FORCEPOINT

# A RISK-ADAPTIVE APPROACH

## REALIZING THE GARTNER CARTA FRAMEWORK IN PRESENT-DAY SECURITY

Gartner

# THE SECURITY ROADBLOCK

Your employee Kate is visiting a client and is planning to give a presentation to senior leadership. She's prepared her slides and attempts to copy them to a USB stick, but her request is swiftly denied in a single message: Your request has been blocked in accordance with your corporate information security policies. IT security has done their job in protecting company data, but have inadvertently prevented a very frustrated Kate from doing her job.

Kate has two options: find a way to bypass the controls and render the company's data protection program ineffective, or miss the presentation and potentially deal a self-inflicted blow to the company's reputation. Determining the lesser of the two evils in Kate's situation depends on who you ask within the organization, and therein lies the fundamental problem: data protection has pushed security and enablement to opposite ends of the business spectrum, when they should be working in unison as one superfluous unit.

In this digital age, business opportunities are plentiful, and so are the risks that accompany them. At the core of every business is data — customer PII, intellectual property, system data—and protecting it is a top priority. But today's IT security systems are designed with binary "all or nothing" capabilities, leading companies to view security as a productivity and revenue roadblock.

### Continuous Adaptive Risk and Trust Assessment Approach

In its current form, data protection lacks the sophistication it needs to be effective in today's complex and fast-paced enterprise environments. For one, it looks at each event individually, making it impossible to understand its effect on the company's overall security posture. Second, it relies on static policies to decide what is good or bad behavior at a single point in time; however, risk and trust are dynamic and ever-changing.

Lacking a clear picture of risk within their organizations, security admins protect data the only way they can, by tightening the screws. As a result, they spend the majority of their day scanning disparate systems for critical threats hiding inside a haystack of alerts. This is why it can take weeks — sometimes even months — from the time of entry to find threats in your network.

Over-indexing on security also restricts a company's tolerance for risk, forcing an ultra-conservative business stance. This causes the system to say "no" when it should thoughtfully say "maybe" or "yes, but with limitations." Every uninformed, illogical, or misaligned block can carry a hefty cost in the form of opportunity loss and productivity decay.

Gartner's continuous adaptive risk and trust assessment (CARTA) approach is how we evolve security from rigid and reactive to flexible and proactive. With this approach, continuous monitoring and analytics take center stage, allowing you to quickly detect and respond to behavioral anomalies — in other words, risky activity. You not only see and organize risk as it occurs, but can manage it more intelligently through small, individualized measures of confidence and responses.

## Risk-Adaptive Protection

Aligning with the CARTA approach, Forcepoint's Risk-Adaptive Protection focuses on how, when, and why people interact with critical data, correlating behavior with the context of user activities so you can see risk holistically. Instead of locking down productivity, risk-adaptive protection gives users more freedom by enforcing policies that are unique to the user and only when needed.

Going back to the previous scenario, if an analytics tool understands Kate as an employee that frequently travels for presentations, it makes sense to allow her to download slides to a USB stick. However, if the analytics tool surfaces behavioral anomalies — unusual web browsing activity or a peculiar badge-in — then security should have the ability to automatically limit which actions she can take while on the network.

What could Risk-Adaptive Protection mean for your company? For one, analytics and automation go hand-in-hand to speed up detection and response without adding additional manpower. With the ability to manage permissions down to an individual user level, you can truly customize your response according to the level of risk your company is willing to accept. In the end, you gain the confidence to optimize both sides of the business spectrum — to embrace opportunities and manage risks in a seamless way.

Source: Forcepoint

Research from Gartner:

# Seven Imperatives to Adopt a CARTA Strategic Approach

Gartner Research Note G00351017 , Neil MacDonald, 10 April 2018

**Supporting digital business transformation in an environment of advanced threats requires a new approach for all facets of security. Security and risk management leaders can use the seven imperatives of a CARTA strategic approach to embrace the opportunities and manage the risks of digital business.**

## Key Challenges

- Perfect attack prevention, perfect authentication and invulnerable applications were never possible, and in futile pursuit of perfection, security infrastructure and processes became constraining and cumbersome, slowing down the organization and the speed of innovation.
- Digital business transformation is moving full speed ahead, with or without information security and risk people, processes and infrastructure being ready.
- Digital risk and trust are fluid, not binary and fixed, and need to be discovered and continuously assessed, alerting security and business leaders to areas of unexpected or excessive risk.
- Security infrastructure and decisions must be context-aware and adaptable to different levels of risk, opportunities and trust levels, and to the risk tolerance of digital business leaders.

## Recommendations

To implement a CARTA strategic approach within their information security management programs, security and risk management leaders should:

- Replace one-time security gates with adaptive, context-aware security platforms.
- Continuously discover, monitor, assess and prioritize risk and trust — reactively and proactively.
- Perform risk and trust assessments early in digital business initiatives, including development.
- Instrument for comprehensive, full-stack visibility, including sensitive data handling.
- Use analytics, AI, automation, and orchestration to detect faster and risk prioritize responses.
- Architect security as an integrated, adaptive, programmable system, not silos.
- Put continuous risk visibility, decisions and ownership into business units and product owners.

## Strategic Planning Assumptions

By 2020, 25% of new digital business initiatives will adopt a CARTA strategic approach, up from less than 5% in 2017.
By 2020, cognitive computing capabilities and prescriptive security analytics will perform 15% to 20% of the security response functions currently performed by human security staff.

By 2020, 60% of digital businesses will be integral parts of larger digital business ecosystems.

