Gartner.

Top Security and Risk Management Trends

Published: 31 January 2019 **ID:** G00378361

Analyst(s): Peter Firstbrook, Brian Reed, Sam Olyaei, Gorka Sadowski, David Mahdi, Prateek Bhajanka, Earl Perkins

Several new trends are emerging in security and risk management that reflect longer-term trends. Reacting to these developments provide opportunity for security and risk management leaders to improve resilience, better support business objectives and elevate their standing in the organization.

Key Findings

- Risk management leaders are developing risk appetite statements linked to business outcomes.
- There is a renewed interest in implementing, maturing or outsourcing security operations centers with a focus on threat detection and response.
- Leading organizations are utilizing a data security governance framework to prioritize data security investments.
- “Passwordless” authentication is starting to achieve market traction driven by customer demand availability and the need to protect credentials.
- Security product vendors are increasingly fusing products with services.
- Leading organizations are investing in and maturing their cloud security competency.
- Leading organizations are investing in inside-the-perimeter security.

Recommendations

Security and risk management leaders seeking to capitalize on these trends should:

- Engage business stakeholders to create risk appetite statements.
- Build or outsource a security operations center.
- Use a data security governance framework before investing in tools.
- Exploit passwordless authentication to improve security and convenience.

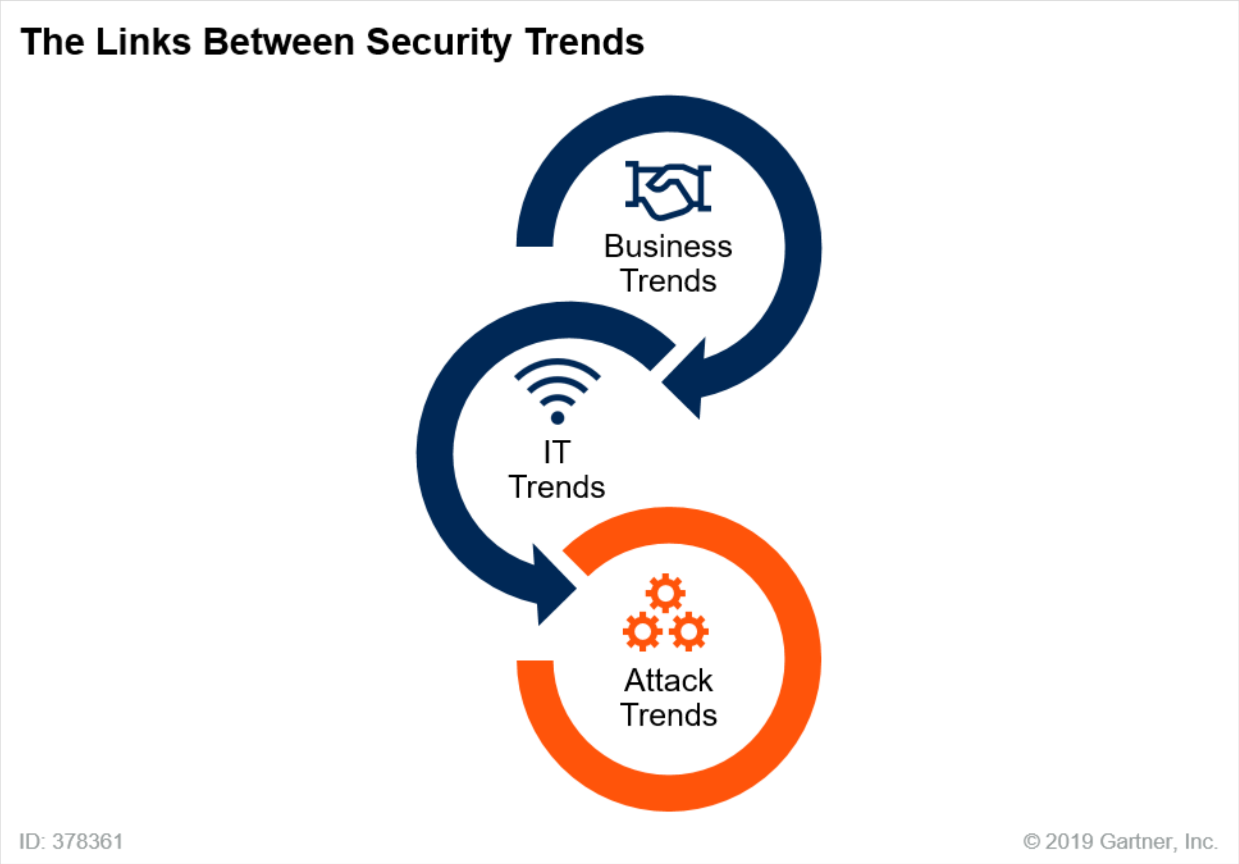
- Seek out solution providers that offer a fusion between products and services.
- Establish a cloud center of excellence team and invest in training.
- Augment one-time security gates with internal detection capabilities.

Analysis

As we explore these trends in detail, it is important to point out the definition Gartner uses to identify top cybersecurity trends. In Gartner's definition, **"top" trends highlight ongoing strategic shifts in the security ecosystem that aren't yet widely recognized, but are expected to have broad industry impact and significant potential for disruption.** Through 2025, technologies and strategies related to these trends will reach a level of maturity that offers leaders valuable capabilities in the effort to secure digital business. This analysis does not attempt to predict what will happen. Rather, we aim to describe what's significant about what we see happening in the cybersecurity discipline. Astute security and risk management (SRM) leaders should be aware of these trends, and take advantage of those that will help secure their organization.

Top trends do not live in isolation (see Figure 1). Rather they are generally driven by longer-term trends. Before we dive into the current trends, it is important to point out some longer-term mega trends that are driving some of the subtrends that we see today. Mega security and risk trends are broader longer-term trends that are influencing the overall security and risk landscape. These mega trends can be split into two groups, external trends that are influencing the market and internal trends that are a result of the changing IT landscape and architectural approaches.

Figure 1. The Links Between Security Trends



Source: Gartner (January 2019)

Mega External Trends

- The velocity and creativity of attacks will continue to grow, and attackers will exploit a variety of tools, tactics and techniques against an ever-increasing diversity of targets to achieve a growing range of goals.
- The security skills gap will persist, abetted by an ever-increasing complexity in IT systems and the security tools used to protect IT systems.
- Application delivery scale and complexity will continue to grow as a result of component containerization and cloud delivery.
- Device and endpoint diversity will continue to grow due to IoT and mobile accelerators.
- Regulatory and privacy challenges will continue to grow in conjunction with digital business's insatiable appetite for personal data.

