RISKSENSE®

Cyber Risk Management: A New Approach to Responding to Complex Threats

FEATURING RESEARCH FROM FORRESTER

The Top Security Technology Trends To Watch, 2017

Cyber Risk Management: A New Approach to Responding to Complex Threats

INTRODUCTION

Over the last few years, cyber threats have emerged as one of the most significant business risks facing organizations. While companies spend huge sums of money every year to maintain a security perimeter designed to fend off cyber and insider threats, daily reports of new data breaches are raising doubts about the effectiveness of these investments.

IN THIS DOCUMENT

A DYNAMIC THREAT LANDSCAPE

Organizations face an uphill battle, as the attack surface they have to protect has grown significantly and is expected to balloon even further. While it was sufficient in the past to focus on network and endpoint protection, nowadays applications, cloud services, mobile devices (e.g., tablets, mobile phones, Bluetooth devices, and smart watches), and the Internet of Things (e.g., physical security systems, lights, appliances, as well as heating and air conditioning systems) represent a broadly extended attack surface.

This “wider and deeper” attack surface only adds to the existing problem of how to manage the volume, velocity, and complexity of data generated by the myriad of IT and security tools in an organization. The feeds from these disconnected systems must be analyzed, normalized, and remediation efforts prioritized. The more tools, the more difficult the challenge. And the broader the attack surface, the more data to analyze. Traditionally, this approach required legions of staff to comb through the huge amount of data to connect the dots and find latent threats. These efforts took months, during which time attackers exploited vulnerabilities and extracted data.

Rather than adding more tools, organizations need to implement a new, more efficient enterprise security model.

AUTOMATION AND HUMAN-INTERACTIVE INTELLIGENCE

Breaking down existing silos and automating traditional security operations tasks with the help of technology has therefore become a force-multiplier for supplementing scarce cyber security operations talent. In this context, the use of human-interactive machine learning engines can automate the aggregation of data across different data types; map assessment data to compliance requirements; and normalize the information to rule out false-positives, duplicates, and enrich data attributes.

Unfortunately, a significant portion of information security resources are consumed by data gathering and aggregation processes. This is one of the biggest limitations when it comes to driving down time-to-remediation and predicting threats before they come to fruition. Another challenge involves creating context around security data, so it can provide actionable insight. To achieve this, data needs to be correlated with its business criticality or risk to the organization. Without a risk-based approach to security, organizations can waste valuable IT resources mitigating vulnerabilities that in reality pose little or no threat to the business. Furthermore, security data needs to be filtered to just the information that is relevant to specific stakeholders' roles and responsibilities. Not everyone has the same needs and objectives when it comes to leveraging security data.

THE NEW ENTERPRISE SECURITY MODEL: CYBER RISK MANAGEMENT

In this context, intelligence-driven cyber risk management is often seen as a clear path for organizations to operationalize cyber security practices, breaking down silos, and enhancing security operations tasks through automation.

FIGURE 1: Cyber Risk Defined

Cyber risk is made up of many factors including compliance posture, threats, vulnerabilities, reachability, and business criticality. For each of these, organizations collect huge volumes of data that they need to aggregate, normalize, and then assess for their impact on the business. Fortunately, new technology – cyber risk management – is emerging that helps not only aggregate internal security intelligence and external threat data, but more importantly correlates these data feeds with its business criticality or risk to the organization. The end result is automated, contextualized security metrics that align with business objectives.

Figure 2 below illustrates this new enterprise security model, which is labeled intelligence-driven cyber risk management.

FIGURE 2: The Pro-Active Cyber Risk Management Concept

Besides the operational advantages that cyber risk management brings to the table, it also propagates better collaboration among otherwise siloed stakeholders across the organization, ranging from the board, C-suite, business stakeholders, as well as security and IT operations teams to internal / external auditors.

RiskSense provides a new, pro-active approach to cyber security risk management that enables enterprises and government to reveal cyber risk, quickly orchestrate remediation, and monitor the results. This is done by unifying and contextualizing internal security intelligence, external threat data, and business criticality across a growing attack surface.

RiskSense offers a unique value proposition as it serves both as a force-multiplier for increasingly scarce cyber security operations talent, as well as providing cyber risk management visibility and best practices for the C-Suite. By leveraging RiskSense's cyber security risk management solution, organizations can significantly reduce risk, reduce costs, improve response readiness, and increase risk-posture visibility.

The Top Security Technology Trends To Watch, 2017

Tools And Technology: The S&R Practice Playbook

by Merritt Maxim, Jeff Pollard, Amy DeMartine, Nick Hayes, Joseph Blankenship, Josh Zelonis, and Andras Cser

April 26, 2017 | Updated: May 3, 2017

Why Read This Report

Each year, analysts from across Forrester's security and risk (S&R) research team draw insight from hundreds of client questions, vendor briefings, and consultations; the 40-plus research projects we complete each quarter; and perspectives from key industry events such as the RSA Conference to answer two of our clients' most frequent questions: 1) "What security innovations are emerging?" and 2) "What disruptive technologies should I pilot?" This report cuts through hype and helps you assess the most important developments in the next 12 months.