By 2022, 60% of large enterprises will influence their operational risk and cybersecurity budgets with business-facing service descriptions, costing and governance related to business units selecting their desired level of cost and risk.

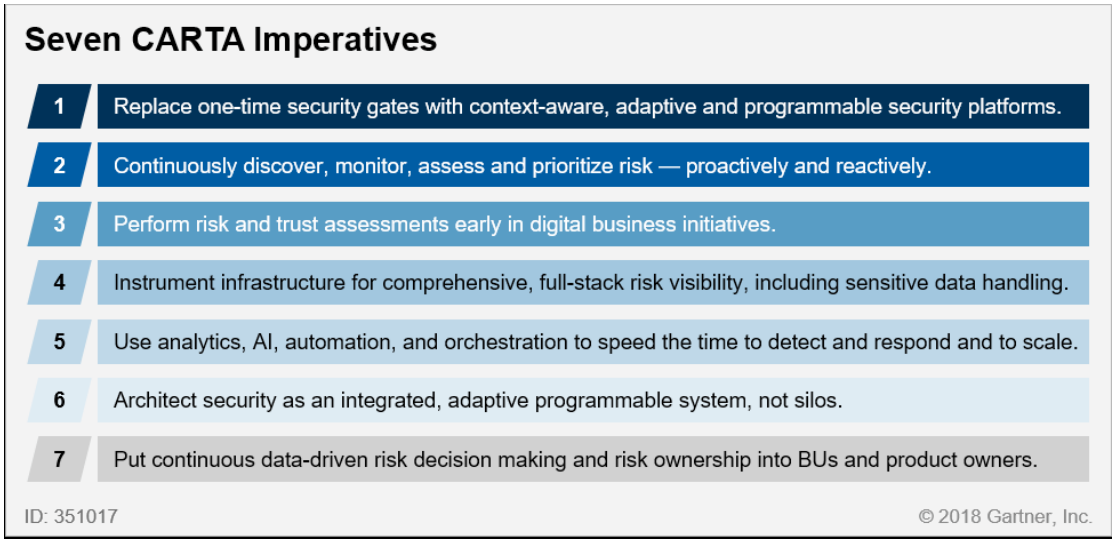
## Introduction

Information security and risk management people, processes and infrastructure are at a critical inflection point. Multiple forces are converging, breaking traditional security and risk approaches:

- Digital business transformation initiatives are creating an urgent need for speed and agility in IT, including information security and risk management, which are seen as slow and unnecessarily restrictive.
- The threat environment continues to adapt and evolve with new types of threats and attacks against new types of IT and business architectures.
- Increasingly, the organization — IT or business units (BUs) — don't own or control the infrastructure where its services are accessed and where its workloads and data are held, breaking security models that used ownership of assets as a proxy for trust.

Digital business opportunity and digital business risk are fundamentally intertwined — zero risk, zero opportunity. The key capability for security and risk management professionals over the next decade will be to continuously discover, assess and adapt to ever-changing risk and trust levels. We need security infrastructure and security decisions to become continuous and adaptive — enabling real-time decisions that balance risk, trust and opportunity at the speed of digital business.

**FIGURE 1**
Seven CARTA Imperatives




Source: Gartner (April 2018)

Security and risk management leaders need to embrace a strategic approach where security is adaptive, everywhere, all the time. Gartner calls this strategic approach "continuous adaptive risk and trust assessment," or CARTA. Adopting a CARTA strategic approach provides a foundation for security and risk management leaders to:

- Use more context, more visibility and more intelligence for continuous, adaptive risk-based decision making, rather than the static, binary "allow or block" security decisions of the past.
- Enable their risk management teams to move beyond yearly "risk management" checklists to make continuous, adaptive, and intelligent risk-optimized security control decisions.
- Work with the BUs and product owners to proactively define acceptable levels of risk and trust when creating new business capabilities, and map this into adaptive security decisions when the business capability is made operational.
- Once operational, provide continuous risk visibility feedback to BUs and product owners to adjust acceptable risk levels and controls as necessary.

Adopting a CARTA strategic approach will require substantial changes to people, processes and security infrastructure. By embracing the seven imperatives outlined in Figure 1, security and risk management leaders can begin adopting a CARTA strategic approach as their map — their charter — to the future for information security.

## Analysis

### Imperative No. 1: Replace One-Time Security Gates With Context-Aware, Adaptive and Programmable Security Platforms

Perfect security is impossible. Yet, much of our existing security infrastructure is based on one-time security gating decisions using predefined lists of "bad" and "good." This approach is fundamentally flawed when there is no pre-existing signature for a zero-day or targeted attack, or when bad guys (and insider threats) have gained credentialed access. To compensate, we subject our users to ever-longer anti-malware scans and ever-longer passwords combined with ever-more-frequent password changes in a futile pursuit of the perfect allow/deny gating decision.