Mega Security Trends

- Security products are rapidly exploiting cloud delivery to provide more agile solutions.
- Perfect prevention and authentication is not possible. Security architects must build detection, response and controls to enable trust levels that meet the risk tolerance of business leaders.
- Machine learning is providing value, but it will not solve all security problems and comes with its own challenges.
- The requirement for automation, orchestration and integration across security domains will continue to grow as the complexity of security solutions increase and the skills gap persists.
- Cyber-physical systems are forcing organizations to think about physical risk and safety.

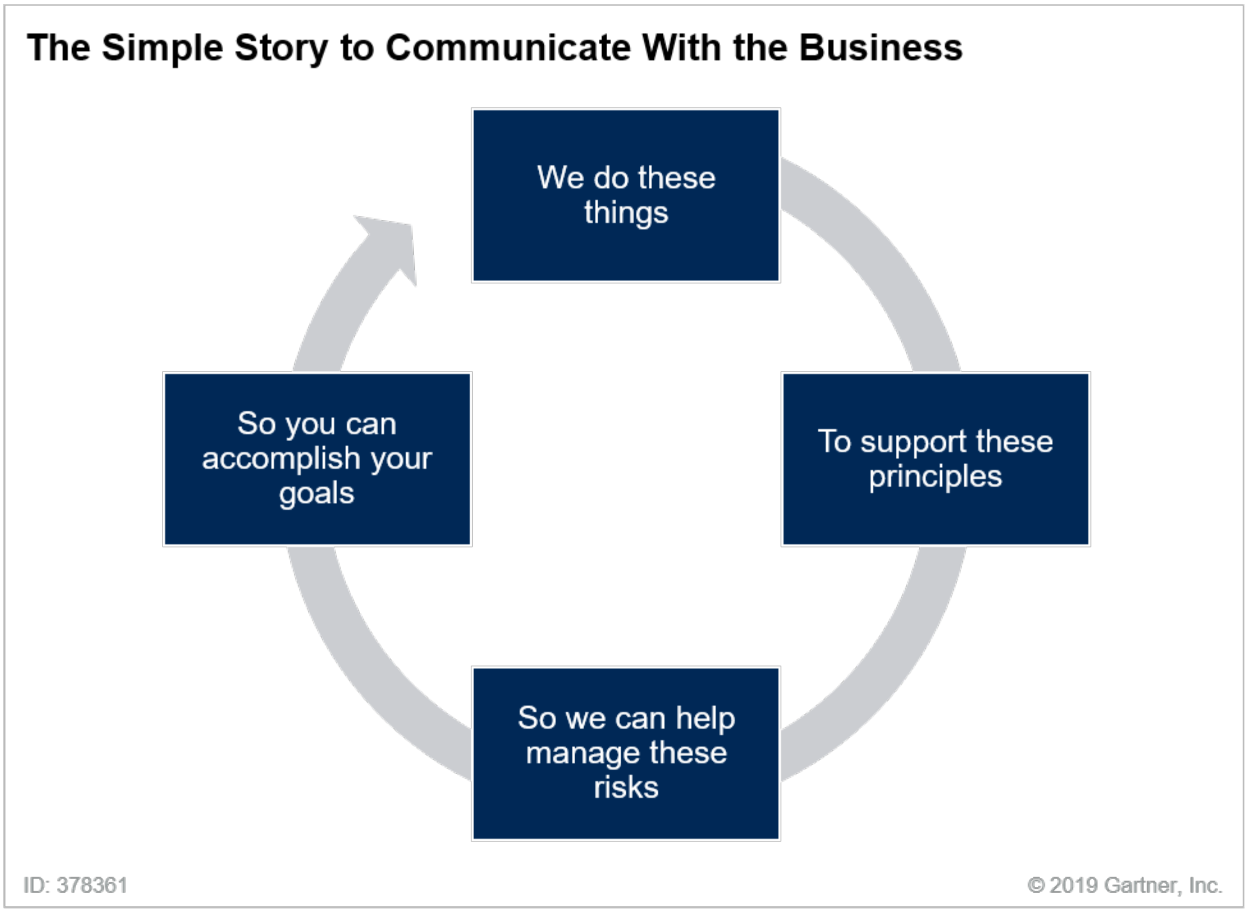
2019-2020 Trends

Trend No. 1: Leading SRM Leaders Are Creating Pragmatic Risk Appetite Statements Linked to Business Outcomes to Engage Their Stakeholders More Effectively

In 2018, 90% of large enterprises were expected to present security issues to business leaders. For years, CISOs and security managers have steadily begun to participate in meetings involving line-of-business stakeholders. However, discussions often focused on tactical matters, leaving many business leaders confused as to why security leaders were even present at strategic meetings. As a result, CISOs miss a clear opportunity to advocate for security and inform stakeholders.

Gartner client inquiries make it clear that one of the most serious challenges faced by security and risk management leaders is their inability to communicate effectively with senior executives and other key business decision makers (see Figure 2).

Figure 2. The Simple Story to Communicate With the Business


The Simple Story to Communicate With the Business
We do these things
To support these principles
So we can help manage these risks
So you can accomplish your goals
ID: 378361
© 2019 Gartner, Inc.

Source: Gartner (January 2019)

In particular, SRM leaders continue to struggle with business engagement to support risk decision making. Business stakeholders don't always grasp how much technology-related risk they are exposed to or how much they are willing to accept. This leads to decisions that expose them to too much risk or pull back from beneficial initiatives due to an overestimation of how much risk they actually represent. In other words, businesses suffer if they take on too much risk and fail to grow if they are too risk averse.

As a result, SRM leaders are beginning to create simple, practical and pragmatic risk appetite statements that are linked to business goals and risk treatment plans (see the sample risk appetite statement below and Note 1). A risk appetite statement is a useful document that informs stakeholders and partners of the organization's intentions when taking on risk.

> National Rail System has no appetite for safety risk exposure that could result in injury or loss of life to the public, passengers

> and the workforce. All safety targets are met and improved year over year. In the pursuit of its growth and modernization objectives, the NRS is willing to accept risks that may result in some financial loss.

When preparing risk appetite statements, CISOs should be aware of the power of emotions when communicating risk issues. Emotion is frequently more important than data when decisions are made. In addition, CISOs should focus on other aspects of effective business communication when developing an effective risk appetite statement:

- Clarity: Be very clear about the message. Statements must be simple, clear and concise.
- Consistency: Mixed messages and inconsistency lead to distrust and lack of follow-through. The message must be consistent both within single messages as well as across the entire program.
- Medium: There are myriad ways to deliver a message. Successful communicators match the medium to the audience, time frame, culture and venue.
- Relevancy: The core message needs to be related to something the audience cares about.

