REPORT EXCERPT

PREVIEW

2017 Trends in Information Security

NOV 2016

Scott Crawford, Research Director

Garrett Bekker, Principal Security Analyst

Adrian Sanabria, Senior Analyst, Information Security

Dan Cummins, Senior Analyst, Security

Eric Ogren, Senior Analyst, Security

Patrick Daly, Senior Research Associate

Cloud. DevOps. Analytics and automation. The good: Victory for anti-malware at last. The bad: So what comes after malware? The ugly: The scale of Internet of Things security exposure has now been demonstrated, with more shocks surely to come. 2017 could mark the beginning of an entirely new world for information security.

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to more than 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
20 West 37th Street
3rd Floor
New York, NY 10018
P 212-505-3030
F 212-505-2630

SAN FRANCISCO
140 Geary Street
9th Floor
San Francisco, CA 94108
P 415-989-1555
F 415-989-1558

LONDON
37-41 Gower Street
London, UK WC1E 6HH
P +44 (0)20 7299 7765
F +44 (0)20 7299 7799

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
P 617-261-0699
F 617-261-0688

ABOUT THE AUTHOR

SCOTT CRAWFORD

RESEARCH DIRECTOR

Scott Crawford is Research Director for the Information Security Channel at 451 Research, where he leads coverage of emerging trends, innovation and disruption in the information security market.

Executive Summary

2017: IT'S A NEW WORLD

A year ago, when we looked ahead to 2016, we expected the time to be ripe for the emergence of fundamental changes in the security landscape that had been building for some time. In large measure, we weren't disappointed. This past year, as cloud and SaaS continued reshaping not only IT but security as well, we saw some of the industry's biggest names make aggressive moves into cloud application control (CAC), with Symantec all but betting its future on alignment with Blue Coat Systems and its then-most-recent acquisition, Elastica. We've seen new endpoint security and anti-malware technologies reach a point of real effectiveness when compared to past approaches. We've also seen the anticipated impact of these advances on the legacy technologies of some of the industry's largest players, as three major vendors – Dell, Hewlett Packard Enterprise (HPE) and Intel – each reached deals to sell non-core software assets, including all or part of their security businesses.

Other predictions came true with a vengeance. The security of the Internet of Things (IoT) did indeed become the 'buzz' topic of the year – but September's distributed denial-of-service (DDoS) attacks (the largest to date) exposed the alarming simplicity with which poorly secured IoT devices could become tools of disruption.

Where will these trends, as well as more recent developments, take us going forward?

In this year's report, we see the extension of trends that will continue to influence security in 2017 and beyond, such as the ongoing seismic shift being brought about by advances in anti-malware, analytics and the cloud, and the possible fallout from an over-crowded field of startups seeking to capitalize on these opportunities. We examine the growing role of automation in closing gaps: not only taming the complexity of IT security, but also helping to shore up security despite the continuing shortage of experienced staff.

We expect to see even more fundamental changes in the nature of how security is 'done' in IT, with enterprises continuing to move away from legacy and on-premises techniques to the agility of the cloud, containers, microservices, infrastructure as code and offerings based on subscription. We expect the continued advance of DevOps and its associated toolchains and processes to play a role in this evolution. These are areas in which security practitioners may not be as well versed as they will need to become, and the impact of these changes could be as disruptive as it could be beneficial.

The threat landscape concerns us even more. With the emergence of more effective anti-malware, where will attackers turn for the results that they have previously relied on malware to produce? With foreign attacks targeting US political objectives in our rearview mirror, we must wonder how far nations are willing to go in exploiting the cyber realm. Now that IoT security fear, uncertainty and doubt (FUD) has been replaced with real evidence of the scale of IoT risks, where will attackers – and the industry's response – take us next?

To paraphrase the inimitable Bette Davis, fasten your seat belts. It's going to be a bumpy ride.

