Research Agenda, Q1 2017

Information Security

Covering innovative technologies and trends that characterize the ever-changing nature of the security landscape, within the contexts of risk management and business processes.

The Information Security Channel covers technologies that organizations deploy to protect themselves against an ever-increasing array of threats, with emphasis on areas including advanced threat defense, endpoint protection, cloud security, security analytics and intelligence, data protection and emerging trends in identity and access management. Aimed at senior security practitioners as well as vendors and investors, the Information Security Channel examines technical issues within the contexts of risk management and business processes. Our research reports run the gamut of critical security topics, from profiles of companies just out of stealth to exploring how security products end up as shelfware.

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 over 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.

Analysts

Scott Crawford
Research Director, Security

Kathryn Ball
Senior Research Associate

Garrett Bekker
Principal Security Analyst

Dan Cummins
Senior Security Analyst

Patrick Daly
Senior Research Associate

Eric Hanselman
Chief Analyst

Daniel Kennedy
Research Director, VotE

Eric Ogren
Senior Analyst, Security

Adrian Sanabria
Senior Security Analyst

Aaron Sherrill
Senior Analyst

Overview

With data breaches and targeted attacks continuing to capture headlines, security remains a top priority for the enterprise. As we describe in our 2016 M&A Outlook Report, a recent 451 Research survey of investment bankers showed that security edged out mobile technology for the first time in six years as the segment anticipated to have the most M&A activity. This is not a new phenomenon. Enterprise security has appeared in the top five categories of this survey for the past four years. Why the persistent demand for technologies to assure protection and integrity for sensitive information assets?

For one thing, security technology is expanding in multiple directions. Advances in speed and storage capacity, along with cloud computing, are making new features and techniques not only possible, but necessary. More complete and more detailed event data can be stored longer and analyzed in increasingly complex ways. At the same time, the security industry must react to every development in IT.

But there is more to the continuing demand for security technology than simply riding the coattails of IT evolution. According to breach data maintained by the Privacy Rights Clearinghouse, the number of records breached has continued to grow over each of the past four years – and it actually doubled in 2015 over the previous year. Thus, a paradox: While security spending remains high, so do security breaches.

Clearly something needs to change. For years, compliance has been a principal driver for infosec spending in the enterprise. Even if it was tacitly acknowledged that a state of compliance wouldn't necessarily keep the riffraff out, compliance was still handy for security managers as a lever for getting the budget they needed. Today, however, organizations recognize that they really do need to be secure – and they are demanding both technologies and expertise that go beyond legacy approaches to get the job done.

And now, the demand for better security goes beyond IT. The increasingly pervasive nature of computing promises to extend intelligence to a wide variety of environments that have heretofore been regarded primarily as operational technologies. The Internet of Things (IoT) not only introduces new risks to safety and security; its growing intersections with IT mean that it expands the attack surface of the enterprise as well.

In the coming months, 451 Research's Information Security practice will concentrate on some of the key changes in the security market that reflect this demand.

Security and the Internet of Things

With the hype surrounding IoT reaching a fever pitch, it seems that every technology vendor is rushing to market with an IoT offering. But for once, enterprises are placing security concerns ahead of blinkered optimism about a new technological development. In 451 Research's Voice of the Enterprise: Internet of Things, Workloads and Key Projects - Quarterly Advisory Report, security concerns were considered the number one impediment to deploying IoT initiatives by a wide margin (46% of respondents, as compared to the number two response, 'lack of internal skillsets' at 32%).

The concern is understandable. Even if threats are only just beginning to emerge, the range and severity of risks cannot be overlooked – from disruption of day-to-day operations to the safety of life on an unprecedented scale. Technology vendors have, of course, responded to this keenly felt concern – but not all responses to IoT security concerns are created equal. We have seen a great deal of 'IoT washing' already among vendor offerings – but some new entrants into the world of IoT security do offer promise. We'll be taking a closer look at some of these as the drivers influencing directions in IoT security continue to take shape.