Recommendations

- Engage business stakeholders and general counsel directly through executive workshops to discuss the current risk landscape and current and future business initiatives that may lead to excessive risk.
- Create simple, practical and pragmatic risk appetite statements that are linked to business goals and risk treatment plans.
- Create a concise narrative that links the security and risk management program goals to business goals.
- Place everything in a business context that is relevant to board-level decisions and informs decision making, while avoiding issues that are relevant only to IT decision making.

Recommended Readings

“Leverage Emotions to Communicate Risk More Effectively”

“Top Tips for Communicating Security and Risk to Business Stakeholders”

“Toolkit: Information Security Strategy on a Page — Deconstructed”

“Learn Your Risk Appetite or Fail at Risk Management”

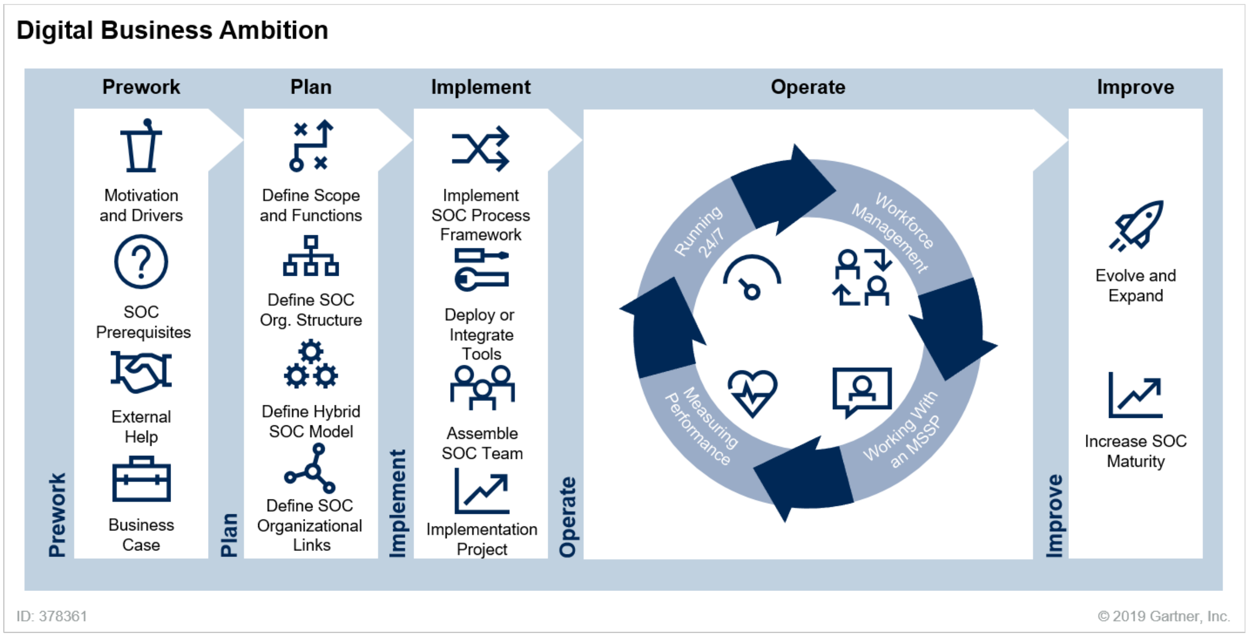
“Institute Cybersecurity and Risk Governance Practices to Improve Information Security”

“Use Storytelling to Bolster Your Security Communication Plans”

Trend No. 2: There Is a Renewed Interest in Implementing or Maturing Security Operations Centers With a Focus on Threat Detection and Response

Since 2016, Gartner has been documenting a clear shift in security investments, from threat prevention to threat detection and response. The increased velocity, complexity and business impact of attacks, and the complexity and sheer number of security tools generating alerts, have elevated the requirement to build, or revitalize, a security operations center (SOC). Leading security and risk management organizations are reinvesting in SOCs or are starting to build or outsource this function for the first time (see Figure 3).

Figure 3. Digital Business Ambition



Source: Gartner (January 2019)

By 2022, 50% of all SOCs will transform into modern SOCs with integrated incident response, threat intelligence and threat hunting capabilities, up from less than 10% in 2015.

Many organizations have been burnt by the lack of preparation for security incidents, or lack of tools and processes to rapidly respond. Concurrently, security architectures have evolved from a strong focus on preventive capabilities to a more balanced approach that covers prevention and detection, with a renewed effort to improve response and prediction capabilities. This balanced approach compels investments in more sensitive detection technology, such as endpoint detection and response (EDR), user and entity behavior analytics (UEBA) and deception.

These tools are invaluable in detecting under-the-radar threats that have already evaded perimeter and traditional defenses. However, they are also more sensitive, and thus generate more alerts to investigate and require a more sophisticated skill set. Other tools have emerged to accelerate the response process after an alert has been generated, such as security orchestration, automation and response (SOAR), also requiring an expert skill set to operate properly. The migration to cloud computing has also introduced a number of new tools and new hybrid architectures that open new attack vectors, forcing many SOCs to extend their scope beyond on-premises infrastructures.

The requirements for sophisticated detection and response in this complex environment have amplified the need to centralize and optimize capabilities, and offer an opportunity to demystify the SOC and establish it as a business asset. While some organizations are establishing and staffing their first SOC, others are revitalizing theirs with new investments to improve operational efficiency.

The biggest challenge for new SOCs is staffing, followed by adopting new tools. The most common unifying toolset in most organizations is the SIEM. However, SIEMs do not provide enough value in the response phase of threat detection and response, and are often complemented in mature organizations with SOAR tools that can orchestrate and automate response playbooks.

Existing SOCs are investing in integrating threat intel, consolidating alerts, and establishing and automating workflow and playbooks to provide a more efficient response capability. Leading SOCs are also investing in more active penetration testing that tests the SOC's ability to detect attackers and neutralize them.

Clearly, not all organizations are capable of building their own SOC, and indeed most may not require one if they only get a few incidents per year. However, all organizations, regardless of size, must be on the lookout for threats and be prepared to respond in the event of a major incident. Some organizations may choose to completely outsource their security operations. Managed detection and response (MDR) services are filling the need of organizations of all sizes that lack internal security resources and expertise, and want to expand their investments beyond preventive security technologies to address their detection, response and 24/7 monitoring gaps. Many organizations are also establishing retainer incident response services to ensure the process of finding and contracting an IR service is not an impediment to fast incident response.

Outsourcing accountability and decision making is, of course, impossible. Therefore, Gartner's advice to customers engaged in a fully outsourced model is to at least retain control of business-centric security activities, such as business-level incident response actions.