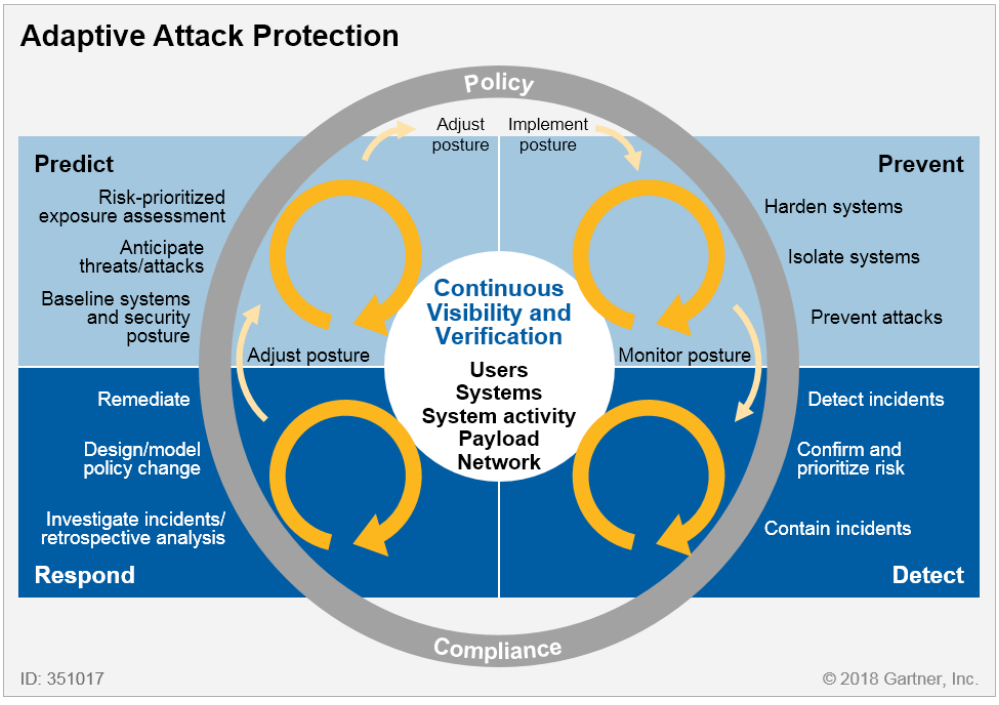
Once access is granted, security and risk management leaders have limited visibility into what users, systems and executable code are doing. Lacking continuous visibility into risk and trust, we have no choice but to be conservative and say "no" at the initial gate. A CARTA strategic approach moves away from one-time intensive security gating decisions, and toward real-time, continuous, adaptive, risk- and trust-based "micro" security decisions at runtime. This means we can spend less effort on the initial gating decision — which can never be perfect to begin with — because we are continuously assessing the implications of that initial decision.

Traditional security infrastructure was designed for more static IT environments housed in enterprise data centers with a focus on intensive assessments as initial allow or deny decisions were made (firewalling, intrusion prevention systems [IPS], antivirus, authentication and so on). All of this infrastructure must become context-aware and adaptive to different changing levels of risk and trust. Starting in 2014, Gartner pioneered research on building adaptive attack protection and access protection architectures using life cycle approaches, Figure 2 is focused on adaptive attack protection, or "keeping bad things out," and Figure 3 is focused on adaptive access protection, or "letting and keeping good things in."

In the figures below, the initial gating decision in the upper right of each figure is still important and continues to improve using additional context and enhanced analytical methods (such as machine-learning-based analysis of executable code for improved prevention decisions and adaptive authentication for improved access decisions). However, even with improvements, the initial gating assessment must be assumed fallible. Once in, the next phase (bottom right of Figures 2 and 3 below) must become our focus for the detection of excessive risk. Specifically, we must have visibility into what the entity — the user, the executable, the device, the network connection and so on — is doing once it gains access. How is it behaving? Does the entity or its behaviors represent excessive risk? If so, then we should have the ability to detect this, confirm that it is real, prioritize it and take action.

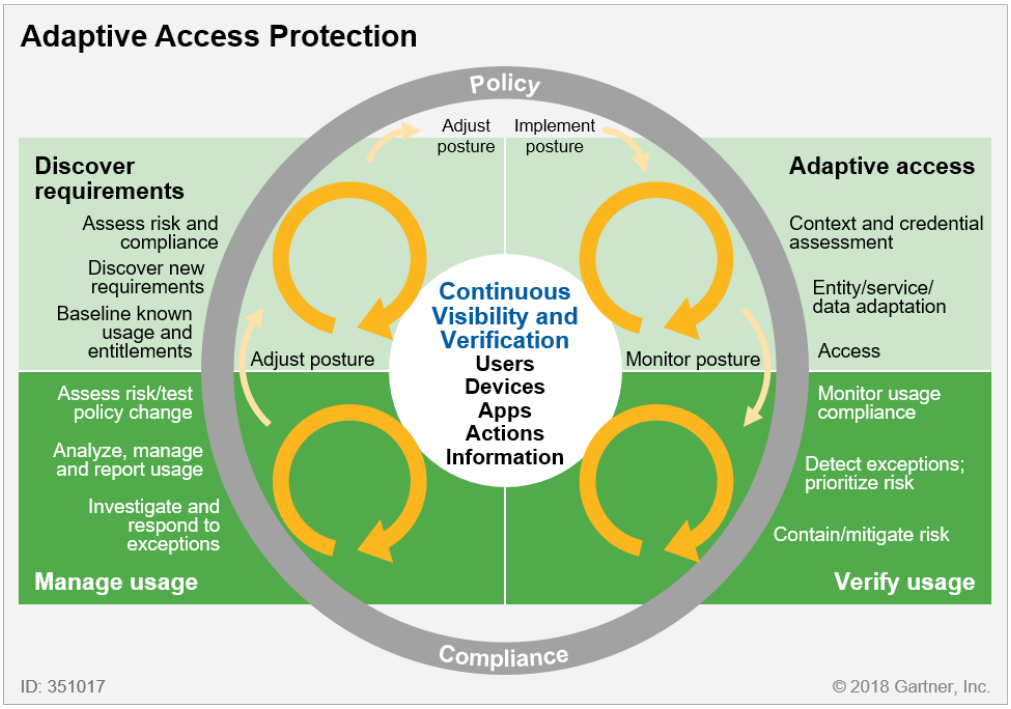
The security infrastructure used to allow/deny the initial access (upper right) shouldn't be siloed and separated from the need to monitor ongoing usage patterns (lower right). Attack and access protection must be treated as life cycle problems — from the initial access though the ongoing behaviors — until the session ends. Security infrastructure must evolve to support this. What was a simple yes/no security gate must evolve into integrated, real-time and runtime risk and trust assessment platforms. For example, endpoint EPP offerings are adding EDR, network firewall platforms are adding network traffic analysis capabilities, and authentication offerings are evolving into adaptive access control platforms. Security gates become continuous and programmable security sensors, providing runtime visibility and assessment of behaviors and adapting accordingly. The importance of programmable security infrastructure will be explored in more detail in a later imperative.