Security in the Post-AV World: Threat Detection, Remediation and Endpoint Security

What used to be the province of plain, old-fashioned antivirus is now a panoply of technologies, techniques and products. In 2010 we were writing about anti-malware, anti-spam, anti-spyware and platform-specific protection such as email and web security. In response to polymorphic malware, credential theft, man-in-the-middle attacks and more, security vendors have rushed to bring out sandboxing, indicators of compromise that go far beyond signatures, behavioral heuristics, exploit technique detection and 'sinkholing' to detect signs that an attack was already successful. We produced a Market Map in 2015 covering a number of aspects of this (r)evolution affecting a number of segments in endpoint security – and as these overall trends remain a primary focus of security transformation, we will continue to track them going forward.

'Post-AV' Threat Detection and Remediation

The 'post-antivirus' world of threat detection and remediation is a segment that emerged out of incident response services and is now one of the most active new security markets we're monitoring. Though techniques are capable of detecting malware, the approach of continuous recording and collection of a detailed record of events that occur on the endpoint allow new technologies to detect attacks and other anomalies that may not involve malicious software at all. It comes in agent and agentless variants, with customers split over the two options – some are willing to install yet another agent, while others prefer to go agentless and wait for market consolidation to eventually give them a single unified agent. It seems like we've gone through this process at least once before…

The Evolution of Endpoint Defense

Complementing new approaches in threat detection are technologies emerging to provide a more effective toolset than legacy techniques for deflecting threats that target the endpoint. Examples include approaches to compartmentalization of targeted applications, namely the web browser and office apps, as well as variations on both whitelisting and focused blacklisting techniques inherited from the world of application control. Approaches that employ virtualization or emulation/sandboxing techniques require additional resources on endpoints, while approaches that stream a remote app to the desktop go the opposite route. Both aim to limit or prevent the attacker's ability to get to sensitive files or compromise the target system, and are complemented by threat detection in the network through techniques such as sandboxing and analysis of malware behavior.

Security Analytics and Intelligence

The continued growth of security analytics in part reflects the boom in 'big data' and analytics generally. But security teams have their own reasons for embracing advances in machine learning, modeling and the management of data at speed and scale. Security operations have long been hamstrung by limitations on recognizing and acting on evidence that indicates a real threat. Today, a broad spectrum of analytics have arisen not only to help security teams break free of those limits, but to help deal with a shortage of expertise that grows daily, through tools that reveal actionable information and limit burdens of analysis that often inhibit the effectiveness of security management.

Behavior Analytics

After previous studies where they ranked second or lower, the security risks posed by user behavior moved into the top spot among enterprises in our Voice of the Enterprise (VotE) Information Security survey. Whether their actions are intentional or inadvertent, people remain one of the weakest links in security. Phishing attacks routinely capitalize on the ability to entice users to click on malicious links or execute dangerous content. Those with access to sensitive data or a high degree of privilege over IT assets pose another set of risks, regardless of whether they choose to act maliciously or are themselves targeted by third parties. When adversaries succeed in compromising a user's credentials, the ability to differentiate malicious activity from normal behavior – long a thorn in infosec's side – becomes paramount to defending against a serious threat.

Recently, a new segment of technologies has grown up to address this concern. As with security analytics generally, behavior analytics span a spectrum of approaches. At one end are technologies focused primarily on the actions of people, helping organizations identify and act on risky behavior before it leads to serious consequences. At the other, however, are techniques that encompass the behavior of IT systems and information assets as well as people. Both enter into play to baseline behavior, identify anomalies and call out threats that legacy techniques are ill equipped to identify. They also serve to help investigators proactively model and analyze potential threats and discover evidence that may otherwise remain hidden until a breach has done its damage. Our first major report on applied behavior analytics was published in mid-2016.

Threat Detection Analytics

Another addition to the security analytics spectrum are platforms that capture threat-revealing data primarily from IT and security infrastructure, both inside the enterprise and beyond. As with behavioral analytics, these technologies serve to reveal indicators of potential or actual threats before they wreak havoc on a victim enterprise. Unlike techniques that focus on user behavior, however, these tools tend to focus on threat actor tools, tactics and practices as revealed in the actions they take against a target. Threat detection analytics have a further intersection with endpoint-focused TDR, where they complement tools that focus on actions taken against a target endpoint or personal system.