Recommendations:

- Develop requirements for a SOC in conjunction with security, IT, risk management and business stakeholders, taking into account current risks and threats, as well as the business objectives.
- Expand the SOC's capabilities beyond just SIEM solutions to provide greater visibility into the IT environment, using tools such as EDR and UEBA.
- Define a SOC target operating model that addresses people, processes and technology, along with business-aligned goals and applicable metrics. Develop a SOC staff retention strategy from the outset, as well as a continuous hiring capacity.

- Use managed security services (MSSs) or managed detection and response and incident response retainers to fill coverage and skills gaps, either tactically or as part of the long-term strategy.

Recommended Readings

"Selecting the Right SOC Model for Your Organization"

"How to Plan, Design, Operate and Evolve a SOC"

"SOC Development Roadmap"

"Market Guide for Endpoint Detection and Response Solutions"

"Market Trends: The Security Operations Center Opportunity"

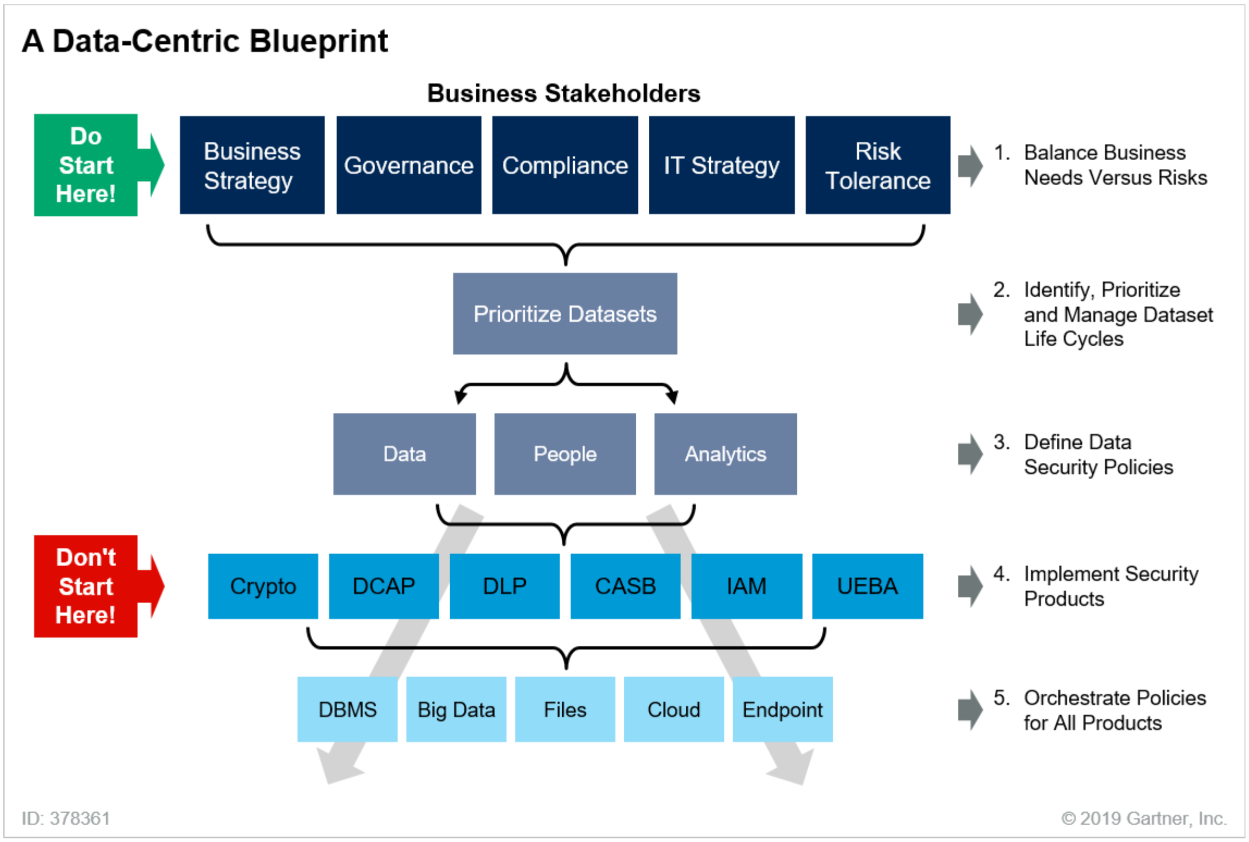
"Market Guide for Managed Detection and Response Services"

Trend No. 3: Leading Organizations Are Utilizing a Data Security Governance Framework to Prioritize Data Security Investments

As organizations continue to expand their data footprint, many assume that solving data security is just a technology problem. However, data security cannot be completely addressed through implementation tools, such as data classification, DLP, EDRM or encryption. Data security is a complex issue that cannot be solved without a strong understanding of the data itself, the context in which the data is created and used, and how it maps to an established governance framework.

Leading organizations are starting to address data security through a data security governance framework (DSGF) approach (see Figure 4). DSGF provides a data-centric blueprint that identifies and classifies structured and unstructured datasets across all enterprise computing assets and defines data security policies. This also helps to select technologies that implement risk mitigation and further support the DSGF process.

Figure 4. A Data-Centric Blueprint



Source: Gartner (January 2019)

SRM leaders must first address the business strategy and risk tolerance of the organization to data security events, the regulatory environment, and identify and classify data assets based on business risk. Only then can leaders start to prioritize technology investments to meet the policy objectives derived from DSG. Data security tools also need to instrument data access and usage sufficiently to provide intelligence and make DSG a fact-based process.

Data security must include other technologies beyond traditional data security technologies. A strong identity and access management (IAM) program is a critical component to help understand user context and track data access, especially in the case of responding to issues of compromised credentials. IAM provides a structured and coherent approach to managing the identity of people and things, and their access to systems and data. UEBA solutions use analytics to build the standard profiles and behaviors of users and entities (hosts, applications, network traffic and data repositories) across time and peer group horizons. Activity that is anomalous to these standard baselines is presented as suspicious, and packaged analytics applied on these anomalies can help discover malicious insiders and external attackers.

It is no longer acceptable to play “defense only” when it comes to securing data. Organizations must uncover what user intent really is, as well as attacker intent, to better determine and distinguish between legitimate data security incidents and cases of negligence/misuse. “Is this truly an incident I need to address immediately?" or "Will this data incident result in a material impact to our organization?" are questions that a combination of DSGF and technology must answer, using automation and intelligence.

