Modernize Your IT Security Now: 10 Reasons Why and 10 Ways How

Let's face it. Your organization is probably not doing all it could be to secure your users and IT resources. You know all about the high-profile hacks and exploited vulnerabilities, and you're of course concerned. But security is not the only thing consuming your organization's limited resources, and besides, you haven't been seriously breached. So far, anyway.

As other companies have learned the hard way, hope is a valuable human trait, but is not a firm foundation for an enterprise security strategy. Fortunately, there are both compelling reasons to focus on improving your enterprise's security, and steps you can begin to take today to do so significantly.

10 Reasons to Modernize Your IT Security Now

1. To minimize risk. More effective, comprehensive, and pervasive security will provide more protection for your users and your enterprise's IT resources. This reduces multiple risks, from the risk of being breached to the risk of failing an audit.

2. To minimize IT and security costs. The 2015 Cost of Data Breach Study, conducted by Ponemon Institute and sponsored by IBM, surveyed more than 1,500 IT, compliance, and information security practitioners at 350 organizations in 11 countries. The study found that the average consolidated total cost of a data breach is $3.8 million, a 23 percent increase since 2013. Further, the cost incurred for each lost or stolen record containing sensitive and confidential information increased six percent from a consolidated average of $145 to $154. Improved security also reduces the time and money required to remediate successfully exploited vulnerabilities, and enables more and better cost-curbing automation.

3. To protect in silence. Modern, truly effective security is pervasive, ubiquitous, and invisible, with little to no impact on user productivity or business operations. The ability to improve security without disruption is essential to user satisfaction and broad adoption of new features and tools.

4. To see more, know more, and protect more. Maximum protection requires maximum visibility into and knowledge about your IT environment and its security posture. Only modern, integrated tools can deliver the visibility and knowledge you need to deliver the best possible security across your environment and enterprise.

5. To increase enterprise agility. Your enterprise must become and remain agile to survive and thrive competitively. Put simply, there is no agility without comprehensive, consistent security.

6. To increase enterprise resilience. A 2013 Ponemon Institute study sponsored by Emerson Network Power found that data center downtime costs approximately $7,900 every minute. A 2014 study conducted by Avaya found that each incident of downtime costs between $140,000 and $540,000, depending on the size and type of enterprise affected. And a 2015 survey by Kaspersky Lab and B2B International found that it can cost from $38,000 to $551,000 dollars to recover from a single cybersecurity breach. Numbers such as these make resilience—your enterprise's ability to minimize planned and unplanned downtime—an absolute necessity.

7. To increase enterprise trustworthiness. Edelman, the world's largest PR firm, surveyed some 33,000 people for its 2015 Trust Barometer. Some 63 percent of respondents said they simply will not do business with those they do not trust, while 80 percent said they only do business with trustworthy people and companies. And without modern, effective security, it is difficult or impossible to assure and demonstrate trustworthiness.

8. To enable user-centered security. Modern, user-centered IT focuses less on devices, files, and tools and more on users. To achieve user-centered IT, your enterprise needs user-centered security—comprehensive, integrated protection of all authorized users, resources, connections, and devices.

9. To operationalize security. Modern security management is less reactive and tactical, and more operationally focused and proactive. At larger enterprises, operations personnel are increasingly performing security-related functions, enabling security specialists to focus more sharply on more complex and strategic issues. And at enterprises large and small, the trend is to move away from reactive "firefighting" and toward continuous delivery of new and improved security measures and more effective, proactive security operations (or "SecOps").

10. To prepare for the future. According to the Verizon 2015 Data Breach Investigations Report, some 70 percent of malware activity a decade ago was accounted for by only seven families or types of malware. By 2014, that 70 percent of malware activity was distributed across 20 different malware types. During this same period, malware has evolved significantly, from email "worms" to "stealthy command-and-control botnet membership, credential theft, and some form of fraud." That same study estimates that five malware events take place every second of every day. Only modern, comprehensive, user-centered security can provide the protection and adaptability your enterprise needs today and will need tomorrow.

10 Ways to Modernize Your IT Security Now

1. Implement consistently timely and comprehensive patching for all of your critical operating systems.

2. Implement consistently timely and comprehensive patching for all of your critical third-party applications.

3. Implement consistently timely and comprehensive patching for all of your critical devices, everywhere on your network, whether local, remote, or mobile.