Threat Intelligence

Threat intelligence gathered from third-party commercial suppliers, open sources and peers remains an area of high interest. As the field matures, organizations are more focused than ever on turning insight into action. This has resulted in a growing array of new features and capabilities among threat intelligence providers and integrators, from workflows and analytics to platforms that support the development of apps to expand their range of usefulness.

Intersections with SIEM… and Beyond

Not surprisingly, today's innovators in security analytics and intelligence promise to expand the effectiveness of existing approaches such as SIEM. SIEM has seen its own boundaries stretched in recent years, from capitalizing on the potential of cloud to mine historical data with a completeness not feasible in previous years, to serving as a source for data required for specialized use cases such as forensics investigations, user activity monitoring and incident response.

The future of analytics and intelligence has an equally provocative intersection with emerging technologies that extend the ability to automate security response, closing gaps in defense and enhancing protections when indicators point to a clear and present danger.

451 Research's Information Security Channel will continue to examine these trends, and we expect to further this exploration in emerging areas of intelligence, analytics and security automation.

Data Security

As the enterprise becomes more abstracted from the underlying hardware of IT and the perimeter gasps its last breath, more vendors are offering a data-centric approach to security. This includes data discovery, classification and governance, encryption, data-loss prevention (DLP), file integrity management, secure file sharing, cross-domain security and newer implementations of DRM/IRM technologies. Hand in hand with identity and access management (IAM), we expect data security to become more sophisticated, contextual and pervasive.

Some emerging trends we expect to cover include the growing use of encryption as a primary means to ensure data integrity and meet compliance demands as sensitive data increasingly ‘lives’ outside the confines of corporate boundaries, and the application of data discovery and encryption techniques for big-data use cases.

Identity, Access and Privilege Management

IAM has become even more critical as the number and variety of systems explode. The technology for enterprise, cloud and mobile comes from such a large field that we expect to see more consolidation happen. Privileged IAM has also grown in scope, thanks to hosting and cloud providers that need to manage both their own access and that of their customers. Authentication, which is separate from identity management, has taken the leap from hardware to software, although you could argue that phone-based authentication is just a larger, consumer-friendlier piece of hardware. Authentication is key to fraud detection, and it will play a critical role in controlling IoT. With more ubiquitous use of SSL across the web, certificate management is also key (if you'll pardon the expression).

With such a complex topic as IAM – which serves as the embodiment of how the business uses IT – it’s not surprising that more effective privilege management has appeared on the scene to help the enterprises handle access with greater granularity. Role and entitlement mining, governance, behavioral and content analysis, and attribute providers will also have their parts to play as IAM continues to have a central role in securing the enterprise.

Application and Software Security

The security of software continues to be a primary emphasis for protecting organizations from technology risks. As transformative trends from the cloud to DevOps have influenced the direction of IT, they have influenced directions in application and software security as well.

In the past, application security was regarded primarily as a periodic exercise in which an application system could be evaluated for flaws in source code, as well as in running applications after deployment. Today, applications may be in continuous or near-continuous use. Changes may be deployed incrementally as features are added and problems are addressed. The trend toward continuous development and integration of functionality into working applications increasingly defines a new set of practices around DevOps – and security must become a part of this trend.

The realm of application and software security extends beyond IT, however. Software defines the functionality of a great many operational technologies, from a wide variety of endpoint ‘things’ to the centralized systems that manage and control highly distributed (and often sensitive) functionality and collect volumes of operational data. This places software security on the front lines of IoT risk management.

Software and application security is also spreading beyond the development lifecycle, as organizations embrace concepts of mitigating risk early in the software supply chain – before vulnerabilities in available modules and code are integrated into development. And in defending applications in runtime, application self-protection is transforming the nature of perimeter- and gateway-based software defense. We will continue to watch these trends reshape application and software security in coming months.

Cloud Security

When it comes to cloud security, there are plenty of things new under the sun. Better security management for virtualized instances, converged IAM, increased monitoring and more granular control over SaaS functionality are all coming to the fore. The term 'cloud security' itself can be misleading: IaaS/PaaS and SaaS differ widely in terms of access to the underlying infrastructure, as do the tools and techniques – and vendors – that attempt to secure them. While some of the former are merely repackaged or 'cloud-washed' versions of existing security tools for a vastly different delivery model, others offer completely new approaches.