Recommendations

- Use the DSGF to prioritize business risks that need to be mitigated.
- Use continuous adaptive risk and trust assessment to select appropriate security policy rules and functionalities that mitigate the critical business risks.
- Align data security programs with overall enterprise data governance, evaluating policies and data classification before selecting controls.
- Develop capabilities to identify sensitive or critical datasets and audit the full enterprise environment.
- Commit to orchestrating rules across multiple tools because a single tool or control can rarely address all enterprise data security risk.
- Conduct periodic gap analyses in enterprise data security programs to address changing business goals and dynamic threat landscapes.

Recommended Readings

"How to Use the Data Security Governance Framework"

"Use Infonomics to Reset Data Security Budgets"

"Improving Data Security Governance Using Classification Tools"

"How to Align Enterprise Data Security Initiatives With Overall Data Governance"

"Applying Effective Data Governance to Secure Your Data Lake"

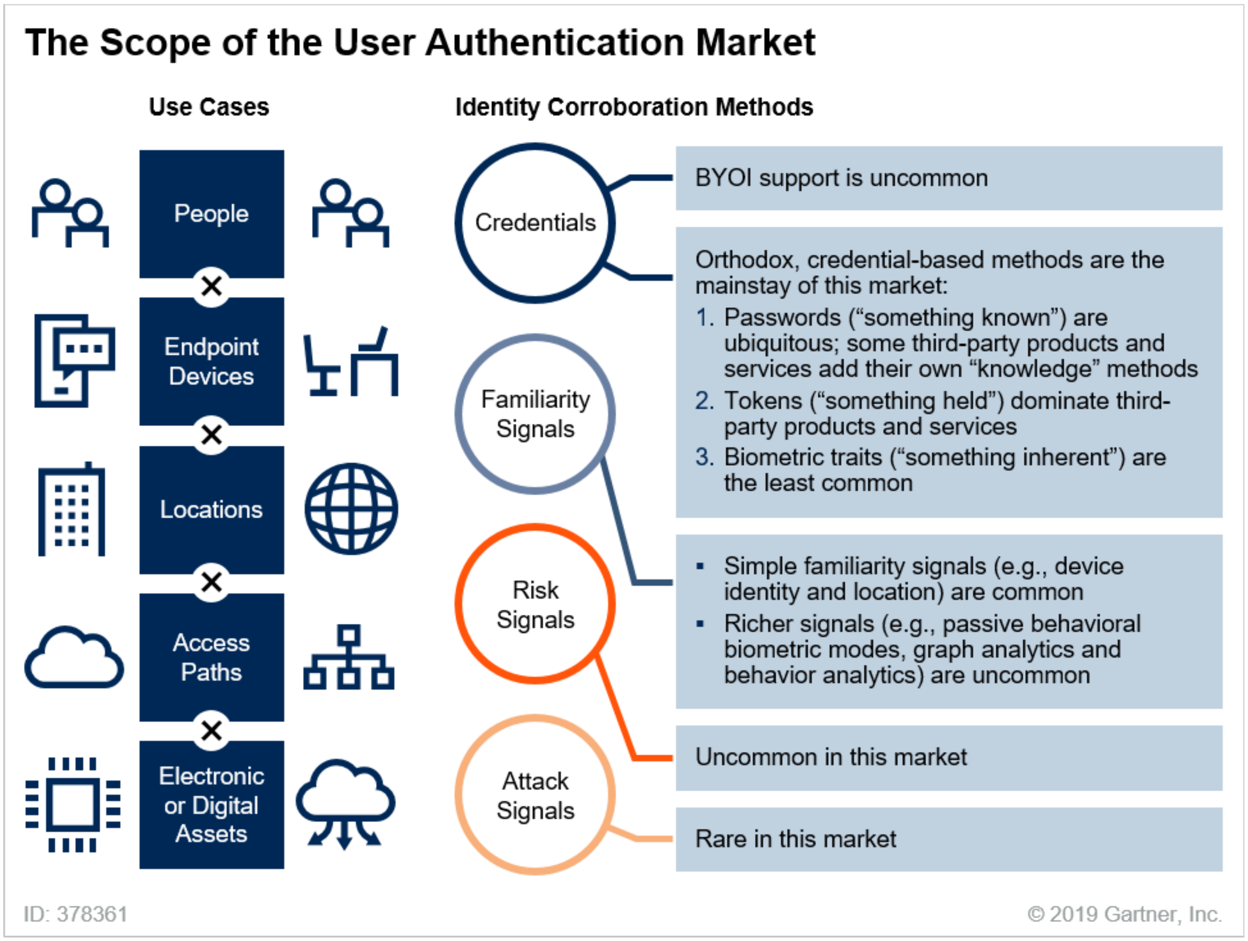
Trend No. 4: "Passwordless" Authentication Is Achieving Market Traction, Driven by Demand and the Availability of Biometric and Strong Hardware-Based Authentication Methods

Driven by a customer demand for convenience, biometric authentication, such as Touch ID and phone as a token, are already widely deployed in mobile banking apps and are now making their way into enterprise applications for consumers and employees. Passwordless authentication is starting to achieve real market traction due to both supply and demand. On the supply side, there is an ever-increasing ecosystem of software and hardware vendors that support passwordless authentication out of the box (see Note 2). On the demand side, IT organizations are moving to cloud-based applications, accessible by unmanaged devices, leaving authentication as the only security control. Attackers have detected this weakness and are relentlessly targeting passwords with numerous well-crafted account takeover attack techniques. This leads to increasing demands for more secure multifactor authentication to replace passwords. Passwordless methods that, for example, ties users to their devices, perhaps with a biometric, can offer stronger authentication. This is a rare win for security, which achieves both increased security and usability.

Passwordless authentication methods leverage approaches, such as (see Figure 5):

- Device-centric biometric authentication, such as Windows Hello, Samsung Fingerprint and Apple Face ID
- Hardware tokens, such as Yubico Yubikeys and Google's Titan Key
- Phone as a token
- Fast IDentity Online (FIDO) alliance universal authentication framework, which provides a standard for passwordless multifactor authentication methods
- Analytics consuming a range of familiarity signals, potentially including passive behavioral biometric methods (see "Don't Treat Your Customer Like a Criminal")

Figure 5. The Scope of the User Authentication Market



BYOI support is uncommon

Orthodox, credential-based methods are the mainstay of this market:

1. Passwords ("something known") are ubiquitous; some third-party products and services add their own "knowledge" methods
2. Tokens ("something held") dominate third-party products and services
3. Biometric traits ("something inherent") are the least common

- Simple familiarity signals (e.g., device identity and location) are common
- Richer signals (e.g., passive behavioral biometric modes, graph analytics and behavior analytics) are uncommon

Uncommon in this market

Rare in this market

Source: Gartner (January 2019)

Historically, most mainstream strong authentication solutions are really “second-factor” (2FA) solutions, which typically add some kind of token to an existing password. More recently, a number of vendors have come to market with 2FA methods that are passwordless by default. Many conventional phone-as-a-token vendors can incorporate a local PIN or device-native biometric mode, such as Touch ID or Samsung Iris scanner, as an additional factor in a mobile application (most notably, Microsoft Windows with Azure AD Premium). Microsoft’s Windows Hello allows for further methods that can be deployed within the enterprise, such as face recognition (for example, with the Microsoft Surface Tablet) or fingerprint.

