, Ivanti tools can be up and running to help you discover, assess, and remediate the Windows, macOS, Linux, and UNIX systems across your enterprise—automatically—based on policies you define. Our tools simplify patching across your physical and virtual systems. Find online and offline workstations and servers, scan for missing patches, and deploy them. Then patch everything from the OS and apps to virtual machines (VMs), virtual templates, and even the ESXi hypervisor with the product's deep integration with VMware.

Ivanti also offers a plug-in to Microsoft System Center Configuration Manager that automates and simplifies the process of discovering and deploying your third-party app patches through the SCCM console.

An advanced API stack for our patching solutions integrates with security solutions, vulnerability scanners, configuration management tools like Chef and Puppet, and reporting tools. While making patch operations native to a large ecosystem of security products, this integration also helps you bridge the gap between Security, IT, and DevOps. For example, you can automatically import the latest vulnerability assessment into the next batch of patches to test, helping make IT Operations a more effective partner in securing the organization. For its part, DevOps is all about continuous improvement and automation—and when integrated with patch management can lead to more resilient and consistent infrastructures and systems. And you can pull critical data into solutions like Splunk, Reporting Services, Archer, and Crystal Reports for faster analysis of, response to, and closure rates for critical security incidents.

Block What You Can't Patch

Patching won't protect against zero-day exploits, of course. 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.

It's essential that users receive only the 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.

However, while locking down desktops reduces risk, it also significantly reduces the quality of the end user experience. Users hampered by poor experiences produce less and call the help desk more. Those users can also react to system lockdowns by turning to 'shadow IT' workarounds, creating new security risks.

Ivanti offers leading solutions that help you prevent unauthorized code execution without making IT manage extensive lists manually, and without creating obstacles to user productivity. Trusted Ownership™ automatically prevents the execution of any code, even unknown, that a non-trusted owner (a typical user account, for example) introduces. You can manage user privileges and policy just as easily, at a granular level, while allowing for self-elevation when exceptions occur. We make it simple to give users just the privileges they need to fulfil their roles—no more, no less.

We also extend our support for the SCCM environment to application control. Control applications and end user actions on the endpoint using a centralized console. And use System Center Operations Manager (SCOM) to gather Application Control events and auditing details.

Level Up with Security Management

Ivanti's endpoint security platform combines automated patch management and app control with powerful, integrated endpoint security management—global policy, security diagnostics, remote endpoint control, security dashboards and reporting, and more.

At this level Ivanti can add advanced antivirus and antimalware capabilities to your security solution. We can also provide device control (controlling removable device usage and enforcing encryption on removable devices and hard drives) and advanced protection against fileless attacks (disabling scripts downloaded from the Internet, learning app behavior, allowing only trusted apps to run scripts, and protecting against in-memory attacks, etc.). In addition, you can limit access to authorized networks or IP addresses, and customize firewall configurations for individual systems or groups of systems, including configuring the latest Windows firewalls. And you can detect attempts to encrypt files on the local machine, stop the encryption process, and notify all other computers on the network to blacklist the malware—effectively thwarting the attack.

A convenient single interface lets you easily manage settings and tasks for integrated security components and services. And powerful remote control capabilities mean you can isolate, investigate, and clean endpoints across the network. Take control of machines that are running sluggishly or otherwise present with a security concern. Get real-time information to find a problem's root cause quickly—display information about app reputation, discovery/running time, and other metadata—and remediate from the same console. Plus, integration with systems management tools increases efficiency and control over your IT environment.

Real-Time Dashboard Reporting

Finally, Ivanti can 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.

[i] Privacy Rights Clearinghouse
[ii] https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/
[iii] Verizon 2016 Data Breach Investigations Report (DBIR)
[iv] Verizon 2015 DBIR
[v] Verizon 2016 DBIR