WHAT WE LEARNED ABOUT CYBER SECURITY IN 2017

4 Lessons to Help You Shape Your Strategy in the Year Ahead

vmware®

New Threats, New Opportunities

For the business world, 2017 was a year of major change. Organizations began to map the digital landscape and stake new claims—and malicious attacks quickly followed. It was a year that saw businesses and IT leaders face a growing set of threats, even as new opportunities emerged for growth and innovation.

What did we learn along the way? Here are several key takeaways that can help guide your security strategy in 2018 and beyond:

1 The attack surface continues to grow

2 Attacks are outpacing protection

3 New threat capabilities require a new approach

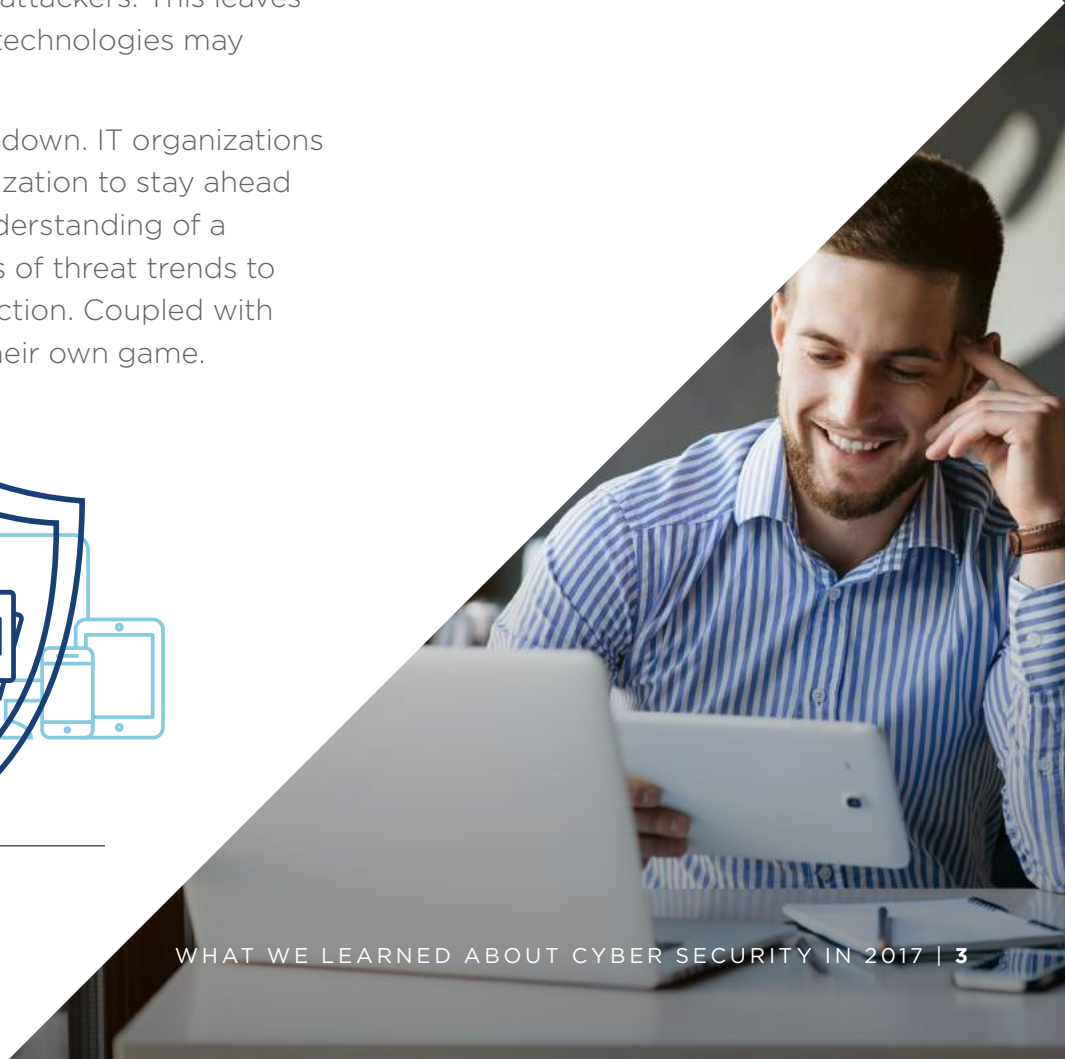
4 Shortages in cybersecurity staffing increase risk

1 The Attack Surface Continues to Grow

Devices, users, applications, and data are proliferating rapidly. While this is good for business—increasing flexibility, improving productivity, and encouraging innovation—it also creates more opportunities for malicious attackers. This leaves IT leaders scrambling to determine how new initiatives and technologies may leave the business exposed. It's a never-ending task.

Chasing threats is futile. There are simply too many to track down. IT organizations must take a proactive approach that's unique to their organization to stay ahead of emerging attacks. This type of approach pairs a deep understanding of a business's specific vulnerabilities with an ongoing awareness of threat trends to help teams create an intuitive strategy for data center protection. Coupled with the right tools, this approach enables IT to beat threats at their own game.

The information security market is expected to grow at a 7.9% compound annual growth rate, reaching $120.2 billion by 2021[1]



1 Gartner, Forecast Analysis: Information Security, Worldwide, 3Q17 Update, December 2017

2 Attacks Are Outpacing Protection

Despite an increase in security spending, the number of breaches continues to grow—and no business or industry is immune.

The widespread use of encryption is making threat detection more difficult, and advanced threats from nation states have made it even harder for security leaders to protect their infrastructure and data. For organizations today, it's not a question of "if" when it comes to security breaches—it's simply a matter of "when."

Spending more money isn't the solution. To protect your data, users, and brand, you'll need to transform the way you approach security.

+27.4%

Increase in the average annual number of security breaches in 2017[2]

+22.7%

Increase in the cost of cybersecurity in 2017[2]

2 Accenture Security, '2017 Cost of Cybercrime Study,' December 2017

3 New Threat Capabilities Require a New Approach

As data centers, cloud technology, applications, and devices evolve, so do threats. Traditional security solutions designed for a different era don't have what it takes to stop them. Modern attackers take many forms and disguises that can't be detected. Instead of chasing threats, IT needs to focus on prevention to address threat vectors and reduce the attack surface.

In the past, IT has placed a widespread tactical emphasis on chasing after the bad—but today, that only draws an organization's energy away from preventing attacks. Using strategies such as least privilege, IT can maintain a proactive stance against even the most sophisticated threats.

The concept of least privilege allows a user, device, process, or application to access the information it needs—and no more. Additionally, applications are carefully monitored in their intended state and runtime states, so any changes can be quickly identified. Automatic alerts prevent tampering and unexpected changes.

4 Shortages in Cybersecurity Staffing Increase Risk

In 2017, ISACA released a cybersecurity report indicating there was a labor crisis of skilled security workers. 64% of senior IT and business leaders surveyed said that half or less of their applicants are qualified for an open security position. There is industry-wide acknowledgment today that there simply aren't enough people who know what they're doing to keep up with security.[3]

High turnover in security roles is also a problem in many organizations. This turnover can lead to a loss of critical institutional knowledge; when workers leave a company, they often take valuable insights and skills with them. In their absence, others may not advocate for expanded security budgets or solutions the organization needs.

The talent shortage puts the enterprise at a disadvantage, as its ability to respond to new challenges depends on the people able and willing to meet those challenges. Without skilled professionals to stop the growing number of attacks, organizations remain easy targets for threats.

Ongoing education and established processes, tightly coupled with automation and frameworks, can help organizations retain talent and mitigate risks.

3 ISACA, State of Cybersecurity 2017, 2017

The security team is pressured by the organization's sometimes unreasonable expectations, and, facing the inevitability of an intrusion or seeking greater challenge, security operators and leaders move from job to job with notable frequency. This turnover has an enervating impact on institutional knowledge; as the savvy and those in-demand move on to lucrative roles—or are terminated in the wake of a breach—and no one remains to advocate for expanded security budgets and programs.[4]

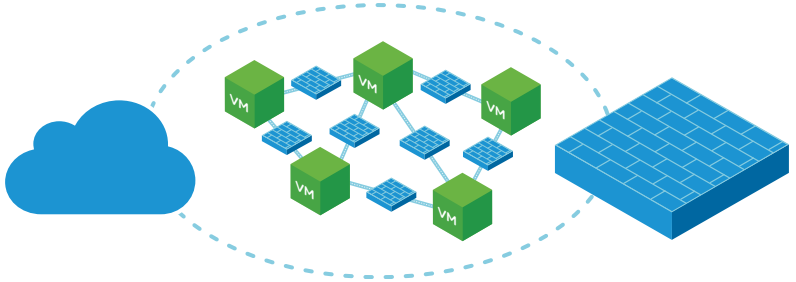
4 Gartner, How to Respond to the 2018 Threat Landscape, November 2017

Take Strategic Action: VMware Recommendations for 2018

While the threat landscape can seem daunting, it's far from invincible. These best practices from VMware security professionals will help you strengthen your security posture and keep your organization protected in the months and years to come.

Place emphasis on detection and prevention

Establishing known application behavior serves as a baseline for threat detection and prevention. If behavior ever deviates from this "known good" configuration, responsive measures can automatically be activated.



Use segmentation to reduce the attack surface

Keeping virtual machines and individual workloads separated stops threats from spreading fast. By creating enclaves, you can limit the reach of a threat. Micro-segmentation, enabled by network virtualization, stops the lateral spread and effectiveness of an attack. By shutting down the ability for threats to use east-west traffic, you can detect, isolate, and eliminate an attack before it spreads.

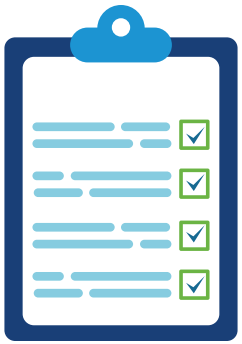
Take Strategic Action: VMware Recommendations for 2018

Use threat intelligence

The best threat intelligence solutions are unique to businesses. There is no one-size-fits-all approach. A customized strategy is able to deliver a high-confidence alert, initiating an actionable response from your IT team.

Maintain basic cyber hygiene

Use patching and systems hardening to keep threats at bay. Information security should prioritize patching efforts for IT operations, and share the reasons for the patch. This helps increase cooperation and reduce friction. Patch what you can, and use detection everywhere.



Plan your acquisition of new security technologies

Not every security solution will work for your business. IT has to ensure that new technology addresses specific threats within the business, and can be managed with existing staff skill sets. If security professionals don't know how to use a tool, it's not worth the investment.

Keep Your Business Secure Today, Tomorrow, and Beyond

Securing your data has always been an important part of any business—and today, it's more crucial than ever. As the threat landscape continues to evolve, IT must proactively anticipate threats and continually think ahead.

The VMware approach to security is transformative, moving beyond the limits of traditional solutions to embrace a future that is flexible, mobile, and virtualized. VMware solutions give you the ability to implement a secure and resilient application infrastructure that understands application needs and takes a cloud-native approach that aligns with today's DevOps framework. With the right infrastructure in place, you can automate security functions and integrate them into the development workflow for more protection at every level.

START TRANSFORMING YOUR SECURITY

Learn more about VMware solutions >

Join Us Online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmware-what-we-learned-about-cyber-security-in-2017-TS-0353 02/18