Other technology provider examples include Entrust Datacard’s Mobile Smart Credential, which integrates in different ways to achieve different use cases. For virtual private network (VPN) and SaaS applications, it combines mobile push with a local PIN, device-native biometric modes or a non-native face mode (via FacePhi). For Windows PC and network login, the person’s smartphone works as a contactless, multifactor, cryptographic token via Bluetooth LE. Passwordless authentication is another example of a CARTA approach to security. It removes the friction from low-risk transactions, and can be used as a steppingstone to gaining trust.

Recommendations

- Explore in-market biometric authentication methods that enable passwordless approaches (such as Windows Hello for Business) and mobile-based methods (such as Samsung Face or Apple Face ID).
- Identify candidate vendors that provide multiple optional methods to enable step-up authentication.
- Pay close attention to technology familiarity across user populations.

Recommended Readings

“Market Guide for User Authentication”

Trend No. 5: Security Product Vendors Are Increasingly Offering Premium Services to Help Customers Get More Immediate Value and to Assist in Skills Training

The shortage of skilled security professionals has been a perennial problem that consistently results in failed security technology deployments. The number of unfilled cybersecurity roles is expected to grow from 1 million in 2018 to 1.5 million by the end of 2020. Most organizations are struggling to fill the open positions they have, let alone retain skilled staff. To compound the problem, numerous security technologies like SIEM, EDR, UEBA, CASB, DLP and CWPP are not “set and forget” solutions. They are more like continuous projects that need constant monitoring and tuning to derive good insights.

Advancements in detection and response capabilities using machine learning, anomaly detection and behavioral analysis actually increase the requirement of humans to investigate more sensitive alerting. Meanwhile, there is no end in sight of next-generation security startups with even more complex monitoring requirements. Ensuring that the right resources and expertise are allocated for threat monitoring, detection and response tool implementation is paramount for long-term success, but where are these bodies going to come from?

While MSSPs are part of the answer, even these organizations are struggling to find staff. Many MSSPs are hopelessly stuck in the past, addressing the late 1990s demands like firewall rule management and super-basic IDS event monitoring, although half the endpoints and applications don't even live behind the firewall or IDS. Moreover, it is difficult for MSSPs to be experts in every product. Even they have a difficult time getting maximum value out of tools unless they specialize in a limited toolset.

This may mean that we are approaching "peak security product," as there are simply not enough skilled people to use the products.

As a result, we are starting to see security product vendors offering a fusion of products and ongoing operational services directly. This level of support goes well beyond simple break/fix product issues, and focuses on helping organizations get immediate value out of the products while improving the administrator's skills level. The best example of this trend is the increasing array of EDR vendors, such as Crowdstrike, Symantec and Carbon Black, offering various levels of alert and incident response services or managed SIEM shops (managed SIEM services).

There are advantages to both vendors and buyers with this fusion approach. For vendors, it solves an obvious objection of buyers of advanced security products: "We simply don't have the people to administer the product." For buyers, it helps upskill their administrators and eliminate some of the workload. It also improves support when the vendors have staff that use the product every day, and it delivers a direct financial incentive for the vendor to focus product improvements on operator efficiency. Indeed, many of these benefits accrue even for buyers that just want the product, making product service fusion vendors more attractive, even to those that want to manage it themselves.

Recommendations:

- Evaluate the internal readiness for adopting advanced technologies in terms of maturity, skills and human resources, and understand the extra load that the internal team can carry.
- Seek out solution providers that offer:
  - A native service layer on top of the product offering
  - Various levels of service layers for various objectives (such as augmentation, replacement of internal effort and for retainer services)
- Prepare to use one or more of different MDRs or product/service offerings, and expect MSSPs to not be the default choice for this, rather that they are tool vendors.

Recommended Readings

"Market Guide for Managed Detection and Response Services"

"Market Guide for Endpoint Detection and Response"

Trend No. 6: Leading Organizations Are Investing in and Maturing Their Cloud Security Competency as It Becomes the Mainstream Computing Platform

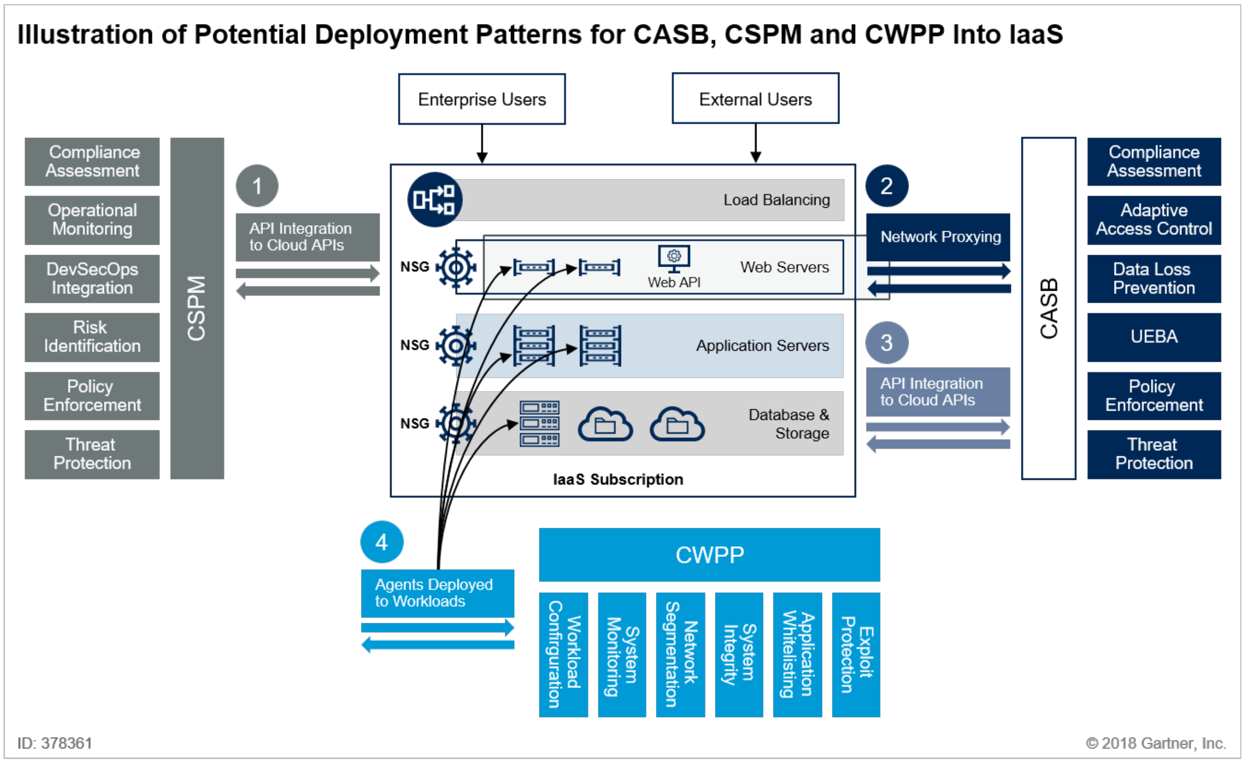
The majority of organizations have begun making substantive use of public cloud services before fully preparing to use them securely. Public cloud computing has proven to be a safe and secure foundation for computing, but it is a shared responsibility model and can easily be used in unsecure ways. Gartner estimates that at least 99% of cloud security failures will be the customer's fault through 2023.