451 Research's 2017 Information Security Trends

Source: 451 Research, 2016

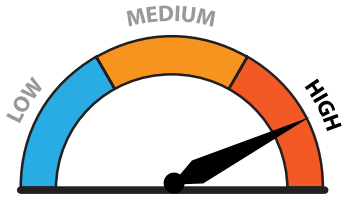
	WINNERS	LOSERS
The Seismic Shift of the Security Market Will Continue	Security platforms built for the cloud and software-defined environments, those designed for integration with DevOps processes, and those that make the most of advances in automation, infrastructure as code and turning analytics and intelligence into action; providers that can help enterprises more effectively connect physical infrastructure and a distributed workforce with end-to-end security	Legacy techniques that attempt to 'lift and shift' toward the cloud or service-oriented IT without a fundamental re-thinking of what they do or why they even exist; vendors seeking to capitalize on the latest trends
Automation Will Come to the Rescue, but Is Stuck in Traffic	Organizations that adhere to a prioritized, risk-based approach to security and IT controls; systems that implement response-oriented APIs so customers and managed security service providers can choose their own remediation steps	Vendors that run the risk of becoming assimilated, commoditized or made obsolete by SIEM vendors; SIEM vendors that may still need a SIEM; analytic vendors that excel at showing SecOps problems they didn't know they had
We'll Solve Malware! What Then?	Organizations that move beyond malware to prepare for and prevent attacks deploying other tools; those who filter signal from noise, focusing on the practical rather than wasting time preventing theoretical attacks	Vendors still addressing 'known' – and therefore common – threats; vendors that try to explain malware effects to customers rather than prioritizing defense; defenders that prioritize enterprise and consumer threats separately
Cloud Security 2.0 Will Feature More Convergence, Less Fragmentation	The cloud security vendors with the most toys, able to span multiple categories and cloud environments; bankers, VCs and developers	Few-trick ponies; traditional security practitioners; CAC wallflowers
Cloud and DevOps Will Go on a World Tour	Those who build for tomorrow's problems and challenges, identifying long-term gaps and needs in the cloud; organizations willing to redesign apps, architecture and workflows to best take advantage of cloud; companies that 'rip off the bandage' to move to new IT thinking and tooling	Vendors that fail to build for the cloud; enterprises that attempt to forklift existing infrastructure, applications and security controls into the cloud; those that lack focus and funding for talent acquisition and training
IoT Security Exposures Will Mean Larger Attacks With More Serious Consequences	Adversaries looking for the next big thing; big government; technologies on a lucky streak	All of us… and time is not on our side; the IoT security market, where only the strong will survive

Table of Contents

TREND 5: CLOUD AND DEVOPS WILL GO ON A WORLD TOUR

Implication: *Cloud and DevOps are simultaneously some of the most disruptive and the least understood trends in IT since the internet gave rise to e-business, e-games, e-commerce and e-everything-else. Much more than just fads, cloud and DevOps will distinguish winners and losers in the contest to best leverage what many envision as the 'new IT.'*

Impact to the Market



The 'new IT' has officially become an unstoppable force. No, it won't replace existing IT environments entirely, but it is destined to disrupt a sizeable chunk of the way that businesses have traditionally used IT. New IT is a big change for existing IT environments, and it isn't just a technology shift. The change in speed and capabilities is so dramatic that many existing IT workers can't easily make the leap, creating a skills gap. The resulting workforce demand resembles something we've only seen once before, during the dot-com boom. Tooling and processes are changing. Design, architecture and dominant software vendors are changing. Product delivery has shifted primarily to as-a-service and subscription-based models. IT has been hit by the tech equivalent of the agricultural revolution. We don't grow our 'food' anymore – and with online shopping taking over so many markets, fewer every day see a need to even go to a store. So it is becoming with IT: The percentage of IT organizations dealing with software is growing, as the percentage dealing with hardware and datacenters is disappearing.

As IT goes, so goes security. These changes are having a profound effect on the skills expected from the average security practitioner and on how security is designed and implemented. Options to 'bolt on' security often disappear as software development teams move from Waterfall to Agile – and that's only the beginning. As trends move from Agile to continuous integration, continuous delivery and on toward a truly integrated DevOps approach, security must be baked in. This means more than just giving lip service to the concept, as both security and IT have done for years with, frankly, not a whole lot to show for it until now. Security products must be either integrated into developer tools or largely automated in the software development lifecycle. This also necessitates a shift in security function: It will become common for non-security IT roles to handle most of the vulnerability management process without the help of the security department. Conversely, security staff will need development skills not only to automate and integrate security controls into cloud-based infrastructure and Agile processes, but also to know how and where to apply security measures in concert with the toolchains that define processes from development to operational deployment. The combination of security, development and operational deployment expertise this picture describes should make it apparent that the skills gap is going to be a common refrain we'll continue hearing in regards to the new IT. As if the security skills market weren't already tight enough, development and operational teams as well will have to become more literate in what it takes to secure the 'new IT' as part of the cultural shift that characterizes the move toward DevOps.