Key Takeaways

Threat Intel Is Finally Maturing

A few years ago, threat intel and security analytics quickly emerged as a hot new cybersecurity category. But this category quickly lost luster as enterprises became confused by vendors' broad array of marketing jargon and mixed intelligence jargon. Many vendors have taken this input to heart and are improving their threat intelligence messaging and positioning to help S&R pros better distinguish between services, including the use of digital risk monitoring as a new descriptive terminology for key functionality.

Machine Learning, Analytics, And AI Are The New Buzzwords

At the 2017 RSA Conference, we witnessed an onslaught of vendor messaging latching onto terms such as machine learning, security analytics, and artificial intelligence. These areas hold tremendous promise to solve security challenges, so it's no surprise that vendors are messaging to them; however, current vendor product capabilities in these areas vary greatly. This places a premium on verifying that vendor capabilities match their marketing messaging to ensure that any solution you select can deliver on the value promised in the marketing brochures.

The Top Security Technology Trends To Watch, 2017

Tools And Technology: The S&R Practice Playbook

by Merritt Maxim, Jeff Pollard, Amy DeMartine, Nick Hayes, Joseph Blankenship, Josh Zelonis, and Andras Cser

with Stephanie Balaouras, Christopher McClean, Laura Koetzle, Salvatore Schiano, Trevor Lyness, and Peggy Dostie

April 26, 2017 | Updated: May 3, 2017

Table Of Contents

Related Research Documents

Predictions 2017: Cybersecurity Risks Intensify

The Top IAM Trends From The RSA Conference 2017

Top Seven Recommendations For Your Security Program In 2017

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

FORRESTER®

© 2017 Forrester Research, Inc. Unauthorized copying or distribution is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

As The Threat Landscape Expands, So Do The Vendors And Solutions

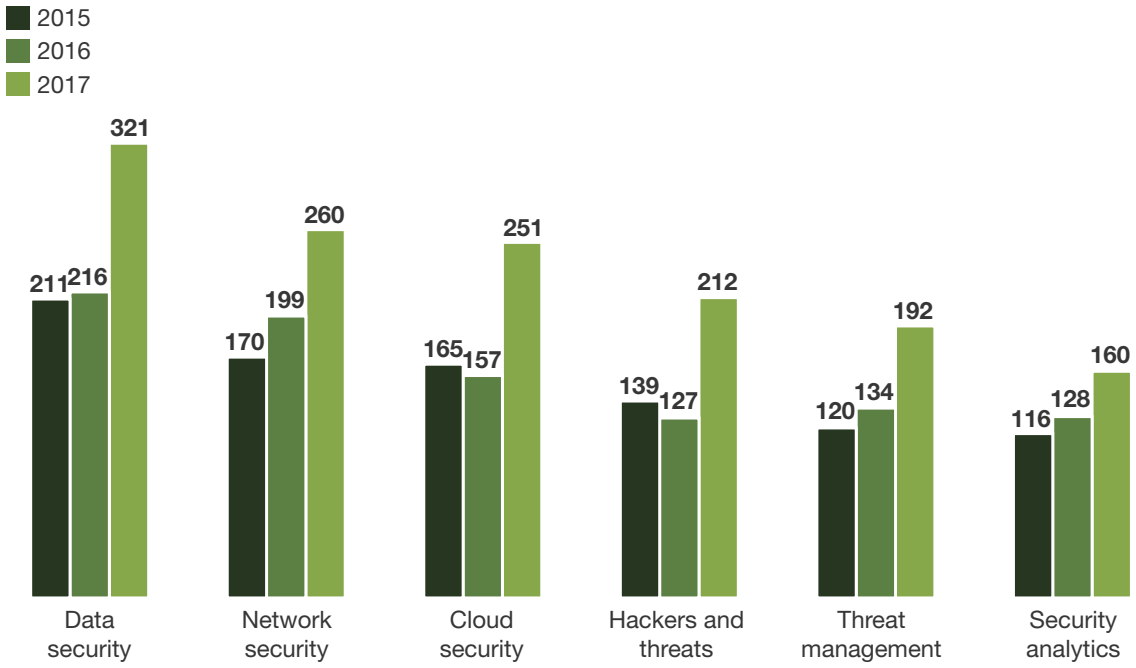
To help S&R pros prepare for the future; navigate through the ever-present security buzzwords like AI, machine learning, and analytics; and defend against a broad spectrum of threat vectors; the Forrester S&R research staff examined the 14 most important cybersecurity trends based on our collective observations from the 2017 RSA Conference (RSAC). There are two overarching trends worth noting:

- **The threat landscape is expanding and mutating once again . . .** Security threats continued to dominate the headlines in 2016. In addition to the highly public Yahoo breaches, which affected at least a billion customer records, we also witnessed a large-scale DDoS attack against DNS operator DYN that, using a botnet of compromised IoT devices, disrupted internet availability. The continued emergence of new threat vectors, combined with the usual plain-vanilla data breaches via social engineering or credential theft, reflect the reality that, despite the broad range of security defenses available today, most S&R pros struggle to protect their organizations.
- **. . . the industry is responding with a flood of new startups and solutions.** In response to the expanding threat landscape, we also see an ever-expanding vendor landscape trying to protect and defend against all these threats. At the 2017 RSAC, there were 600-plus exhibitors, up 56% since 2014, with an exhibitor waiting list that is rumored to be several hundred vendors long. That RSAC does not represent the entire cybersecurity industry further demonstrates the immense breadth and depth of the landscape. But when 300-plus exhibiting vendors self-identify in the data security category (up 50% over 2016), you realize that finding the optimal security solution for your organization is becoming more and more challenging (see Figure 1 and see Figure 2).