As the majority of organizations choose to take a cloud-first approach, encompassing an ever-greater variety of cloud use cases, it is stretching the capabilities of the existing security team in multiple ways. Virtually all organizations are making substantive use of a variety of SaaS services, each requiring its own knowledge base and security approach. In a recent Gartner survey of technical professionals based primarily in North America, 40% of respondents indicated that their organizations would be spending the majority of new or additional funding on the cloud. However, the survey also found that the cloud is the most common area for talent gaps (see "2019 Planning Guide for Cloud Computing"). While most organizations begin their IaaS use with a single provider, steadily increasing the sophistication and number of applications and storage used within it, many organizations also find themselves using multiple IaaS providers.

Cloud storage and applications, especially with IaaS, are extremely dynamic, as automated DevOps processes deliver an ever-changing set of new and modified applications. Hybrid IT and SaaS integration create new network security challenges. The existing operational and security processes, along with the associated tools, either fail to keep up with the pace of the cloud or are totally unsuited for it. Security professionals have found that it can be impossible to effectively secure use of the public cloud without new classes of automated security tools. The biggest challenge is that cloud computing is bigger, faster and more dynamic than previous generations. It is too complex to control without using mechanisms that can scale and keep up with the pace of agile development and dynamic workload provisioning.

There are three types of new controls that SRM leaders must invest in — cloud access security brokers (CASBs), cloud security posture management (CSPM) and cloud workload protection platforms (CWPPs). These tools offer an overlapping set of capabilities to address cloud risks, but no tool performs all the features of any one of the others, although several vendors are starting to converge these capabilities (see Figure 6).

Figure 6. Illustration of Potential Deployment Patterns for CASB, CSPM and CWPP Into IaaS



Source: Gartner (January 2019)

CASBs (primarily for SaaS) and CSPMs (primarily for IaaS) operate at the control plane. They use cloud provider APIs to gain visibility into user behavior in the cloud and implement access controls and data security policies to reduce risk exposure for organizations as they adopt multiple cloud platforms. CASBs also offer real-time enforcement of security controls through in-line proxies. CWPPs help with multicloud security by focusing on securing the workloads (for example, running on VMs or containers).

CWPPs also compete and complement endpoint detection and remediation tools, which provide real-time visibility into server and container instances.

The secure and compliant use of public clouds requires more than just new tools. New skills are equally important, and these skills take time to acquire and mature. Exploiting automation frameworks is perhaps one of the most important skills to master. Successful cloud-using organizations create predefined workload templates that developers can use to start creating applications. The templates contain preconfigured security policies, allowing developers to focus on writing code rather than trying to secure the virtual enterprise. Immutable infrastructure and blue/green deployment strategies replace traditional patching procedures for production workloads (see Note 3). These DevSecOps principles can help you extract maximum value from the cloud. Therefore, it's crucial to allow staff time to experiment and gain familiarity with this new form of computing.

Recommendations:

- Establish a cloud center of excellence team and invest in staff training, including hands-on public cloud experience, to build the necessary organizational knowledge base.
- Develop new policies and processes that enable your organization to exploit the security strengths of cloud services, while avoiding typical security pitfalls.
- Invest in security and governance tools that are built for cloud scale, and the rapid pace of development and innovation.
- Focus on process automation to ensure that replacement workloads are secure out of the gate with tools and DevSecOps development methodology.

Recommended Readings

"2019 Planning Guide for Cloud Computing"

"2019 Planning Guide for Security and Risk Management"

"Staying Secure in the Cloud Is a Shared Responsibility"

"Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services"

"10 Best Practices for Successful CASB Projects"