In both our formal surveys and anecdotal conversations we hear the same story over and over again. Customers and vendors get it – the cloud, containers, DevOps, Agile, automation – it's all amazing, the benefits are clear, the water feels great and everyone wants to dive in. One problem: most haven't yet learned to swim in these new waters – or, for that matter, figured out where to get in. Unsurprisingly, no one wants to drown and the top fear has always been security for the uninitiated. The good news is that most businesses find security to be significantly easier with the new IT once they're familiar and comfortable with the environment. Getting to that point is the key here: We're in the midst of a long transition, and this is the time for IT and security to be getting their feet wet. It is also an opportunity for companies to work with the providers of hosting services, managed services, consulting services and cloud-specific security products to help ease this transition.

Addressing again the technology and product side, the topic of baked in vs. bolted on arises once more. Some newcomers to cloud and containers insist on bringing the existing trappings of traditional IT life with them. To do so is natural – most businesses have significant investment in existing products in the form of experience, staff trained and certified on particular products, and perhaps even years left on existing contracts. While shoehorning virtual appliances into the cloud is possible and can be made to work, however, the more experienced know it isn't practical, economical or even the most secure option. Our research shows that most attempts to 'bring the whole house when we move' fail, and blame is often misplaced on the cloud services.

When building for cloud, priorities change. Automation and APIs are required in a minimum viable product, whereas what once might have been 'core' features can wait until the next production release (which is often just two to six weeks away). The point is that, since products are built quickly, mistakes are caught quickly. The end result is more satisfied customers and a more solid product that will attract a wider audience. Tossing a virtualized version of a security appliance or agent-based product at the cloud doesn't make sense.

The truth is that nearly every success story in the cloud comes with an extremely short list of security products. While the average number of security vendors in a large enterprise is said to range from 50-75, we rarely see a list of more than five security products involved in a successful cloud deployment. We've seen PCI-regulated businesses achieve compliance in the public cloud with as few as three. To be fair, the quote of 50-75 products relates to the entire enterprise, not just servers, but the reported reduction in complexity, management and costs is still significant.

Security procedures in the new and old IT environments aren't directly comparable in a number of other ways. Consider, for example, how defensive strategies might change if:

- The average life of a server is less than a day.
- All servers are replaced within a week.
- All administrative access to servers is removed when they are placed into production.
- Patches are rolled out to all production systems in four, six or nine hours rather than 45, 60 or 90 days.
- A 100%-accurate inventory of assets can be retrieved in milliseconds instead of an 80%-accurate list taking 24-48 hours to assemble and becoming out-of-date before it can be completed.
- Credentials in the production environment are changed every few minutes or hours.
- Enforcing and reporting on 90% of PCI requirements are fully automated.

Sure, all of these strategies don't remove risk entirely. However, consolidating risk from internet-exposed resources and significantly reducing attack surfaces are huge wins all the same.

RECOMMENDATIONS

- **Practitioners should start learning cloud, containers and DevOps now.** Even if no current plans exist to move infrastructure into the cloud or adopt DevOps practices, every organization needs to have direct experience and understanding of these trends, even if it is just to understand 'what the fuss is about.' The good news here is that any budget can support new IT experience, whether the target is a small R&D team and $50,000, two to three people and $1,000, or one person and $0 (most public cloud providers offer free or temporary trial tiers).
- **Technologies should be designed for the cloud, not shoehorn in existing products.** Aim to build for the cloud so that products can be baked into infrastructure and applications. Security controls in the cloud should be as transparent as possible.
- **Let processes drive products, not the other way around.** In the world of cloud and DevOps, nearly every case requires a build vs. buy decision: Many DevOps shops choose the 'build' scenario and conveniently share their solution for the problem on GitHub.
- **Be willing to abandon current thinking.** Imagine being asked to take a $100,000 IT operation and reduce costs to $5,000, while demonstrating significant improvements in uptime, security, disaster recovery and resilience. Be willing to slaughter 100% of the technological and political sacred cows that currently power the $100,000 operation to get to these goals. Could it be done for $5,000? If not, how about $10,000 and improvements in two of the three areas stated? This is the kind of thinking that results in cloud- and DevOps-friendly products and environments. Focus on the idea of continually streamlining applications, operations and processes while reducing complexity and maintaining or improving on business requirements.

WINNERS

- **Those that build for tomorrow's problems and challenges, not just today's.** Winners will identify long-term gaps and needs in the cloud that IaaS/PaaS providers can't or aren't likely to provide themselves. They will have a five-year vision, not a six-month vision. For example, with 'serverless' technologies rapidly rising in popularity, imagine the cloud if there are no operating systems to patch or manage. Imagine if there is nowhere to install an agent.
- **Students of cloud successes and failures.** Cloud isn't a container to move a datacenter into. Successful organizations will redesign applications, architecture and workflows to best take advantage of what cloud has to offer. Look at DevOps practices in companies that have been doing it for three to five years or more. Pay attention to how these businesses manage code and infrastructure and note where gaps and challenges still exist.
- **Companies that don't try to win points for subtlety.** The winners so far haven't tried to ease into trends; they 'rip off the bandage,' even when that requires laying off employees that can't make the move to new IT thinking and tooling. Sometimes, this results in a new IT and old IT coexisting, even in completely segregated teams and environments.

LOSERS

- **Vendors that fail to build for the cloud.** Vendors that repackage existing products and make superficial changes before slapping on a cloud label will find an eager market in the short term, but will fail to make the transition in the long term.
- **Enterprises that attempt to forklift existing infrastructure, applications and security controls into the cloud.** These organizations will find the result to be unnecessarily expensive, operationally burdensome and ultimately disadvantageous. Ideally, everything should be rebuilt, redesigned and rethought for cloud and DevOps. This includes security controls, compliance and privacy considerations.
- **Those that lack focus and funding for talent acquisition and training.** Any company that doesn't retrain or actively hire a cloud and DevOps-savvy workforce will struggle to keep up with both trends.

The Long View

In spite of all the new concerns that have arisen to trouble infosec pros in 2016, many aspects of the future look brighter than ever before. Anti-malware technology seems poised to turn a corner toward real prevention. Continued advances in email defense and behavioral analytics are beginning to put a crimp in adversaries' ability to exploit user credentials and hide anomalous activity. Security automation and cloud-based infrastructures are starting to fill in the broad outlines of a far more agile response.

These achievements, promising as they are, are only the beginning of a much more ambitious vision. The ultimate future would incorporate intelligence that equips defenders with the insight to recognize the precursors of malicious activity before it becomes a serious threat. Once a threat materializes, intelligent systems would be able to deflect and defeat it or, in those cases where evidence-gathering is in view, contain it and allow it to unfold under discreet observation, insulated from actual assets, until data collection is complete. Automation would then follow up to preserve evidence, better automate response processes and remediate exposures where able.

Clearly, the industry has a long way to go. Among many other things that must happen for this vision to become reality, security tools must learn to talk to each other better. Market segments tend to beget silos; while these help emerging technologies to define new spaces and boundaries within which to excel, they can also mask a complete picture of security threats. Adversaries have few such encumbrances. Moving quickly from social engineering to initial penetration to reconnaissance within the target organization, and from there to data discovery, exfiltration or potentially greater damage, the adept attacker has historically been able to leap with comparative ease from network to endpoint and application to data. For defenders to equal this agility, detective and preventive tools must exchange information to reveal how actions in one sphere can potentially threaten the next objective in the attack sequence… and the next, and the next after that.

Our term for the sort of integration that can yield this more effective insight is the Actionable Situational Awareness Platform (ASAP), and we are beginning to see indications of it coming together. Splunk, for example, touts a similar vision, embracing a variety of moving parts in its approach to what it calls 'adaptive response.' Organizations such as Sophos claim 'synchronized security' through cross-technology data integration, McAfee has its Data Exchange Layer and Cisco embraces a nexus of information exchange represented by its pxGrid concept. Threat intelligence platforms, incident tracking and response systems and new threat-hunting technologies, meanwhile, seek to bring together a wide variety of disparate data sources and types to reveal patterns of malicious activity. In order to be truly adaptive, however, these emerging integrations must go much further, automating not only evidence gathering and correlation but also response engagement to contain a threat faster and more effectively than people can ever hope to do. If automation and intelligence is ever to help offset the attacker's asymmetric advantage, this is how it will happen.

These new approaches to enterprise defense won't, however, slow down threats to the broad realm of consumer technology and a growing array of IoT devices that have recently shown themselves to be more than fertile ground for adversaries. Nor will these advances necessarily be within reach of the many organizations *below the security poverty line*. Cloud computing platforms and service providers may be in the best position to help close these gaps. The large-scale implementations of IT necessary for viable IaaS platforms align well with the sophistication needed for more adaptive security, making many advantages of both enterprise-class computing and security more accessible to a wider audience, and boding well for the future of security SaaS. The ability of service providers to stem network-borne attacks has already been demonstrated in the anti-DDoS offerings of CDNs. Security SaaS offerings could extend this ability to smaller or more poverty-stricken security initiatives, while the role of ISPs in improving security for everyone may receive greater scrutiny if emerging large-scale attacks pose a more serious threat to the public interest going forward.