FIGURE 1 Top Vendor Categories At RSA Conference, 2012 To 2017

2012	2013	2014	2015	2016	2017
Data security	Data security	Cloud security	Data security	Data security	Data security
Compliance management	Application security	Data security	Network security	Network security	Network security
Authentication	Enterprise security management	Network security	Cloud security	Cloud security	Cloud security
Enterprise security management	Compliance management	Mobile security	Hackers and threats	Threat management	Hackers and threats
Cloud computing	Mobile device security	Authentication	Compliance	Security analytics	Threat management

FIGURE 2 Breakdown Of Top Vendor Categories At RSA Conference, 2015 To 2017



NO. 1: IOT-SPECIFIC SECURITY PRODUCTS ARE EMERGING, BUT IT REMAINS A DIFFUSE SEGMENT

As the adoption of consumer and enterprise IoT applications continues to grow, so does the concern from S&R pros of its potential to increase the enterprise's attack surface. Every security conference from RSA to Black Hat seeks to raise awareness of the dangers associated with IoT and the risks they could pose to organizations.[1] However, many questions arise over what to worry about when it comes to IoT, how to quantify the risk, and how to ultimately address the threat. The Mirai botnet in October 2016 raised public consciousness about IoT security concerns, and that incident appears to be giving some momentum to this space. At the RSAC, many vendors were using Mirai as an example of the threats and how to address them, but there is still a wide and growing range of vendors going after this space.

› **What you should know:** The importance of IoT is clear: It will greatly change how enterprises serve their customers due to the improvements it provides for areas like operational logistics and customer engagement. However, the types of data these IoT devices create, collect, or distribute are often rife with sensitive intellectual property or customer data that would be damaging if compromised. Additionally, some connected devices, such as cars and machinery, could have life-threatening effects if tampered with.

- **What you should do about it:** Enterprises will continue to assess and then roll out IoT applications into the enterprise environment. However, the market to address IoT concerns is still underdeveloped. Securing IoT will require people and process as much as technology. S&R pros need to be a part of the IoT initiative and extend security processes to encompass these IoT changes. For tools, seek solutions that can inventory IoT devices and provide full visibility into the network traffic operating in the environment.[2] Also, S&R pros need to enable strict access control and ensure that data security applies regardless of device or node.
- **Vendors to watch:** Arxan, Cisco, Covisint, Entrust Datacard, Gemalto, HPE, IBM, Kaspersky Lab.

NO. 2: ENCRYPTION OF DATA IN USE BECOMES PRACTICAL

As IoT devices and nodes generate vast amounts of sensitive data, much of it will ultimately reside in back-end systems and databases — which increasingly are in the cloud. Encryption is a core technology for control in our efforts to protect data and enforce privacy and data protection policies.[3] Encryption of data at rest and data in transit have become easier to implement with each passing year, but many S&R pros and their colleagues still struggle to overcome challenges like data classification and key management. But encryption of data in use hasn't been practical at any sort of scale — until now. This couldn't come at a better time, because if you don't need to decrypt the data to use it, you never need to decrypt it at all — which means it's only vulnerable to attackers once (when you initially create or receive it). Thus, you can use this encrypted data wherever you like, including in the public cloud, even if it's what Forrester considers "radioactive" data — intellectual property plus personal data subject to regulation.[4]

- **What you should know:** Homomorphic encryption, a system in which computations performed on ciphertext produce identical results to those carried out on plaintext, has been known in theory since 1978 and technically feasible since at least 2009. This means that you can keep data encrypted as you query, process, and analyze it. For example, a retailer could encrypt a customer's credit card number at first use and keep it to use for future transactions without fear, because they'd never need to decrypt it. So why isn't everyone already doing this? Because, until recently, it was far too slow for commercial use. However, researchers then managed to reduce the processing time from 30 minutes per operation (2011) to 2 seconds (2014).[5] And we're now seeing the first commercially viable homomorphic encryption implementations come to market.
- **What you should do about it:** If you have data you need to protect in use (which includes the vast majority of firms), investigate homomorphic encryption implementations now. Remember, however, that homomorphic encryption isn't perfect. For example, if an attacker gains full control of your application, he can run it on your encrypted data and get the same answers you can — which may allow him to reverse-engineer his way to the data itself.
- **Vendors to watch:** Baffle, EnVeil, HPAtalla, IBM, Inpher, Kryptnostic, Microsoft, Stealthmine.