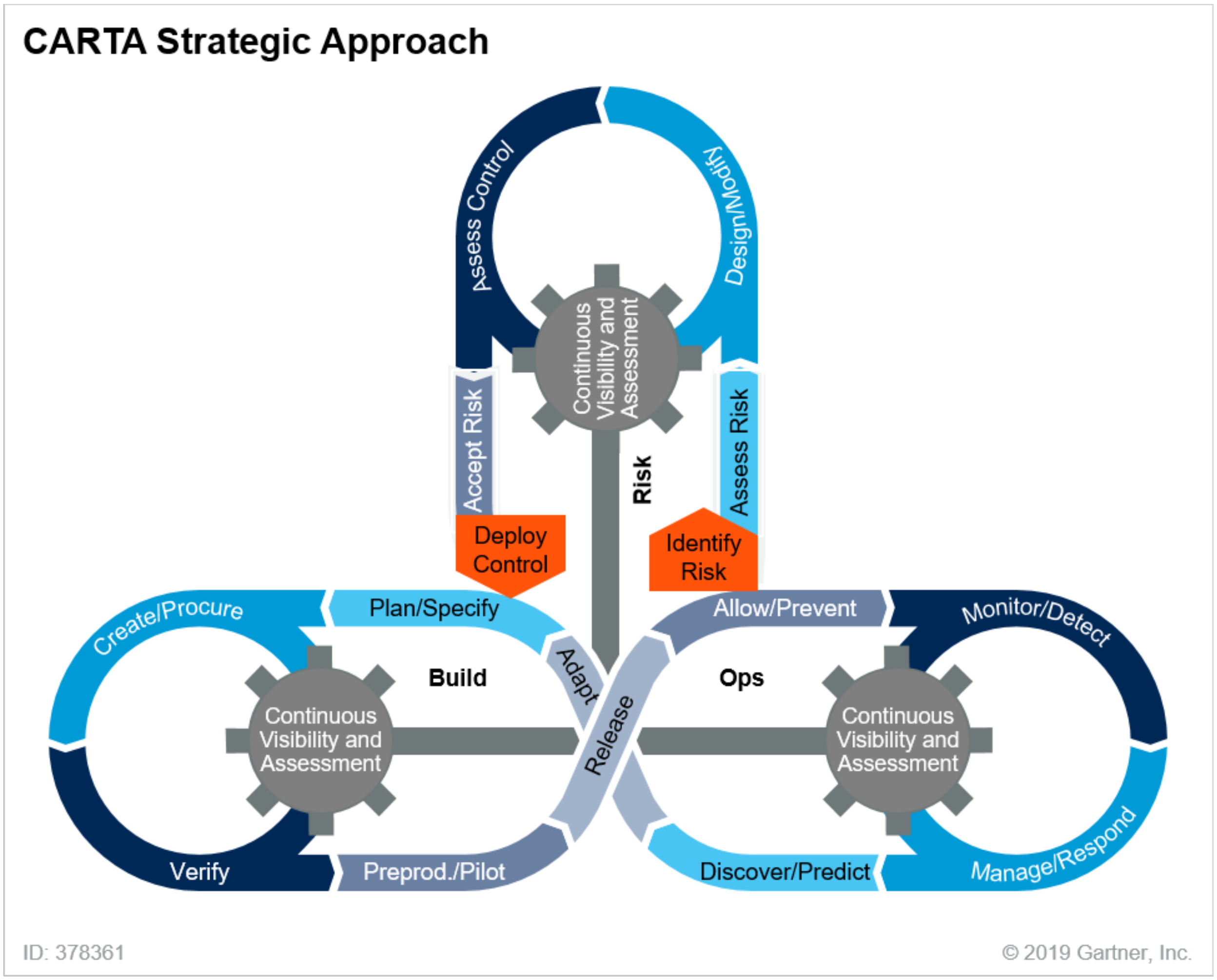
"Magic Quadrant for Cloud Access Security Brokers"

"How to Secure Cloud Applications Using Cloud Access Security Brokers"

Trend No. 7: The Strategic CARTA Approach to Security Is Starting to Appear in More Traditional Security Markets

Network and email security solutions are two great examples of markets that are beginning to deliver a CARTA approach in response to the dissolving perimeter (see Figure 7). CARTA is a strategic approach to security that balances security friction with transaction risk. A key component to CARTA is to continuously assess risk and trust even after access is extended. At its core, CARTA is an acknowledgment that perfect attack prevention, perfect authentication and invulnerable applications were never possible. In futile pursuit of perfection, security infrastructure and processes became constraining and cumbersome, slowing down the organization and the speed of innovation.

Figure 7. CARTA Strategic Approach



Source: Gartner (January 2019)

In a CARTA-inspired architecture, security controls are always monitoring, assessing, learning and adapting based on the relative levels of business risk, threat intelligence and trust that is actually observed. Many solutions and security architects are implementing aspects of CARTA, and this year's trends include a few examples. However, implementing CARTA will be a multiyear journey.

Traditional LAN network security strategies are evolving from a perimeter-only approach to include "inside detection" investments. Indeed, LAN security architects are increasingly acknowledging the fragility of relying only on perimeter detection and seeking inside detection capabilities. They are investing in traditional perimeter controls like intrusion detection and prevention systems (IDPSs), devices in new places and adding new tools (such as network traffic analysis [NTA] and deception devices) to catch attackers that have already evaded perimeter controls. Gartner research suggests that 45% of new stand-alone IDPSs are deployed inside the network, creating a new market focus for IDPSs.

Email security is another market that is starting to adopt a CARTA mindset. Secure email gateways, positioned in front of the email server, have been the traditional email security perimeter. However, increases in account takeover attacks and an acknowledgment that perfect protection is not possible, have increased the interest in internal email protection. Attackers are increasingly seeking authenticated access to mailboxes, which they can use to phish other users in the same mail system, bypassing perimeter security. Moreover, as attackers get more sophisticated, email admins are becoming aware that a second layer of detect and response capability may be necessary. As a result, new vendors are emerging that can provide detect and response capabilities inside the mail system. These solutions inspect the mail server or archives for threats that may have evaded perimeter security, remove malicious messages from inboxes and manage the workflow required to respond to user-identified suspected messages.

Recommended Readings

"Seven Imperatives to Adopt a CARTA Strategic Approach"

"Stand-Alone IDPS Growth Will Come From Inside Detection Use Cases"

"Fighting Phishing — 2020 Foresight"

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Learn Your Risk Appetite or Fail at Risk Management"

"How to Plan, Design, Operate and Evolve a SOC"

"How to Use the Data Security Governance Framework"

"Market Guide for User Authentication"

"Market Guide for Endpoint Detection and Response Solutions"

"2019 Planning Guide for Cloud Computing"

"Seven Imperatives to Adopt a CARTA Strategic Approach"

Note 1 Examples of Risk Appetite Statements

National Bank: <The Bank> faces a broad range of risks in its responsibilities as a central bank. Acceptance of some risk is often necessary to foster innovation and efficiencies within business practices. The risks arising from our policy responsibilities can be significant. These are managed through processes emphasizing the importance of integrity, maintaining quality staff and public accountability.

National Rail System: <Organization> has no appetite for safety risk exposure that could result in injury or loss of life to the public, passengers and the workforce. All safety targets are met and improved year on year. In the pursuit of its objectives, <organization> is willing to accept risks that may result in some financial loss. The company will only tolerate low to moderate gross risk exposure in the delivery of operational performance network reliability and capacity and asset condition; disaster recovery and succession planning; breakdown in information systems; or information integrity.

Local Credit Union: The organization has a tolerance for risk, allowing it to achieve its business objectives in a manner that is compliant with the laws and regulations in the jurisdiction in which it operates. The organization has a low risk appetite for the loss of its business and customer data. The organization has a medium risk appetite for physical information security assets and will track assets greater than $2,000. Information assets will be protected per the organization's data classification framework. The organization has a high risk appetite for access controls. All access to the organization's mission-critical systems will be controlled via biometric authentication.

Note 2 Sample Vendors That Provide Passwordless Authentication by Default

Example vendors include Exostar-Pirean, Forticode, HYPR, MIRACL, Secret Double Octopus, Trusona and Veridium.

Note 3 Blue-Green Deployment Strategy

Blue-green deployment describes an environment that has two identical production environments, so called blue and green. At any given time, only one of the environments is in production. Maintenance is done on the nonproduction system, and it takes over from the production system. This technique is designed to reduce planned and unplanned downtime.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp