REPORT EXCERPT

PREVIEW

2018 Trends in Information Security

DEC 2017

Scott Crawford, Research Director

Garrett Bekker, Principal Security Analyst

Eric Ogren, Senior Analyst, Security

Fernando Montenegro, Senior Analyst, Information Security

Patrick Daly, Associate Analyst

In 2018, the gains realized from applied analytics will become so pervasive that we expect virtually every product to be an analytics product. Automation will become more evident, while identity will assume new importance. With EU Global Data Protection Regulation and privacy in the spotlight, what risks are on the horizon?

THE FOLLOWING IS AN EXCERPT FROM AN INDEPENDENTLY PUBLISHED 451 RESEARCH REPORT, "2018 TRENDS IN INFORMATION SECURITY" RELEASED IN DECEMBER 2017.

TO PURCHASE THE FULL REPORT OR TO LEARN ABOUT ADDITIONAL 451 RESEARCH SERVICES, PLEASE VISIT HTTPS://451RESEARCH.COM/PRODUCTS OR EMAIL SALES@451RESEARCH.COM.

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
1411 Broadway
Suite 3200
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
Paxton House
Ground floor
30 Artillery Lane
London, E1 7LS, UK
P +44 (0) 207.426.1050
F +44 (0) 207.657.4510

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
P 617-598-7200
F 617-428-7537

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

2018: A YEAR FOR CONSOLIDATION

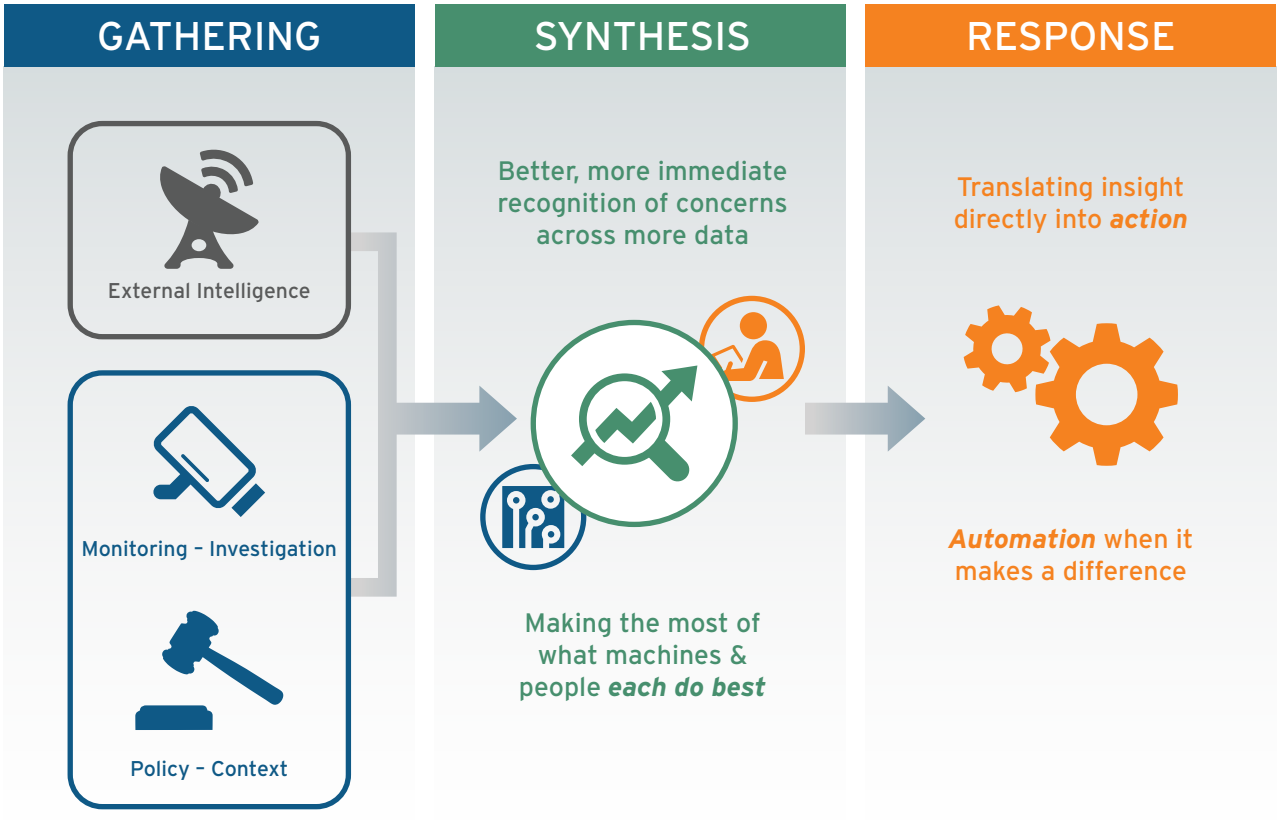
Last year at this time, we forecast a bumpy ride for infosec through 2017, as ransomware continued to wreak havoc and new threats emerged to target a burgeoning Internet of Things (IoT) landscape. 'New IT' concepts – from DevOps to various manifestations of the impact of cloud – seemed poised to both revolutionize and disrupt not only the implementation of security technology, but also the expertise required of security professionals as well.

Our expectations for the coming year seem comparatively much more harmonious, as disruptive trends of prior years consolidate their gains. At center stage is the visibility wrought by advances in data science, which has given new life to threat detection and prevention – to the extent that we expect analytics to become a pervasive aspect of offerings throughout the security market in 2018. This visibility has unleashed the potential for automation to become more widely adopted, and not a moment too soon, given the scale and complexity of the threat landscape, as well as of IT, and the strain this complexity continues to place on security professionals – people who are becoming increasingly challenging to find, train and retain.

Together, these advances can help break down longstanding silos that have held security back from doing a better job, and relieve practitioners overwhelmed by security's demands. We first described this much-needed coming together of data, analytics and automation in early 2016 in a concept we called the *Actionable Situational Awareness Platform (ASAP)*, shown in the figure below.

Actionable Situational Awareness: A Long-Cherished Security Goal

Source: 451 Research, 2017



Improved analytics and automation have remade some segments in security, and given new importance to others. Endpoint security has been particularly aggressive in waving the 'machine learning' flag. In 2018, we expect to see continued consolidation of features as 'next-gen' endpoint security matures – and perhaps consolidation among vendors as well.

We also expect to see identity and access management (IAM) assume greater importance. Improvements in the ability to discern whether or not users and their endpoints should be granted access, to give users greater control over their personal information, and to do all this at scale will combine with the desire for users to connect to the enterprise from any endpoint, on any network. Together, these drivers will threaten to displace the traditional role of the network as the primary gatekeeper of access.

But these advances aren't without their downside. Few terms were as overused in 2017 as 'machine learning,' to the extent that it has been all but invoked as the deus ex machina come to save to all that ails security – from better detection of malware, to resolving human behavior that exposes organizations to threats, to answering the security skills shortage. There is, of course, a kernel of truth in its applications, and a naïve dismissal of machine learning risks missing the forest for the trees. The 'herd immunity' results achievable with well-thought-out applications of massive datasets, sophisticated models, and cloud-based sharing will continue to help achieve good results, particularly in areas such as the fight against selected forms of malware. It is also true that people do far too much repetitive drudgery to support security operations in many enterprises. While AI may yet have a ways to go before we see a virtual security operations center (SOC) analyst, there's much that analytics and automation can do to alleviate demands on many operational tasks that machines could do faster or more efficiently, freeing people to focus on what people can do better than machines.

The increasing pervasiveness of intelligence that we see beginning to permeate so many aspects of digital experience does, however, pose a threat to privacy – a matter of no small concern, given that the total number of records compromised in data breaches tracked by the Privacy Rights Clearinghouse since 2005 has tripled to nearly 10 billion in the last two years. We see a resurgence in compliance as a primary driver for enterprise security – privacy will be at the forefront in Europe next year, with the EU Global Data Protection Regulation (GDPR) entering into force in May.

As the digital realm becomes more pervasive, these and other risks become increasingly universal, with the implications of technology risks extending through virtually every aspect of life shaping our future. We conclude our look ahead to 2018 with a view toward this farther horizon – and a taste of forthcoming research on the long-term future of IT touched by these aspects of universal risk.

REPORT EXCERPT

Table of Contents

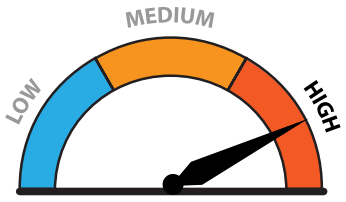
The following Table of Contents represents the full research report, which can be found on the 451 Research website ***here***.

Trends

TREND 1: EVERY SECURITY PRODUCT WILL BE AN ANALYTICS PRODUCT

Implication: *The modern security approach centers on the need for more sophisticated analysis of security data, for everything from threat and vulnerability mitigation to assuring confidence in IT access and use. This points directly to a pervasive need for analytics throughout multiple segments of the security market. It's not just because data is needed to understand and resolve security issues in specific domains. It's also because analytics coupled with automation and response brings to life the connective tissues that integrate silos of technology and practice into a more coherent whole.*

Impact to the Market



"Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!" – Lewis Carroll, Through the Looking-Glass

This is exactly how security teams must feel these days, as they run a 'Red Queen's race' that has them in constant motion just to keep up with the security data that inundates them. With traditional approaches, security events and alerts are often fed to an SOC for resolution by human security experts – but the volume of data coming at them means that they must pick their battles. Imagine trying to keep up with a unending deluge of security tasks knowing that, at some point, any that are ignored could be the source of a major problem down the road. For those that aren't deferred or disregarded, SOC teams face a constant threat of 'alert fatigue' that places even high-impact issues at peril of inadequate response. CISOs simply do not have the time or resources for every security issue to fall into the lap of a human for resolution, and if a specialist must get involved, the relevant operational data had better be neatly packaged and at their fingertips.

Most security teams heavily tilt toward using people to interpret internal events, leading to an imbalance of energy spent by CISOs and security organizations on managing resources. After user behavior, the greatest security pain points reported by respondents to our recent Voice of the Enterprise (VotE) security surveys are organizational politics/lack of attention, staffing, lack of budget, security awareness training and accurate/timely monitoring of security events (see Figure 1).

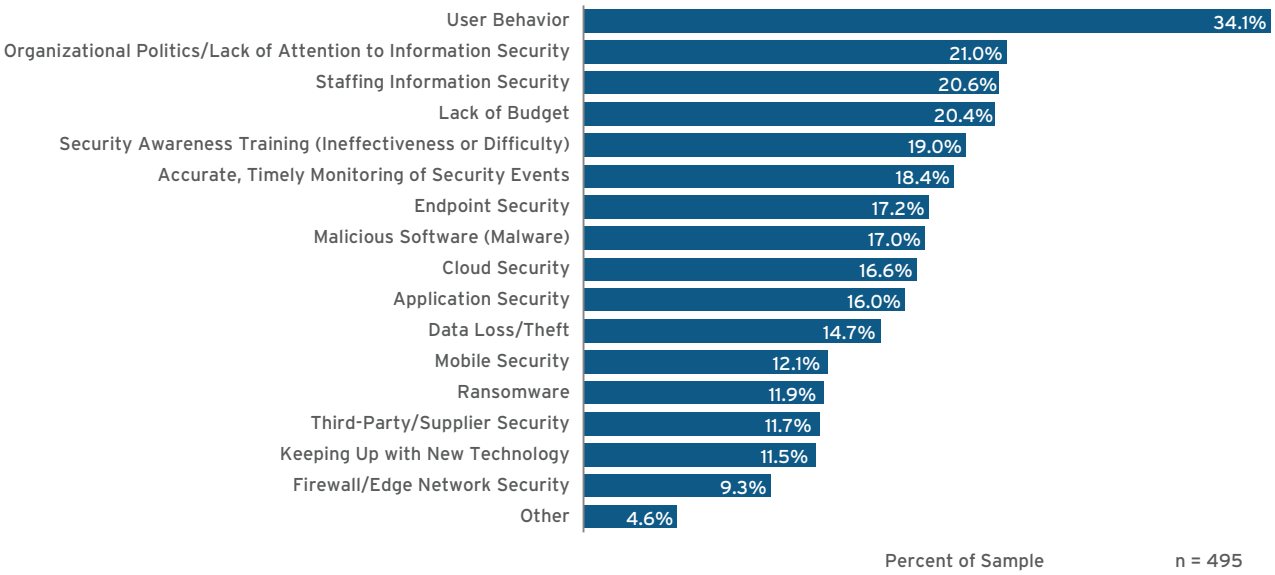
With these top pain points, ones that we see in VotE responses quarter after quarter, it is no surprise that CISOs are turning toward data-driven products, not only to assist SOC orchestration and automation of predictable response actions, but also to integrate better detection and prevention more directly and broadly into the technologies of defense. CISOs are demanding data-driven approaches in areas that do a better job of prevention than past techniques, respond faster and more effectively than people when necessary, or alleviate problems in meeting security labor shortages.

This means that we can expect virtually every security vendor to make 2018 a big year for analytics in multiple areas of the market. A quick review of major security segments already finds analytics playing important roles:

- Endpoint software has been adding machine learning layers to better detect threats both pre- and post-execution. The segment has been doing this for years, beginning with honeypots where automation learns about file attachment characteristics and operations to identify classes of attacks. Since then, major vendors have invested in insight into malware and malicious activity they collect from products deployed on millions of endpoints around the world. To this, more recent disruptors in endpoint security have integrated more sophisticated approaches to analysis into endpoint security suites to lessen the risk of successful new attack variants.
- Practically all attacks leave traces in the network as they explore the network, propagate to adjacent machines and exfiltrate data. Network security vendors are providing analytic offerings to detect attack behaviors and identify endpoints participating in nefarious actions. We also see network security vendors synchronizing with endpoints in offering a more resilient security defense.

Figure 1: Top Enterprise Information Security Pain Points

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2017



- Websites are susceptible to account takeover threats, often starting with credential stuffing attacks powered by bots. It is a significant challenge to distinguish when website transactions are driven by chunks of software and when they are driven by real customers. The web behavior analytics segment aims to enhance business performance by filtering out illegitimate bot traffic. In our opinion, any enterprise generating revenue through websites without anti-bot security is leaving money on the table.

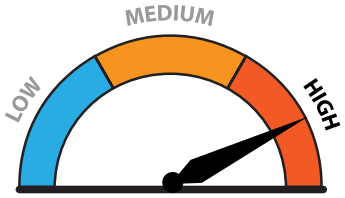
Areas where we would expect to see even further penetration of analytics include IAM. The security industry has anticipated the death of the password basically since there's been a security industry. Behavioral authentication, however, may soon bring the ability to engage analytics to identify people and endpoints more reliably than many current authentication techniques. Rather than toting tokens, the mobile phone has become factor of choice. JavaScript loaded in website login pages analyzes data such as how the phone is being held, touchpad movements, typing pressure and cadence, and location information to identify individuals. To this can be added techniques inherited from the world of network access control to better correlate the context of access and the confidence placed in both the endpoint and its user to discern when access is appropriate, and under what conditions.

SOCs are also looking more closely at analytics to help relieve burdens of triage in event escalation. There's a close relationship there with automation and orchestration, to collect the evidence that analytics can correlate to support investigations, prioritize alert clearance actions, and manage escalation and response workflows.

TREND 2: SECURITY AUTOMATION WILL MOVE CLOSER TO MAINSTREAM

Implication: *The questions many security organizations have about whether or not automation is really for them will fade as they grow from exploring incremental ways to optimize security tasks to embracing automation as the first choice for handling security processes that would otherwise be overwhelming for chronically understaffed teams. In the long run, automation and orchestration will see its fullest flowering as the programmability of infrastructure-as-code defines the evolution of IT.*

Impact to the Market



It's no secret security teams are swamped. Organizations may see hundreds, if not thousands, of alerts each day regarding actual or potential attacks, suspicious activity or new vulnerabilities, coming from both inside and outside the organization. The myriad changes to operational systems required for security can lead to a host of exposures if not resolved consistently – but IT can be overwhelmingly broad and complex. Taking concrete steps to resolve security issues requires specific actions that can have an impact in many areas. End-user productivity can be affected, while changes made to IT can affect on-premises and legacy datacenter resources, cloud providers and other third parties. The scale of change can also be daunting. Large organizations may have to deal with hundreds or thousands of both traditional and newer, more mobile endpoints – not to mention a potentially even larger body of customers, whose interactions with a company's online presence must be secure.

The security industry's investment in advanced analytics, and what is often marketed today as machine learning or artificial intelligence, all bring a great deal of promise to security management for getting a grip on this scale and complexity. Machines that can recognize and baseline patterns and spot deviations can sift through this enormous valume of noise much more quickly than people can – provided they can do a good job of recognizing legitimate issues and prioritizing them appropriately.