Cloud Application Control

In 2016, the security of cloud and SaaS was a primary focus area for the 451 Research security practice, with research published on the cloud application control (CAC) market, a very active focus for security leaders and startups alike in recent months. CAC providers essentially wrap additional security around what users are doing in SaaS applications. Some vendors focus on shadow IT (employees going off and using SaaS/cloud services without corporate approval), some focus on encrypting data that gets stored in the cloud, and others focus on detecting SaaS-targeted threats. Most cover three main functions – discovery (of the apps/services being used), analysis and control.

Cloud Infrastructure Security

Our focus also extends to security for cloud infrastructure, to manage risks in cloud environments themselves. Infrastructure doesn't work the same way in the cloud, and how customers are charged for it is also quite different. These two facts have resulted in some security startups going back to the drawing board on how elastic and scalable cloud infrastructure should be protected.

Scope of Security Coverage

In addition to the market dynamics listed above, the Information Security Channel will continue to collaborate with fellow 451 Research analysts across other channels as we assess the wider implications of the increased industry focus on Information Security. Areas followed by the broader 451 security team include:

- The wider scope of IoT
- Network security
- Vulnerability management
- Security for mobile devices and applications
- User awareness technologies that strengthen the human link in defense
- The security staffing challenge
- Distributed denial of service (DDoS) protections and WAN-scale application defense
- Security as an aspect of cloud and datacenter infrastructure
- The role of security in managed and professional services
- M&A activity in the security market

They also include new topics that may surface in 451 Research's VotE studies or appear in our M&A KnowledgeBase, or in the course of the Information Security Channel's evolving coverage. Numerous vendors overlap areas of our research, and some have multiple products in different technology domains.

Upcoming Research on Information Security

Voice of the Enterprise (VotE)

Combining 451 Research's industry-leading analysis with an extensive network of more than 50,000 senior IT professionals, Voice of the Enterprise tracks adoption across thousands of organizations and exposes the major opportunities for enterprises, IT vendors, suppliers and investors. Each quarter's survey has a focused theme, as indicated in the table below.

	Workloads and Key Projects	Organizational Dynamics	Vendor Evaluations	Budgets & Outlook
Information Security	Q1	Q2	Q3	Q4

Technology & Business Insight Reports

M&A Outlook 2017: Information Security

Analysts: Garrett Bekker, Scott Crawford, Eric Ogren, Adrian Sanabria, Dan Cummins, Brenon Daly
Publication Date: Q1 2017
Even after a recent record tech M&A run, dealmakers still had ambitious shopping plans in 2016. Across the globe, tech acquirers announced $500bn worth of transactions in the just-completed year, ranking 2016 as the second-highest annual total since the internet bubble burst. More than any other year, 2016 saw an expansion of buyers beyond the 'usual suspects,' as old-line companies got caught up in transforming their businesses through M&A.

Information Security Directions and Disruptors 2017

Analyst: Scott Crawford, Kathryn Ball
Publication Date: Q1 2017
On the heels of two international industry events to kick off 2017, this report highlights the trends and topics setting the direction for the information security market, along with new entrants looking to shake up the status quo.

Market Map: Data Security

Analyst: Garrett Bekker
Publication Date: Q2 2017
This report profiles competitors in specific major segments with a graphical display of the market and key segments in the form of a 451 Research Market Map^{TM}. The analysis includes key attributes for each segment and a view of each vendor's solution.

Cloud Infrastructure Security

Analyst: Adrian Sanabria
Publication Date: Q3 2017
As measures for securing cloud environments continue to evolve, new approaches to protecting elastic and scalable cloud infrastructure are emerging. 451 Research examines key aspects of these techniques that not only protect the cloud, but its enterprise clients – and their customers – as well.

Preview: Trends in Information Security 2018

Analyst: Scott Crawford
Publication Date: Q4 2017
This report provides a view of key trends that will affect the market in 2018. It details the top trends, likely impact and recommendations for each.