NO. 3: THREAT INTELLIGENCE VENDORS CLARIFY AND TARGET THEIR SERVICES

Encryption can reduce the impact of a cyberattack or breach, but security teams must still try to prevent these incidents in the first place. Good threat intelligence can give you enough advanced warning of attacks on the horizon to adjust security policies and controls and address vulnerabilities. However, a major challenge in the threat intelligence market has been trying to decipher vendors' broad array of marketing jargon and mixed intelligence jargon, confusing to even experienced intelligence pros. Fortunately, we're seeing a shift in threat intelligence messaging as vendors aim to improve positioning and help customers better distinguish between services. For example, some vendors like Digital Shadows, RiskIQ, and ZeroFOX are embracing our concept of digital risk monitoring as a complementary category of the massive "threat intelligence" vendor market.[6] This trend of vendors using more targeted, specific messaging to articulate their capabilities and value is in turn helping customers avoid selection frustrations and develop more comprehensive, and less redundant, capabilities.

- **What you should know:** There's not a single threat intelligence solution that fits all. Requirements for the type of intelligence you should collect will vary by vertical, size, maturity, channel domain, and more. You need a strategic collection approach that will provide you the intelligence you need to properly inform security spend and improve detection rates for your organization. Discussions about the deep and dark web may sound mysterious and maybe even a bit ominous, but what you really care about is the information collected from these sources. Expect more vendors to follow the example of Recorded Future, which has shifted its messaging to highlight the types of data it provides to the customer, away from traditional discussion of how the information was sourced.
- **What you should do about it:** Start by developing a collection strategy, or shopping list, before approaching providers so you can better assess the intelligence sources they provide and achieve a mature level of coverage. Inform your collection strategy based on internal factors such as intelligence processing capabilities and security operations metrics while tracking external factors such as exploitation trends as another source of information. If you're unsure how to develop such a strategy, consider hiring a resource to oversee your threat intelligence capability or utilize third-party resources to assist you before investing in data sources.
- **Vendors to watch:** Digital Shadows, Flashpoint, Intel471, Proofpoint, Recorded Future, RiskIQ, ZeroFOX.

NO. 4: IMPLICIT AND BEHAVIORAL AUTHENTICATION SOLUTIONS HELP FIGHT CYBERATTACKS

Of the firms that suffered at least one breach at the hands of external threat actors, 37% report that use of stolen credentials was a means of attack.[7] Using password-based, legacy authentication methods is not only insecure and damaging to the employee experience, but it also places a heavy administrative burden (especially in large organizations) on S&R professionals. This is because S&R pros must constantly manage a large policy rule set that identifies which users and devices are good and bad.

- **What you should know:** There are two facets to this trend. First, Forrester sees identity and access management (IAM) solutions incorporating a variety of data sources such as network forensic information, security analytics data, user store logs, public human intelligence feeds (e.g., Verizon Data Breach, IBM X-Force), and shared hacked account information, into their IAM policy enforcement solutions. Second, Forrester sees authentication solutions using navigational clickstream analytics, device location and sensor data, and mouse and touchscreen movement attributes to build normal behavior baselines for users and devices, which the solutions can use to detect anomalies. This helps S&R professionals: 1) identify internal threat and lateral movement; 2) ensure that only the real administrators use privileged credentials on privileged sessions; and 3) ensure that the right users authenticate to mobile devices, applications, and data assets.
- **What you should do about it:** Verify vendor claims about automatic behavioral profile building and demand demonstrable answers to the following questions: 1) Does the solution really detect behavioral anomalies? 2) Does the solution provide true interception and policy enforcement features? 3) Does the solution integrate with existing SIM and incident management solutions in the SOC? and 4) How does the solution affect employee experience? Vendors often underestimate the impact of the solution to end users.
- **Vendors to watch:** Allure Security, Behaviosec, Biocatch, NuData Security, UnifyID.

NO. 5: ALGORITHM WARS HEAT UP — MY DATA SCIENCE CAN BEAT UP YOUR DATA SCIENCE

When virtually every security vendor makes the claim that they're using artificial intelligence or machine learning for detection, security decision makers are left shaking their heads, trying to figure out what's real and what's not. Conversations that begin with "We have the best data science" are also not helpful. Vendor overhype about artificial intelligence and machine learning capabilities has led to an arms race of claims about data science "automagically" addressing security problems.

- **What you should know:** Data science has been part of cybersecurity for as long as there has been a category called cybersecurity. Machine learning and artificial intelligence do have roles to play in security, but they are not a panacea for the prevention of all cyberattacks. They are useful tools for recognizing patterns in large quantities of data and informing decision making as a supplement to rules-based or signature-based detection.
- **What you should do about it:** Ignore vendor claims about data science, and concentrate on use cases. Look for vendors that solve the problems you're dealing with and have referenceable customers in your industry. If a vendor claims that their solution recognizes unknown malware or detects malicious user behavior using data science, challenge them to prove it, preferably on your own data.
- **Vendors to watch:** Any vendor claiming to have artificial intelligence, machine learning, or intelligent algorithms. That's everyone from Avata Intelligence to WebRoot.

NO. 6: SECURITY AUTOMATION AND ORCHESTRATION IS GAINING TRACTION

Having long shied away from automation, S&R pros are now slowly approaching the idea that taking some automated actions and having orchestrated processes may be a good thing. Security teams struggle with investigating all of the alerts they receive, investigating incidents, and responding to threats quickly. Security automation and orchestration (SAO) promises to automate repeatable, manual tasks, giving analysts more time for analysis and higher-value work. Processing more alerts, investigating more incidents, and automating some remediation processes, therefore, will allow faster response.

- **What you should know:** SAO is still in its infancy but gaining acceptance. Current SAO solutions act as an orchestration layer, allowing different security technologies to talk to each other. Users can create workflows and playbooks for different situations, then automate parts of the process that don't require a human analyst. Automated remediation without analyst interaction will depend on confidence level.[8] Before we get to a point where we trust the machines to make decisions rather than just give advice, they'll have to prove themselves.
- **What you should do about it:** Before considering SAO, assess the maturity of your processes, document them, and work to standardize across the security team. Established security teams with mature processes will get more benefit from SAO. After all, automating poor processes will only allow you to make bad decisions faster.
- **Vendors to watch:** Cybersponse, Demisto, FireEye, IBM, Hexadite, Phantom, Siemplify, Swimlane.

NO. 7: GESTURE-CONTROLLED VR DASHBOARDS AND SIMS THAT SPEAK MAKE SECURITY TANGIBLE

There is no doubt that S&R pros need a different set of dashboards to measure and analyze security data, allowing them to kick off security actions. While there have been some incremental improvements to enhance the dated "events over time" spark charts and "red/yellow/green" alerts security practitioners are used to, not all interfaces are taking baby steps — a few technology vendors are challenging security vendors to vault forward and begin using the latest in bleeding-edge human computer interfaces.

- **What you should know:** The barrier between general computing innovation and security technology has disappeared. It took time for security to catch up to mobile, and S&R pros still battle with control over some workloads, particularly as hybrid becomes the norm, but the interface security leaders use has finally started to change as well. We saw not only demonstrations of gesture-controlled VR dashboards but real-world use of these dashboards at RSAC 2017. Intelligent assistants and voice recognition also announced themselves on the show floor as security information management (SIMs) shouted "Red alert!" in addition to lighting up.
- **What you should do about it:** Today's SOC analysts' time is limited, and they are forced to separate time between analysis and action. SOC analysts must open several user interfaces, perform analysis, make decisions, and then execute a series of commands as discrete steps, and

as a result, they suffer cognitive penalties due to forced, rapid context switches.[9] The future SOC analyst will use VR and gesture control to analyze an event with 3D links in virtual reality while commanding an intelligent assistant to capture forensic data from a host — simultaneously. For the first time, S&R pros will be able to analyze and take action in near real time. With faster analysis and decision making, combined with automation and orchestration, CISOs should set expectations that security operations must move faster.

› **Vendors to watch:** Landrian Networks, ProtectWise, Splunk.

NO. 8: THE TRAINING AND AWARENESS VERSUS TECHNOLOGY DEBATE RAGES ON

While we invest in sophisticated tools for threat intel, authentication, and automation, many security teams and vendors still see value in addressing the human element of security. On the one hand, security training and awareness reinforces a firm's "human firewalls," reducing the chances that employees succumb to phishing and social engineering attacks; on the other hand, human firewalls will always contain flaws and a CISO could better spend these resources hardening other security defenses. Both arguments have merit, but ultimately, Forrester advocates for security awareness and training investment for three main reasons: 1) The significant percentage of cyberattacks and breaches stemming from human error or user manipulation makes any effort to reduce these odds a meaningful one; 2) security training should be viewed as one element of a broader cyber risk mitigation strategy, not the silver bullet; and 3) it's a compliance requirement for many firms already, so S&R pros should make it as effective as possible.

› **What you should know:** Fifty-six percent of firms that suffered at least one breach did so at the hands of external threat actors. Of these firms, 37% report that a breach was carried out via user interaction such as replying to phishing scams, clicking on malicious links, or downloading malicious email attachments.[10] These breaches result in critical financial, operational, regulatory, strategic, and reputational losses for organizations of all sizes. According to the FBI, the exposed monetary loss from business email compromise (BEC) scams within a two-year period amounted to $3.1 billion — with a 1,300% increase since January 2015.[11] Whether it's BEC or another issue like ransomware, IP loss, system downtime, or negative media coverage, it's critical to arm your workforce with information and techniques to prevent these events from occurring.

› **What you should do about it:** Accept that a softer initiative like security awareness still has a place alongside other technical controls. Secondly, realize that, unless you have a communications background, you need help with the education and messaging components. This can be in the form of partnerships with other internal teams like HR, or soliciting security awareness tools that generate year-round programs with their own content and can measure your training efforts with phishing simulations and interactive dashboards. However, don't be fooled by marketing collateral that positions these tools as "antiphishing" or "antiransomware" solutions. They are still eLearning solutions at their core, meaning the best solutions are those that offer creative and engaging content, not superfluous simulators and intelligence.

› **Vendors to watch:** AstraID, BeOne Development, KnowBe4, MediaPro, Popcorn Training, PhishMe, SANS Institute, The Security Awareness Company, Security Innovation, Terranova WW Corporation, Twist & Shout Communications, Wombat Security.

NO. 9: APPLICATION SECURITY GETS A CONFUSING RESURGENCE WITH DEVOPS AND CONTAINERS

The importance and criticality of application security has received a new boost with the advent of development and operations (DevOps). Now security teams can automate their security testing and empower developers to create secure applications like never before. Attaching themselves to this trend, application security vendors have created marketing messages that confusingly all say that their products enable secure applications with DevOps. In addition to the confusion about where exactly these application security products fit in the software delivery life cycle, and what exactly their sweet spot is, many vendors also claim that they solve container security also in the context of DevOps.

› **What you should know:** No vendor has of yet created a single product that truly enables application security with DevOps. You will continue to need a layered approach. This applies especially to vendors in the container security space who each claim they solve all of container security. These vendors are really point products solving a particular problem the new container architecture exposes.

› **What you should do about it:** Ask probing questions about what the application security solution really does to increase application security in the software delivery life cycle. The answer could be as simple as the vendor added a Jenkins integration to a deep integration into the developer's IDE. Either way, with the emergence of DevOps, it's more important than ever to partner with your developers to evaluate application security products jointly. These products must integrate into your developer's process and existing tools or they will not be adopted.

› **Vendors to watch:** Aqua Security, Illumio, StackRox, Symantec, Synopsys, Twistlock, Veracode.

NO. 10: RASP SOLUTIONS ARE VINDICATED, BUT THEY STILL AREN'T READY FOR PRIME TIME

Runtime application self-protection (RASP) has been around since 2013, but it took four years for the concept and commercial solutions to take off and to be a feature of the 2017 RSAC Innovation Sandbox. With RASP, an agent, which you install along with your application that instruments the code, prevents the application from performing nonsecure functions such as SQL injection or displaying sensitive data to gain acceptance as a real possibility. RASP tools' sweet spot is to provide protection for applications that are too expensive to fix or to prevent critical applications from encountering any latent vulnerabilities such as zero day attacks.

› **What you should know:** RASP only applies to very specific applications. For example, RASP tools support only very specific development languages. If your application has lived any amount of time and your application is therefore built with different software languages like C or C++, your

application won't qualify. Some RASP tool vendors claim they can replace your web application firewall (WAF) because they can provide PCI DSS compliance by providing protection against the OWASP Top 10. Unfortunately, because the RASP agent is installed with the application, RASP tools do affect performance. For some applications, this performance hit will be negligible, but for others the performance degradation will not be acceptable. Also, for any applications that are subjected to bad bot traffic, DDoS, or DDoS Layer 7 attacks, RASPs will not be able to prevent the application from suffering from performance issues, and, therefore, RASPs will not replace your WAF.

› **What you should do about it:** Unless you have an application that meets the very strict rules that RASP currently requires to work, you're going to have to take a wait-and-see stance. If you have an application that isn't very sensitive to performance degradation and your developers built it using one of the supported programming languages, it's time to start evaluating RASP, but in a layered approach with your WAF.

› **Vendors to watch:** Arxan, Avocado Systems, BrixBits, Contrast, Immunio, Prevoty, Signal Sciences, tCell, Veracode, Waratek.

NO. 11: VULNERABILITY REMEDIATION IS SHIFTING TO THE PRODUCT OWNER

Vulnerability management has long suffered from a disconnect between the security team, which traditionally performs vulnerability scanning, and the operations team, which usually unhappily inherits the work that these scans generate. Companies such as Bay Dynamics are attacking this disconnect head-on by making Agile product owners responsible for documenting information workflows and classification, as well as for managing vulnerabilities in their applications. This shift is also supported by technology trends. As containers continue to gain widespread growth, more and more of what has been part of the responsibility of operations for system management is getting packaged into DevOps processes. Tenable's acquisition of FlawCheck is an example of the market embracing this trend.

› **What you should know:** Containers are changing everything. Custom code, libraries, frameworks, and/or apps are being packaged early in the build process, which allows vulnerability and configuration management to occur very early in the Agile development life cycle. Server configuration analysis and software vulnerability scanning may now be performed long before production, reducing the cost of remediation and, hopefully, the number of vulnerabilities making it to production.

› **What you should do about it:** Stay informed on technology adoption within your organization as DevOps continues to gain traction. Become a champion for these new technologies, and search for ways to work with development and operations teams to improve efficiency and security of your organization. Further, follow these vulnerability and risk management trends to help center the security discussion on Agile product owners.

› **Vendors to watch:** Anchore, Aqua Security, Bay Dynamics, Tenable, Twistlock.

NO. 12: "SERVERLESS" IS THE NEW CLOUD PARADIGM — AND S&R MUST SECURE IT

Many of today's IaaS, PaaS, and SaaS platforms have difficulty scaling to the extreme elasticity needed for such scenarios as large-scale marketing campaigns, order storms (new Nike sneakers launched and customers wanting to buy them minutes afterward), or concert tickets going on sale. After IaaS, PaaS, and SaaS, we're now seeing the cloud offering serverless microservices such as AWS Lambda, Google Cloud Functions, and Microsoft Azure Functions. For example, if you want to send 10 million marketing campaign messages, instead of spinning up thousands of IaaS or PaaS workloads, you simply call a hyper-elastic microservice that will do that for you and pay a fraction of a cent per invocation.

- **What you should know:** Because of their fine grain, these microservices present even greater security challenges to cloud user organizations. Caller apps (on-premises, in the hybrid cloud, etc.) need to supply credentials and inject data into these serverless microservices. Since these microservices are in the cloud, hackers may intercept calls on-prem, on the network (in-transit from on-prem to the cloud), or directly in the cloud. Forrester expects that specialty players as well as microservices providers such as AWS, Google, IBM, and Microsoft will provide these microservices with security capabilities. Specifically, we will see data leak prevention (DLP); identity and access management (IAM) services like provisioning, deprovisioning, authentication, authorization, and self-services; dynamic software-defined networking; and DDoS solutions in new gateway and brokering solutions.
- **What you should do about it:** Work with your ADD and SVM counterparts to refactor on-premises and cloud applications so that these apps can call microservices securely. Given their simplicity, IoT-connected devices calling microservices is a convenient way of serving and securing large IoT infrastructures' external data movements to the cloud. S&R pros should assess workload utilization reports and data movement patterns and define governance regimes for implementing serverless microservices security policies to on-prem and hybrid cloud hosted applications.
- **Vendors to watch:** AlertLogic, AWS Lambda, CloudPassage, Google Functions, Microsoft Azure Functions, Mulesoft, TrendMicro.

NO. 13: CYBER RISK QUANTIFICATION TEMPTS CISOS TO BYPASS RISK MANAGEMENT FUNDAMENTALS

In order to encrypt data, segment networks, and deploy granular application security technologies, S&R pros must base their decisions on the value of the assets to this organization and the risk to them from cybercriminals, malicious insiders, accidents, and noncompliance. Meanwhile, S&R pros face intensifying scrutiny from top executives and the board today. Questions have shifted from "Is our spend on security worth it?" to "What's our cybersecurity exposure?" and "How well are we protected?" Meanwhile, cyberinsurers seek more data and more sophisticated and efficient means to determine appropriate coverage and premiums. The theme across all of these trends is risk: To communicate with top leadership effectively today and make the appropriate risk-based decisions, S&R leaders must translate threats, vulnerabilities, assets, and controls into more tangible business terms — the more concrete and quantifiable, the better.

- **What you should know:** Information risk management is not a new function, but trying to move beyond qualitative measures (e.g., low/medium/high or 1 to 10 scales) and "quantify" cyber risk is an area even experienced information risk managers have avoided. Assigning dollar values to cyber risk with any high degree of confidence is incredibly challenging due to the number of inconsistent variables, the lack of actuarial data, and the unknown value of the intangible assets and intellectual property that security programs must protect. Cyber risk quantification isn't fundamentally different from previous risk management efforts: The core process is still to determine the business impact of cyberevents and estimate the probability that they will occur; the difference is that with this type of quantitative approach, you apply dollar figures to assess impact and confidence intervals to supplant likelihood.
- **What you should do about it:** Expect business pressure from CFOs, CEOs, board members, strategic partners, insurers, and others to keep pushing forward with cyber risk quantification initiatives. Two frameworks aiming to standardize related efforts are gaining traction: 1) factor analysis of information risk (FAIR), and 2) cyber value-at-risk (CyVaR). Meanwhile, consulting and software solutions are also on the rise to help S&R pros apply the frameworks' methods and to automate the collection and analysis of risk data for quantification purposes. However, stick to the mantra "Try to walk before you run," and make sure you have a fairly mature risk management process already in place.[12] And don't overlook the value that qualitative risk scores can offer — they still help you identify your biggest areas of cyberexposure, communicate in consistent terms with top leadership, and prioritize strategic projects.[13]
- **Vendors to watch:** Bay Dynamics, Corax, Cyrence, Cytegic, Kenna Security, Quantar Solutions, RiskLens, RiskSense, UpGuard.

NO. 14: CORPORATE AND DEFENSE SECURITY INCUBATORS ARE CHALLENGING SILICON VALLEY

We end our top trends report with a trend that is likely to further expand the vendor landscape. The lure of security's total addressable market, for which 2016 estimates range from $60 billion to $122 billion, is tempting for many enterprise CISOs and former military cyberspecialists.[14] These founders are striking out on their own, bringing their real-world practitioner experience to help solve security problems while there is ample investment capital available. The traditional technology startup mecca might be Silicon Valley, but these entrants are headquartered in Cincinnati, Ohio, Louisville, Kentucky, and Tel Aviv, Israel.[15]

- **What you should know:** Internal technology that becomes an external success isn't new in technology — but it is a newer concept in the security industry. For example, Lucasfilm is the birthplace of what became Adobe Photoshop and Pixar Animation Studios. Organizations like GE, Netflix, and Unit 8200 of the Israel Defense Forces might be the origin of the next big security vendor. These startups possess a unique advantage, using their enterprise and military experience to bring solutions to market. These companies have a shorter path to travel before finding product-

market fit, using their background to understand the needs of potential clients. They also bring an authentic message to the market, their days of dealing with complicated security issues being not too far behind them in the rearview mirror.

› **What you should do about it:** There are two potential paths, one for companies that might have a viable external offering, the other for those looking for a different kind of security vendor. Those with custom-built security solutions should analyze what problems it solves, how much solving it was worth, and if others would be willing to pay for it. CISOs might be running their security program on something that could become a revenue-generating product or service for their employer. That value could be in adding to their organization's patent portfolio, as a licensed feature of another technology, or through a seed round as their parent company decides to spin them off as a full-featured product or service. The others that want a different type of security vendor should look at these startups because they may find a vendor that better understands the reality of solving today's security problems at the enterprise level.

› **Vendors to watch:** Cymmetria (Unit 8200 IDF), Morphick (GE), Swimlane (TBD).

Endnotes

[1] Forrester examines the current IoT attack surface and provides guidance for security and risk (S&R) professionals on how to protect and defend against IoT-based threats. See the Forrester report "The IoT Attack Surface Transcends The Digital-Physical Divide."

[2] Forrester defines the use cases, business value, and outlook for the 13 most relevant and important technologies for delivering IoT security. See the Forrester report "TechRadar™: Internet Of Things Security, Q1 2017."

[3] S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model; position data security and privacy capabilities as competitive differentiators; and build a new kind of customer relationship. See the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[4] More specifically, radioactive data consists of what Forrester calls "the 3 P's plus IP." The 3 P's are data that is subject to local or national laws or compliance regulations, such as payment card information (PCI), personal health information (PHI), and personally identifiable information (PII). The fourth element is intellectual property (IP). Further, you should also consider data whose loss will violate a business agreement as "radioactive." You should protect radioactive data primarily through robust technical controls such as encryption, tokenization, or data masking. See the Forrester report "Rethinking Data Discovery And Data Classification Strategies."

[5] Source: Craig Gentry and Shai Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," Eurocrypt, 2011 (https://eprint.iacr.org/2010/520) and Shai Halevi and Victor Shoup, "An Implementation of homomorphic encryption," GitHub (https://github.com/shaih/HElib).

[6] In Forrester's Digital Risk Monitoring Wave, we evaluated the top software solutions that comprehensively and persistently monitor for brand, cyber, and physical risk across digital — i.e., social, mobile, and web — channels. See the Forrester report "The Forrester Wave™: Digital Risk Monitoring, Q3 2016."

[7] See the Forrester report "Top Cybersecurity Threats In 2017" and Forrester Data Global Business Technographics® Security Survey, 2016.

[8] As the remediation costs, customer impacts, and reputational damage of a data breach continue to skyrocket, the security industry must find new ways to prevent the exfiltration of proprietary data by cybercriminals and other malicious actors. Forrester calls for developing more automated threat response processes and a set of cyber rules of engagement. Doing so will empower security professionals to act more quickly and aggressively and stop data breaches before they impact the business. See the Forrester report "Rules Of Engagement: A Call To Action To Automate Breach Response."

[9] "Every time you switch your attention from one subject to another, you incur the Cognitive Switching Penalty. Your brain spends time and energy thrashing, loading and reloading contexts." The more things that you try to pay attention to at once, the more your performance at all of them suffers. The fact that humans are bad a multitasking is a well-studied phenomenon. Source: Josh Kaufman, The Personal MBA: A World-class Business Education in a Single Volume, Portfolio Penguin, 2010.

[10] See the Forrester report "Top Cybersecurity Threats In 2017" and Forrester Data Global Business Technographics Security Survey, 2016.

[11] Source: "Business E-Mail Compromise: The 3.1 Billion Dollar Scam," Federal Bureau of Investigations, June 14, 2016 (https://www.ic3.gov/media/2016/160614.aspx).

[12] Use Forrester's GRC Maturity Model to evaluate your current risk management efforts. This self-assessment tool aims to help risk managers improve efficiency, reduce losses, and strengthen business performance. See how you stack up, and if your organization is ready for more sophisticated risk measurement techniques. See the Forrester report "Assess Your GRC Program With Forrester's GRC Maturity Model."

[13] Depending on your skill level, maturity, resources, audience, and objectives, risk measurement can be very simple or very complicated. Regardless, convince stakeholders that risk measurement isn't just based on hunches, it doesn't have to be overly-complicated, and it will do more than simply confirm assumptions. See the Forrester report "The Risk Manager's Handbook: How To Measure And Understand Risks."

[14] The security market is poised to grow at a rapid rate in the coming years. The total addressable market is predicted to grow to $202 billion by 2021. Source: "Cyber Security Market Worth USD 202.36 Billion by 2021 - Rise in Security Breaches Targeting Enterprises Driving Growth - Research and Markets," BusinessWire press release, August 9, 2016 (http://www.businesswire.com/news/home/20160809005959/en/Cyber-Security-Market-Worth-USD-202.36-Billion) and "Cybersecurity: Time for a Paradigm Shift," Morgan Stanley, June 15, 2016 (https://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm).

[15] Sample vendors include Morphick in Cincinnati, Ohio, and Swimlane in Louisville, Kentucky.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

RiskSense®, Inc., is the pioneer and market leader in pro-active cyber risk management. The company enables enterprises and governments to reveal cyber risk, quickly orchestrate remediation, and monitor the results. This is done by unifying and contextualizing internal security intelligence, external threat data, and business criticality across a growing attack surface.

The company's Software-as-a-Service (SaaS) platform transforms cyber risk management into a more pro-active, collaborative, and real-time discipline. The RiskSense Platform™ embodies the expertise and intimate knowledge gained from real world experience in defending critical networks from the world's most dangerous cyber adversaries.

By leveraging RiskSense cyber risk management solutions, organizations can significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, heighten response readiness, reduce costs, and ultimately minimize cyber risks. For more information, please visit www.risksense.com or follow us on Twitter at @RiskSense.