But what happens then? Insight is good to have, but without coupling it with response when needed, how useful can it truly be?

This question has come up again and again in multiple markets over several years, particularly those that focus on threat intelligence, attack recognition, vulnerability data, and responding to security events and incidents. The customer's demand has been the same in every case: Make this information actionable.

This demand becomes difficult to act upon without engaging automation in multiple ways – hence the investment we've seen, among enterprises as well as VCs and vendors, to equip security organizations with the automation they require to perform often highly detailed or repetitive security tasks, or implement IT change at scale in ways that consistently and predictably harmonize with IT operations and business requirements.

In general, security automation and orchestration occur on two complementary levels:

- **Automation of security tasks and processes:** At its most granular level, security automation focuses on specific actions and tasks. These are often repetitive functions that people must perform. Examples include triage of individual security events to verify malicious activity and potentially escalate investigation, or searching the environment to gether evidence of known indicators of compromise (IoCs).
- **Security orchestration:** Orchestration suggests the coordination of multiple automated tasks, linking processes together in a specific sequence or performing a variety of related actions across multiple assets. Examples here may include a sequence that involves asset inventory, classification and prioritization across an environment, then coupling findings with vulnerability assessment to coordinate and prioritize remediation. Privilege auditing can be coupled with making changes to access management systems in response to changing personnel or business requirements gathered from ERP or HR systems, while the ability to detect and intervene at multiple phases of a complex attack can improve and enhance response to more sophisticated threats.

These examples highlight the segment within the security market that has emerged to serve the multidimensional aspects of security automation. The impact of this trend is expected to be high, affecting multiple market segments, for two reasons: first, the many systems that security automation and orchestration tools are likely to touch to coordinate complex actions, and second, the muitiple segments in which automation has already appeared beyond tools purpose-built to ease demands on security teams – a trend we expect to continue and grow.

The prior art of runbook automation in IT service management is one such example. In other domains, firewall rules deployment automation and validation has long been central to firewall management systems that embrace multiple vendors and rule formats, while endpoint containment has been a function of network access control (NAC) from its beginnings. Risk-based authentication can up the ante on having end users prove their identity when potential fraud or suspicious activity is detected, while the automation of provisioning and self-service at scale plays a role in today's emerging IAM systems that target the enrollment of millions of consumers. Even bug bounty platform providers see automation as a primary capability, since, on behalf of their clients, they must take in hundreds or thousands of potential vulnerability submissions from researchers seeking to find exploitable defects in IT before attackers do.

One key advantage tools purpose-built for security automation and orchestration may have over other technologies is the role they play in closing gaps. Within technology segments, products often leave it up to people to 'do something' with evidence gathered, or controls that can reconfigure and mitigate exposures – even if that 'something' turns out to be a repeatable process that could just as well be automated. Security automation and orchestration can also close gaps between technologies – more closely linking vulnerability intelligence with tools to assess the environment, followed by remediation that engages systems management platforms, for example.

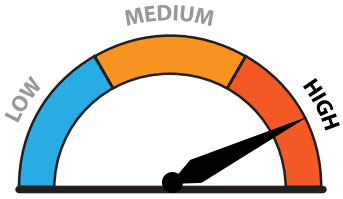
We expect the use cases for security automation and orchestration to continue to grow. We have already seen – and covered – several acquisitions in the space (such as *IBM's of Resilient Systems*, *FireEye's of Invotas*, *Microsoft's of Hexadite* and *Rapid7's of Komand*) and we expect to see more, considering the worthwhile fish still in the sea. Because of the way it complements security information with follow-up action, we expect SIEM vendors to continue to show interest. Other incumbent security leaders may see the value of automation tools for expanding their penetration of security operations, as may those in close adjacencies, such as systems and IT service management platforms. A wide range of service providers, from MSSPs to telcos already familiar with large-scale provisioning, may also find the space attractive.

Ultimately, automation is integral to the evolution of IT itself. It is a central aspect of DevOps environments, while cloud platforms are often predicated on the programmability of infrastructure, where thousands of instances of a single server image or container may be provisioned and retired within seconds, and where vulnerability remediation can be accomplished offline, without disrupting production operations. Today's security automation tools can certainly integrate with the tools that compose and configure 'new IT' as needed. However, as DevOps tools and processes continue to play a role in defining the evolution of increasingly invisible infrastructure, in the long run we expect to see a large part of automation for the sake of security ultimately become a subset of automation that designs, creates, deploys and operates reliable, resilient IT.

TREND 3: NETWORK SECURITY VENDORS WILL FACE THE IDENTITY-AWARE PERIMETER

Implication: *Network-based security has formed the backbone of most firms' security programs for decades and been a primary means of controlling access to corporate resources. Yet mobility, cloud and IoT have eroded the traditional perimeter to the point that network-based controls have become less and less relevant as the type and volume of 'things' we need to access has grown exponentially. While the first strategic gambit for network security vendors was to address the endpoint, the second tectonic shift could be to inject identity into their overall stacks to stay relevant.*

Impact to the Market



In our last two Trends in Information Security reports, we wrote about the coming *convergence of cloud security*, and also about the need for the *'big boys' in security* to take measures to more effectively protect cloud-based resources. Many have done so, largely via M&A, and largely in the form of what have come to be known as cloud access security brokers (CASBs): *Microsoft/Adallom*, Blue Coat (*Elastica*, *Perspecsys*), Symantec (*Blue Coat*), Cisco (*CloudLock*), Oracle (*Palerra*), Forcepoint (*Skyfence*), just to name a few. And we still think there are plays to be made as vendors such as Barracuda, Check Point, Fortinet and Juniper have little direct cloud security presence.

While M&A activity has focused largely on security for SaaS applications, we expect a combination of M&A, internal development and partnerships to break down silos and move the industry toward a broader conception of 'cloud security 2.0.' This will entail several potential areas of convergence, including a blurring of the lines between security for IaaS, PaaS and SaaS, as well as a broader range of security controls (discovery, DLP, threat protection, etc.) and architectures (API, proxy, agent, etc.).

But a third area of convergence could involve a blending of CASB (and even potentially secure web and email gateway vendors) with identity-related features, such as the multi-factor authentication (MFA), single sign-on (SSO) or provisioning functionality commonly delivered by identity-as-a-service (IDaaS) vendors. As an example, we have already seen extensive partnering between CASB and IDaaS vendors, which could serve as a signpost for what cloud security could look like several years down the road.

As such, while some network security vendors have made plays for CASB assets, few have identity-related capabilities. It follows that network-focused security incumbents could also become active on the identity, either independently or in conjunction with existing CASB assets.

For years, the term 'access control' has been somewhat confusing. On one hand, the term was used to apply to identity-related tools such as authentication/MFA and SSO, and authorization/access governance. However, access controls could also be applied at the network level, with firewalls and VPNs enforcing access to networks, initially by IP address or port, and the dreaded access control lists. But firewalls were never 'identity-aware': Imagine an airport security guard asking where someone is coming from and where they are going, but never bothering to look at their ID, let alone check inside their luggage.

In addition to a growing array of devices that will require access to resources, the types of users that require access are changing as well. No longer is it enough to just monitor access by internal employees to internal resources; access control systems have to take into account a growing contingent of third-party vendors, consultants, outsourcers, hosting providers and, increasingly, customers. The latter introduce a whole set of new problems that traditional IAM offerings can't handle (such as scalability, elasticity, customer experience and data privacy).

In addition to cloud, mobile and IoT, another key driver of this trend is that a staple of many network security vendors, the trusty old VPN, is in the process of becoming less relevant thanks to new developments like Google's BeyondCorp, and commercial interpretations of BeyondCorp such as Duo Security's Duo Beyond, the new Zscaler Private Access from Zscaler and perhaps even Akamai's *recent acquisition of Soha*. The latter can collectively be referred to as 'zero-trust networking' that at a high level does away with the traditional concept of 'trusted' and 'untrusted' networks and allows employees, third parties, vendors and auditors to access applications without having to set up a VPN or modify firewall rules. Instead, access policies are based on information about the user, their device, the context from which they seek access, the nature of access sought, and the sensitivity of access targets – and not simply on whether or not the user can become an endpoint on a specific (and perhaps flat) network with little or no additional policy control.

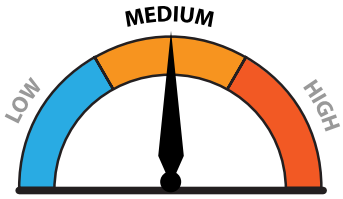
To date, there has been a lot of identity-related M&A activity, and we think it is just a matter of time before incumbent network security vendors look to address identity more directly. And as we have seen with the CASB space, once one vendor blinks, the others could quickly follow suit. The same can be said for 'legacy' IAM suite vendors that have been happy to milk their existing customer bases for recurring maintenance revenue and have yet to develop an answer for cloud-based resources.

However, with IDaaS, CASB and consumer IAM assets carrying potential valuations in the billions (see Okta, Netskope and ForgeRock for examples), both incumbent security vendors and legacy IAM players may be getting nervous about their ability to maintain a seat at the table – at least without forking over big sums for an asset with an exorbitant price tag.

TREND 5: COMPLIANCE WILL REASSERT ITS DOMINANCE

Implication: *Even if it's not what security teams would rather do, compliance has always driven spend. With GDPR just around the corner, its short-term impact will be keenly felt in Europe and beyond. But is regulation having the intended effect? Despite the advent of increasingly punitive regulation, the number of records breached in the last two years has skyrocketed.*

Impact to the Market



We have seen the growing prevalence of analytics and automation in security, as well as the downside that accompanies any new trend: hype that makes it difficult to discern what is really making progress. The rise of pervasive intelligence and an increasingly digital experience for consumers portends an even greater problem, particularly for individuals: the impact on privacy.

Regulation has been policymakers' preferred lever to force businesses to place the interests of individuals before corporate gain – which means that compliance has long been a primary driver of security spending. For enterprises that would rather spend their IT budgets on things with tangible ROI – read: most enterprises – compliance has served as a fatherly prod for companies to do what they should be doing rather than spending on the latest bright and shiny marketing tool or user interface. It should be no surprise, then, that public security vendors tend to generate the bulk of their revenues from the most-regulated sectors: financial services (Sarbanes-Oxley [SOX]), healthcare (HIPAA), retail (Payment Card Industry [PCI]) and government (Federal Information Security Management Act [FISMA]).

However, in recent years, there has been a barely perceptible sense that our compliance efforts haven't been doing enough, prompting a subtle shift toward going beyond just checking off compliance boxes and closer to pursuing industry best practices. Indeed, many of the most noteworthy breaches that have taken place over the past few years have likely happened to vendors that had hit their compliance benchmarks, most notably Target. More recently, statements made by the former CEO of Equifax (who resigned following that company's high-profile data breach) shocked security professionals, when he seemed to lay a strategic security failure on the shoulders of a single IT worker. This despite the fact that Equifax plays in financial services – one of the most heavily regulated industries when it comes to information security.

Yet there is emerging evidence that compliance is resurging as a driver for enterprise security priorities and spending (see Figure 3).

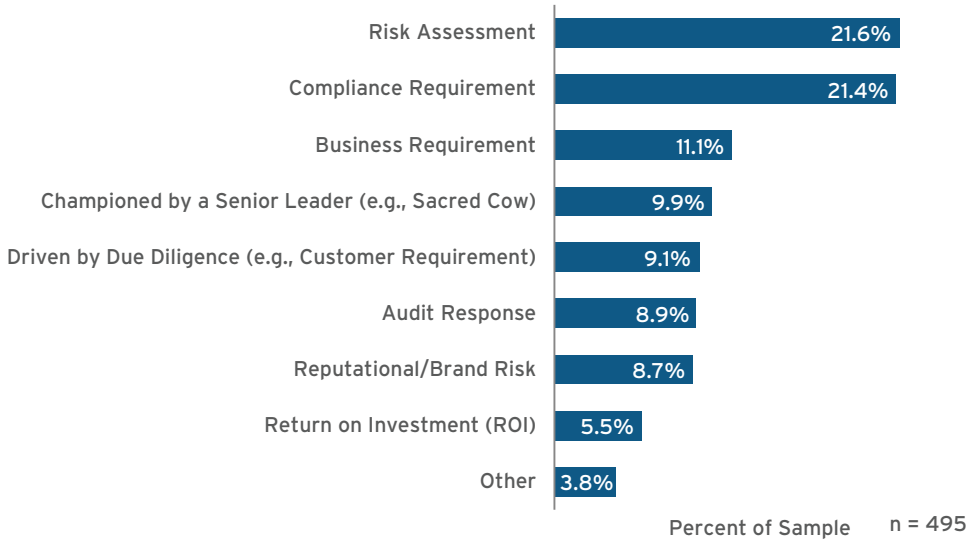
A primary focus of many regulations relevant to information security focus on protecting sensitive data. In Europe, GDPR will enter into force in May 2018, and with it, enterprises will hustle to get their compliance ducks in a row, while vendors have already lined up to make the most of the opportunity, as evidenced by a torrent of GDPR-targeted marketing campaigns. And while many compliance mandates are vague in terms of both prescriptions and penalties, GDPR, like PCI before it, has real 'teeth' in the form of hefty fines for non-compliance: up to 4% of global turnover or €20m in fines, whichever is higher, for the most egregious violations.

As SOX arguably gave rise to the birth of the data loss prevention (DLP) industry in the mid-2000s, will we see a similar resurgence in spending from the likes of GDPR and others? The EU-US Privacy Shield arrangement, which took over where the collapse of Safe Harbor left off, should offer GDPR coverage for US organizations able to self-certify their handling the data of Europeans for the time being – but its future is far from certain. The agreement is subject to annual review, and the EU's watchdogs on the Article 29 Working Party responsible for oversight of EU data privacy policy have made no secret of the dim view they take of US data collection practices, particularly when it comes to the potential for surveillance in the name of 'national security.' With the first Privacy Shield review now in the rearview mirror, expect vendors to respond if requirements on US organizations handling European data change in 2018.

We have already seen such a phenomenon happening on a smaller scale with respect to the risks posed by third-party contractors and suppliers. In the US, recent regulations from the Office of the Comptroller of the Currency, the PCI Security Standards Council, NIST's Cybersecurity Framework, HIPAA Omnibus and the Consumer Financial Protection Bureau (CFPB) have all added third-party vendor risk to their purview and arguably given birth to a cottage industry of new security vendors focused solely on third-party vendor risk management.

Figure 3: Key Determinants in Approval for Top Information Security Projects

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2017



While a few vendors have popped up with an exclusive privacy focus, most of the activity has been by existing security vendors looking to jump on the GDPR bandwagon and boost their toplines. Privacy laws will also likely continue to drive vendors in customer IAM, many of which have developed products – and market messages – focused squarely on helping organizations walk the fine line between mining a treasure trove of personal data for targeted marketing and maintaining consumer privacy.

Unlike other compliance mandates, however, GDPR is inextricably bound with broader societal issues around user privacy, as the well-known 'affaire Snowden' and similar incidents involving the FBI were a driving force in the passage of GDPR and updates to other similar regional privacy mandates such as APPI in Japan and PIPEDA in Canada.

There is also a palpable tension between security and privacy, resulting in a yin-yang that was on clear display in the highly public and emotional controversy between Apple and the FBI that attempted to balance user privacy on one hand, and the needs of law enforcement on the other. Another often overlooked manifestation of this tension is felt by security vendors that operate globally. Much of the telemetry that security vendors rely on for fine-tuning their products and improving the accuracy of detection techniques uses data that may run afoul of certain regional mandates. In effect, one person's IOCs are another's PII/PHI/PCI.

Are trends forcing the data privacy conversation in the US as much as they have in Europe? There are different histories in play, of course: World War II and a divided postwar continent has made Europe far more sensitive to the abuse of personal privacy, whereas the free market ethos continues to prevail in the US. A pronounced anti-regulatory bent is a sub-theme of the conservative governments currently in power on both English-speaking sides of the Atlantic – yet, ironically, the absence of national privacy regulation in the US has led to a highly fragmented patchwork of rules at both the federal and state levels that greatly complicate compliance for everyone.

But is this complex of regulation doing its job? Before 2016, the Data Privacy Rights Clearinghouse had tallied a total of more than three billion records exposed in all the breach types among all the organizations it had tracked from 2005 onwards. By late 2017, that figure had tripled to nearly 10 billion. Estimates in the Yahoo! breach alone now include all three billion users since the initial tally was revised upward in October 2017.

But don't expect the blowback from those incidents to change the nature of regulation in the US anytime soon. Pervasive intelligence and digital experience are already trends that often pull opposite to the interests of privacy. Unfortunately, we feel it will take one or more major incidents with more of an impact than any single breach to date to bring about meaningful change in more widespread privacy protection.