4. Establish non-intrusive, non-disruptive application whitelisting (and blacklisting where needed).

If you do nothing more than the four steps above, you can make great strides toward improving security and protection at your enterprise.

- According to the Australian Signals Directorate, up to 85 percent of targeted attacks can be prevented by whitelisting, patching of operating systems and third-party applications, and restricting administrative privileges.
- According to the U.S. National Vulnerability Database, 86 percent of reported vulnerabilities come from third-party applications.
- According to the Verizon 2015 Data Breach Investigations Report, 99.9% of the exploited vulnerabilities in 2014 were compromised more than a year after the vulnerability was published.
- A Ponemon Institute/IBM survey of some 200 customers who have been breached found that only 45 percent of those breaches were caused by malicious activities or software. The other 55 percent were caused by operational mistakes, inadvertent errors by legitimate users, or problems with systems.

Now for steps 5 through 10:

5. Automate as much of your proven patch and security management processes as possible. This will maximize the consistency of execution and scalability of those processes.

6. Integrate proactive patch management into and with all of your enterprise's other significant IT initiatives, especially those focused in IT Asset Management (ITAM), IT Operations Management (ITOM), or IT Service Management (ITSM). Comprehensive, effective, user-centered security is essential to the success of such efforts.

7. Engage, educate, and motivate users to understand their criticality to effective security. Your users are your enterprise's first and last lines of defense. Comprehensive, effective, user-centered security seeks to protect them from being victims of malefactors and from being conduits of malfeasance. It also encourages users (including customers) to report incidents and suspicious behaviors to IT support, security, or both, as soon as possible.

8. Don't "go it alone." Enterprises are increasingly deciding that IT security is too important and widely needed to be left in the hands of IT and security teams alone. Many are also separating security budgets and activities from mainstream IT, spreading those budgets, efforts, and awareness across the entire enterprise. Some well-known, highly respected companies are on record as "crowdsourcing" security information and intelligence. You can start by engaging colleagues in other departments within your own organization.

9. Use intelligence about your environment and tailored reports to identify and prioritize threats, to promote and encourage support of security initiatives, and to drive and support security- related decisions. Infrastructure intelligence and reports based on "real-life" data from your own environment can often be the most persuasive and effective communications tools with your colleagues within and beyond your IT and security teams.

10. Strive to make continuing education about and evolution of security at your enterprise a priority for everyone. As Gartner analyst Lawrence Pingree told The New York Times in October 2015, "There are 600 million individual files known to be good, and a malware universe of about 400 million files. But there's also 100 million pieces of potentially unwanted adware, and 200 million software packages that just aren't known. It takes a lot of talent to figure out what's normal and what isn't."

You have no way of knowing if and when any of those 400 million known malware files may be targeted at your enterprise—if one of them hasn't been so already. And despite organizations spending some $30 billion annually on security tools, vulnerabilities and threats become actual breaches every day. By modernizing your IT security tools and processes, you and your team can materially improve security at your enterprise, in ways that extend protections today and prepare effectively for the future, whatever it may hold.

Ivanti Endpoint Security for Endpoint Manager: Modern IT Security

Ivanti® Endpoint Security for Endpoint Manager (formerly Landesk Security Suite) offers multi-layered protections that safeguard your users and IT resources against the most sophisticated threats. Features include automated patch testing, deployment, and management for Microsoft Windows and macOS systems, vulnerability detection and reporting for select Linux editions, application and network access control, antivirus integration, and more.

The solution also integrates with Ivanti® Endpoint Manager (formerly Landesk Management Suite) to unify endpoint security and endpoint management. This enables rapid automation of both security and IT management policies, and delivers unequaled visibility across IT security and management activities. The integration also adds the consolidated, customizable interface of Ivanti® Workspaces for the Security Administrator.

Ivanti Endpoint Security for Endpoint Manager also delivers comprehensive, configurable report and dashboard options. These help to sharpen risk and threat visibility, ease compliance with regulations and policies, and improve your overall security posture. More information is available from your Ivanti representative or online at www.ivanti.com.

Learn More

ivanti.co.uk
☎ **01344 442100**
✉ **contact@ivanti.com**

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.

IVI-1863 07/17 AB/BB/DL