**FIGURE 2**
Adaptive Attack Protection




Source: Gartner (April 2018)

**FIGURE 3**
Adaptive Access Protection




Source: Gartner (April 2018)

## Imperative No. 2: Continuously Discover, Monitor, Assess and Prioritize Risk — Proactively and Reactively

Traditional security infrastructure treats risk and trust as binary and fixed, and often infers trust from system ownership. This won't work to support digital business, where IT is asked to provide anywhere, anytime access to systems and data to partners and customers on any device, often from infrastructure we don't own or control. In the world of digital business, risk and trust are fluid. Risk is continuously being created and the context is constantly changing. The level of trust that we have in the user, the application or device accessing our services and data is also constantly changing based on behaviors.

With a CARTA strategic approach, we must architect for digital business environments where risk and trust are dynamic and need to be assessed continuously after the initial assessment is performed. Once allowed into our systems and data, these entities — users, application processes, machines and so on — will interact with our systems and data, and all of these interactions must be monitored and assessed for risk and trust as they happen.

The relative risk and trust increases and decreases dynamically based on context and observed entity behaviors over the duration of the session (and against baselines established across sessions). Based on observed patterns, models of risk and trust can be developed. If the observed risk of an entity or its behavior gets too high and outweighs the trust, we can take steps to either decrease the risk or increase the trust of the entity and its requested action. For example, if a user attempts to download an abnormally large amount of sensitive data to an unmanaged device and this exceeds our risk threshold, we can:

- **Take steps to increase the trust:** For example, send a request to the user for stronger authentication to increase our assurance that the user is indeed who they claim to be. Alternatively, the user could be restricted to downloading only to a managed device.
- **Take steps to reduce the risk:** For example, wrap the content with digital rights management as it is downloaded or, alternatively, the download could be blocked altogether.

Low levels of risk will always be present — and, indeed, should be. With CARTA, our focus shifts away from the pursuit of perfection and elimination of all risk and shifts to the discovery and elimination of unnecessary and excessive risk. Security and risk management leaders must acknowledge and embrace that perfect prevention, perfect authentication and invulnerable applications were never possible. In pursuit of perfect security decisions, we've created security and risk management infrastructure and processes that are an inhibitor to speed and agility. Indeed, perfection is the enemy of "good enough."

As we look across Figures 2 and 3, a common imperative becomes clear: A CARTA strategic approach means that risk and trust are continuously assessed, enabling adaptive security decisions even before the new digital business capability is made operational. This will require that we bring the discipline of situational awareness[1] and apply it to risk management, effectively delivering "situational risk intelligence."

Risk management cannot be just a reactive process (discovering excessive risk after it has been created). Digital business risks can be discovered, anticipated, predicted and assessed with risk-prioritized pre-emptive actions taken to change the organization's security and risk posture (the upper left of Figures 2 and 3). With a CARTA strategic approach, security and risk leaders actively pursue the continuous proactive and reactive discovery and assessment of risk in all disciplines of information security (see Table 1).

New technology categories are emerging to address some of these risk visibility gaps, such as breach and attack simulation tools, sensitive data flow mapping, cloud security posture management and risk-based vulnerability prioritization. Risk is always present. It's the lack of visibility and intelligent management of risk that can be catastrophic. The disciplined and structured approach to proactive and reactive discovery, assessment and response to digital business risk becomes an imperative for CARTA.

## Imperative No. 3: Perform Risk and Trust Assessments Early in Digital Business Initiatives

The prior imperatives focused on operational security and risk protection at runtime. However, the continuous discovery and assessment of risk must extend to the creation (see Note 1) of new digital business capabilities whenever and wherever new digital business capabilities are created or modified, such as:

- Application, service and product development
- IT-enabled systems procurement
- IT and BU-led consumption of new SaaS, platform as a service (PaaS) and infrastructure as a service (IaaS) services
- Download of new applications and services for installation locally
- Selection and deployment of new operational technology (OT) and Internet of Things (IoT) devices
- Opening of internal systems and data via application programming interfaces
- Digital business partnership formation
- Digital business delivery channels co-sourcing or outsourcing

In all of these areas, information security suffers from the same problems that we described in the previous sections — an overreliance on one-time intensive gating assessments that are cumbersome, outdated the moment they are performed and end up slowing the business down. Such assessments might include heavyweight dynamic application security testing (DAST) and static application security testing (SAST) in application development, or cumbersome "verification" checklists when new IT systems are being procured, or 100-page questionnaires when new cloud services are being considered.

We must stop treating new business capability creation and the protection of these capabilities at runtime in production as separate security and risk problems. The risk and trust assessment of these capabilities should be continuous and intertwined as new services/capabilities are requested, created, put into operation, modified and ultimately retired (see Figure 4).

In all of these examples, we need to add the capability for CARTA to "shift left" (see Note 1) and bring risk and trust assessments as close to the genesis of new digital business capabilities as possible. These risk and trust assessments need to adapt to the user's world — their tools and their processes — not the other way around. For example, DevSecOps integrates security testing automatically and

**TABLE 1**

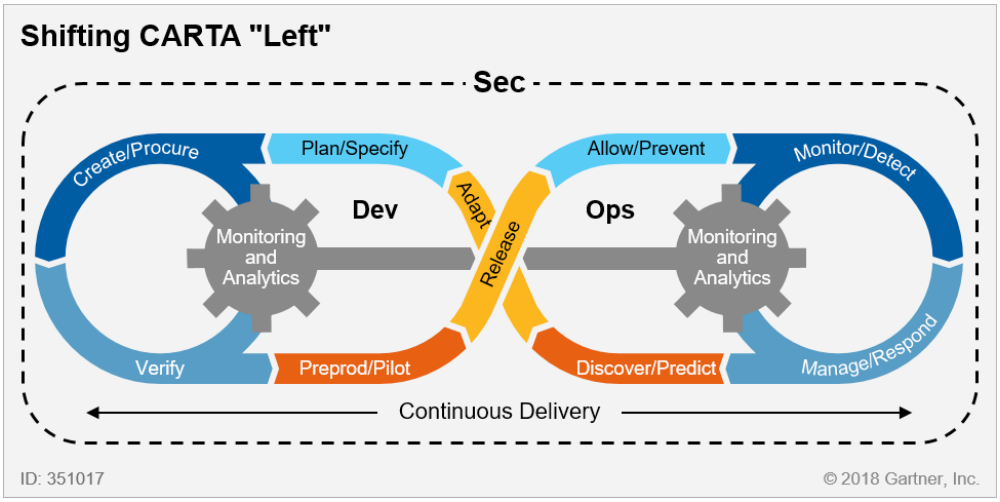
Proactive and Reactive Risk Discovery and Assessment

| Security Discipline | Proactive Risk Discovery | Reactive Risk Discovery |
|---|---|---|
| **Attack Protection** | • Where and how will attackers target? How real is the threat?<br>• How should I adjust my security posture to reduce my exposure to the threat?<br>• What can I do proactively to improve my surface area for attack?<br>• How can I risk-prioritize my vulnerability remediation efforts?<br>• Where does it make sense to proactively test my controls? (For example, continuous penetration testing, breach and attack simulation; see "Hype Cycle for Threat-Facing Technologies, 2017.") | • Where am I breached?<br>• Are these attacks real, and what incidents represent the most risk? |
| **Identity and Access Management (IAM)** | • Where and how will users need access? (For example, to new SaaS apps, BU apps and so on.)<br>• How common is this access?<br>• How much risk does this represent?<br>• How can I reduce the risk using controls (privileged access management, multifactor authentication)?<br>• How critical and sensitive are these resources?<br>• How can I provide just-in-time, just-enough access to a given resource?<br>• How much assurance do I need that a user is who they claim to be before providing access? | • Where do user access/usage patterns represent enough risk that I need to respond? How confident am I that the incident is not a false positive?<br>• How valuable is this user? The system/data they are accessing?<br>• What is the current threat level?<br>• Is there a pattern of suspicious activity across multiple users/domains?<br>• Where is user access overly permissive? |
| **Data** | • Where is sensitive data created in my enterprise?<br>• Where is sensitive data created and stored outside of my enterprise?<br>• What is considered "valuable," and why?<br>• How is sensitive/valuable data being protected?<br>• Is the risk managed? | • Where is sensitive data being mishandled?<br>• How sensitive/valuable is that data?<br>• Does this represent enough risk that I need to respond? |
| **Business Continuity Management (BCM)/Resiliency** | • What areas/processes of the business represent the most impact to revenue if the service is lost?<br>• Which systems support these? | • In the event of suspected failure:<br>• Is the failure confirmed?<br>• What business processes and revenue are at immediate risk?<br>• What systems/processes must be restored first? |

Source: Gartner (April 2018)

**FIGURE 4**

Shifting CARTA "Left" Into DevSecOps (Dev/Build) and Procurement (Buy)




Source: Gartner (April 2018)

transparently into the developer's continuous integration/continuous deployment (CI/CD) pipeline. Security should strive to provide guiderails — not gates — within which the user goes about their work to create the new capability. The guiderails, or high-level policies, may include separation of duties, auditing and logging of activities, background scanning audit, and encryption. As long as the new capability stays within the guiderails, security doesn't get in the way. Even when a warning of excessive risk is raised, it should be in their workflow, their processes and within their tools (in the DevSecOps case, in the developer's CI/CD pipeline). And, as discussed earlier, CARTA risk/trust assessments should be proactive (before production, left side of Figure 4) and reactive (in production, right side of Figure 4), answering questions similar to those shown in Table 2.

New technology categories are emerging to address some of these risk visibility gaps. These include software composition analysis in development to identify risks in open-source software, security rating services for assessing the risk and trust posture of digital business partners, cloud security posture management offerings and emerging interest in independent certification programs for security testing of third-party software and hardware.2 We can use information gathered from the left side of Figure 4 to better deliver protection at runtime — the right side of Figure 4. Examples of improved protection include building whitelist profiles of applications in development for enforcement at runtime, establishing behavioral and network connectivity patterns, using digital signatures to ensure no tampering has occurred, and passing knowledge of vulnerabilities to runtime security controls (such as IPS, WAFs and runtime application self-protection). Finally, security and risk management leaders cannot assume that we will be involved in advance with the creation of all of these new digital business capabilities. Thus, we must also be constantly be monitoring for the creation and consumption of new business capabilities that we weren't aware of. For this reason, discovery and baselining become critical continuous assessment capabilities (in the upper left of Figures 2 and 3). This is especially true with the consumption of cloud-based services (where the barrier to adoption is a browser and a credit card) and why most cloud access security broker (CASB) projects start with a cloud application discovery and risk assessment.

## Imperative No. 4: Instrument Infrastructure for Comprehensive, Full Stack Risk Visibility, Including Sensitive Data Handling

At the center of Figures 2 and 3, are the words "continuous visibility and verification." Essentially, these circles represent CARTA risk and trust assessment engines that make adaptive security decisions continuously. But what exactly are we monitoring and assessing the risk and trust of?

The answer: everything possible.

The goal should be visibility into the portions of the stack wherever possible. Traditional security infrastructure was overly reliant on network and endpoint visibility. However, this won't work when we no longer own the network,

**TABLE 2**

Proactive and Reactive Risk/Trust Assessments

| Security Discipline | Proactive Risk Discovery | Reactive Risk Discovery |
|---|---|---|
| **Application Security** | • Where are the vulnerabilities in the new code/services?<br>• Where are licensing risks if open-source software is being used?<br>• Using simple threat modeling for new services, data and applications, what are the ways this business capability can be attacked?<br>• What is my confidence that the risk is real?<br>• How important is this business capability?<br>• Is the risk great enough that it needs to be addressed? | • Where are the vulnerabilities in running applications?<br>• Are there real attacks on these applications?<br>• Is the risk great enough that I need to take action?<br>• If the system can't be patched, what mitigating controls might be used (for example, web application firewalls [WAFs] and intrusion prevention systems [IPS], or virtual patching)? |
| **Procurement** | • What risk does this potential vendor's product/service represent?<br>• Does the vendor use a proactive bug bounty program?<br>• What is the vendor's track record for timely vulnerability disclosure and patch delivery? | • Have new vulnerabilities been discovered and disclosed?<br>• Are there real-world attacks on the vendor's offerings?<br>• How valuable is the process/asset?<br>• Who is responsible for tracking vulnerabilities and risk in OT/IoT systems? |
| **Digital Ecosystems** | • How much risk does a potential digital ecosystem partner represent?<br>• What systems and information would they have access to? | • Once connected and up and running, has my partner's security posture changed?<br>• What processes/assets are threatened as a result? How valuable are these?<br>• What new partners have they connected to, and how does this affect my risk posture? |

Source: Gartner (April 2018)

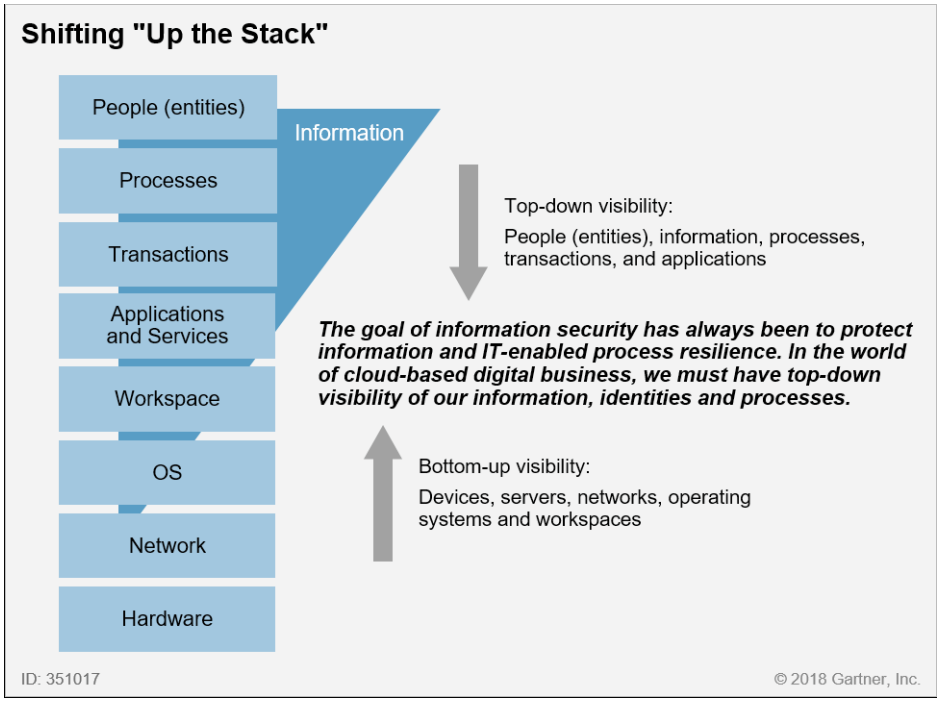
server, OS or application with SaaS apps, and where we often don't own or manage the device. Network security and endpoint security were a "means to an end" — but the end goal of information security has always been the protection of workloads and information. Security and risk management leaders must become as adept at the visibility and protection of entities, applications and data as we have been at protecting networks and endpoints in the past. This will be especially critical for protecting users and data in cloud-based services through visibility and assessment of user actions, interactions, transactions and handling of sensitive data.

Bottom-up endpoint and network visibility are still important (when we have it), but must be augmented with visibility from the top down, as shown in Figure 5. In all cases, the goal is to detect excessive risk as quickly as possible when it happens by ensuring visibility into as much of the stack as we have access to. We will monitor everything where possible — all actions, interactions, transactions and behaviors that deliver situational awareness of users, devices and their behaviors. This full-stack visibility provides detailed retrospective analysis and forensics in the event of a breach or insider threat, and provides the information needed for root cause analysis. Further, the detailed visibility can be used to roll back actions if an entity and its behaviors are later found to be malicious.

To provide visibility into users and data behaviors and interactions, multiple technology categories are appearing

**FIGURE 5**

Shifting "Up the Stack" to Identities, Data and Transactions




Source: Gartner (April 2018)

addressing this need. One example is user and entity behavior analytics (UEBA) focused on sensitive data, monitoring, interactions and transactions. Embedded UEBA capabilities have become critical in monitoring for excessive risk in cloud services where user actions and data sensitivity are available via application programming interfaces. For example, leading CASBs provide this capability, as well as some IaaS providers, such as Amazon Web Services (AWS) with Amazon Macie.[3] This leads to another critical subimperative:

> **Security operations must extend to include identity/entity-related, data-related and process-related risk assessment and monitoring.**

Traditional security operations center (SOC) monitoring and response has focused on the rapid detection and response to attacks — activities in the lower right-hand corner of Figure 2. However, access-related risks, such as theft of sensitive data, insider threats, and account takeover by attackers, must also be detected and responded to (lower right-hand section of Figure 3). In digital business, the detection of risk in how sensitive data is being used might be as important as that of a denial of service attack on a server. Both incidents represent risk, and must be prioritized so that our limited SOC resources can focus their efforts. In many cases, these risks are intertwined (the malicious actor infiltrates the organization and then tries to steal sensitive data), so we must stop treating these as separate problems.

Further, when excessive risk is detected, part of the response effort may include use of the IAM fabric — revoking access, terminating sessions, quarantining accounts or requiring step-up authentication. We are seeing examples of IAM response integration from security information and event management (SIEM) vendors such as Oracle's Identity SOC[4] and Symantec's CASB, CloudSOC.[5] We must have the ability to detect and respond to excessive risk of all types — entity, application, data, process and attacks, and to risk-prioritize our remediation efforts.

## Imperative No. 5: Use Analytics, AI, Automation and Orchestration to Speed the Time to Detect and Respond, and to Scale Limited Resources

The amount of time it takes for security teams to detect and respond to excessive risk (with a goal of preventing or minimizing the financial impact) will be one of the most critical security metrics over the next decade. Further, as we discussed in the prior imperative, the need for full-stack visibility — beyond the initial gating decision and up the stack to users and data — will generate vast amounts of behavior data ("big data") including network, endpoint,

users, transaction and data usage. The sheer volume, velocity and variety of data inhibits our ability to detect and respond effectively to excessive risk. Security analysts are overwhelmed with events and alerts, most of which are false positives or represent low risk. To identify meaningful indicators of risk, this data must be analyzed using multiple analytic approaches, including the use of:

- Traditional signatures
- Behavioral signatures
- Correlation
- Deception techniques
- Pattern matching
- Baselining and anomaly detection by comparing to historical behavioral patterns and peers (groups or organizations).
- Entity link analysis
- Similarity analysis
- Neural networks
- Machine learning (supervised and unsupervised)
- Deep learningWe must acknowledge that the identification of risk in a digital business will require a set of layered, mathematical and analytical approaches against an ever-increasing dataset. Techniques like signatures and pattern matching require less compute power and time. Techniques like machine learning will take longer and require historical datasets to work against. Machine learning and deep learning will be essential to detecting digital business risk, but can be fooled like any other single layer in security.6

Overreliance on a single analytic or mathematic technique will leave organizations exposed. The best security vendors and platforms will use multiple layers of analytic techniques to better detect and surface meaningful risk to focus our limited resources on real and important risks. The effect is much like a funnel taking billions of events and using analytics and context to distill these into the handful of high assurance, high value and high risk incidents that the security team must focus on each day.

**The security principle of "defense in depth" must extend to analytic methods: "analytics in depth."**

Every facet of security and risk will require advanced analytics and machine learning, including next-generation attack protection platforms, access protection platforms, data protection risk, and development risk (see Note 2). The use of analytics will speed our time to detect risk. Automation, orchestration and artificial intelligence (AI) will speed our time to respond. We must use automation, orchestration and AI to act as a force multiplier, improving the efficiency and effectiveness of our limited security operations resources. We don't have time to investigate every incident. Big data analytics and machine learning will allow our limited staff to focus on the intersection of three critical questions:

- Is the risk detected real?
- How dangerous is this risk?
- Is the object at risk important?

The latter is why context is so critical to making risk-based security decisions. For example, a file share (such as an Amazon S3 object storage bucket) open publicly may be risky, but might be a legitimate use case for sharing files. However, a file share open publicly containing sensitive data is entirely different, represents immediate and important risk, and likely should be automatically unshared. The difference in these two examples is context — focusing on what's important based on the business value of the asset, service or sensitivity of the data involved.

Automation and AI will go hand in hand. Using a biological metaphor, humans don't decide to raise their white blood cell count to fight an infection; it happens automatically. Likewise, we believe more routine security decisions will also be highly automated and some will be autonomous. This will free up time for security analysts to triage and focus on the issues that represent the highest risk to the organization and that cannot be automated. Full automation should be applied first where we have highest assurance of the risk with well-understood remediation actions (an example is the quarantine of sensitive data if it is exposed on a public share). In other areas, the ability to automate lets security professionals decide when and where automation can be applied without human intervention.

Automation decisions powered by machine learning and AI (see Note 3) techniques will help for responses that can't be fully automated. For example, AI will be used in human-assisted, SOC analyst decision support systems. Here, the SOC analyst can be guided through a standardized playbook for response actions, or the analytics can provide an intelligent, prioritized list of suggest actions from which the analyst can choose. Enterprises will see significant improvements in SOC efficiency and effectiveness by automating routine tasks and, for more complex tasks, using AI to guide the analyst through the remediation and taking automated actions based on what they decide. For automation, Gartner research has explained the importance of security orchestration automation and response (SOAR) capabilities as another significant growth

area within information security. SOAR will help build out a CARTA strategic approach.

Finally, visualization capabilities on top of the analytics will become critical to navigate large datasets — network flows, user behaviors, system behaviors, data flow, application connectivity and so on. It will be necessary for security analysts to visualize these relationships to better understand and interpret data. For example, a security analyst may visualize a chain of events to understand how individual events relate to one another, the path of the attacker, systems impacted and data exfiltrated.

## Imperative No. 6: Architect Security as an Integrated, Adaptive Programmable System, Not in Silos

Traditional security infrastructure has provided protection in silos, separating the disciplines of network, endpoint, application, data security and IAM. Development security is also often separated from runtime security. There are multiple problems with this approach:

- Siloed controls create too many vendors and consoles, increasing complexity and increasing the chance for misconfiguration.
- Each silo on its own doesn't have enough context for high assurance detection, creating too many alerts. Many of these are false positives or represent low risk.
- Events from siloed controls are often forwarded to a SIEM, which may or may not be able to make sense of the additional events (garbage in, garbage out). This creates yet another source of alerts, many of which are false positives or represent low risk.

The reality is that advanced attacks span our internal security silos. For example, an attacker launches an email based attack containing a URL that links to malicious content. This content is loaded on an endpoint, where it attacks a vulnerability to launch a payload to monitor keystrokes so that it can gain credentials. These are then used to spread laterally to other systems, and ultimately access and exfiltrate sensitive data. Like the story of the blind men and the elephant,[7] each silo has a piece of the story, but none have the entire picture. The best security protection will work as a system combining visibility across these silos — or eliminate them entirely — for improved detection. When an incident is discovered, the offending entity (user account, file, URL, executable and so on) can be communicated and blocked across all channels immediately — endpoint, server, email, web, and network — to prevent further infections. Early examples of this capability are emerging in academic research,[8] in open initiatives such as OpenDXL and in commercial offerings such as pxGrid.

**"Keeping the bad things out" and "letting and keeping the good things in" are fundamentally the same problem, if you assume the initial gating decision is fallible.**

Scanning a file for malware or sensitive content is fundamentally the same problem of discovering and identifying patterns of bits that resemble "badness" or "goodness." At the end of the day, it's all patterns. The move to cloud-based services will force some of this convergence of security controls. As an example, leading CASBs unite threat, identity and data protection in their offerings, providing both malware inspection and credential theft/abuse and sensitive data monitoring from a unified platform.

The vision of "anywhere, anytime" access to digital business services and data by customers and partners won't be realized with static security infrastructure, trapped in a box and anchored at a no-longer-relevant perimeter. Security controls must become a logical "fabric," placed when and where they are needed to monitor and assess risk and trust where possible. In many cases, these controls will be delivered from the cloud itself with control around the workload or information regardless of location. This is radically changing how and where security controls are delivered and priced, which in turn is reshaping security markets (see Note 4). On-premises network security appliances will still have a role to play, but diminishing over time as more and more of our enterprise workloads and information reside outside of enterprise perimeters. The shift to security as a system will affect how we select security solutions in several key areas. Security platforms must:

- Be software-based, fully programmable and accessible via application programming interfaces.
- Be capable of exchanging context, using standards such as STIX, TAXII or JSON, and of supporting industry information sharing and analysis centers, such as FS-ISAC, OpenDXL or pxGrid.
- Shift from intensive one-time allow/deny assessments to continuous assessment with risk-based adaptive outcomes.
- Integrate seamlessly into modern IT environments — cloud, containers and DevOps CI/CD pipelines.
- Not penalize customers for storing and analyzing ever-increasing amounts of data, as more and more visibility (and thus data) is needed for efficient and effective security decision making.

- Not be reliant on a single analytic approach. Instead, use multiple approaches and analytic methods to provide protection, including embedded machine learning and behavioral analytics.
- Leverage rich ecosystems and sources of threat intelligence (TI). Ideally, using correlated visibility across customers to create a community effect and network effect, visibility and sharing of TI across customers. This should span local intelligence (what is happening for your organization) and global (what organizations of similar size in your industry and in your geography are observing).

## Imperative No. 7: Put Continuous Data-Driven Risk Decision Making and Risk Ownership Into Business Units and Product Owners

Our risk governance and compliance processes suffer from the same limitations of one-time macro security gating assessments that we have discussed previously. We use rigid and lengthy controls and compliance checklists to gauge the efficacy of our security program. We need to coalesce a CARTA strategic approach to risk management, moving away from static checklists and making data-driven risk visibility and assessment a continuous process. This mindset is captured within an approach Gartner calls integrated risk management (IRM; see Note 5). And as before, this digital business risk can be assessed proactively and reactively (see Table 3).

New technology categories are emerging to address some of these risk visibility gaps, such as integrated risk management platforms and digital risk management via controls gap analysis. Leading IT risk management platforms are evolving to provide risk visibility into hybrid cloud workloads and integrate with ERP, CRM, configuration management database (CMDB) and SOAR platforms, both on- and off-premises. Many of these platforms rely heavily on analytics, machine learning and visualization to prioritize and highlight areas of risk, and to provide recommendations on how to remediate them. Adopting the owner accountability principle is a key requisite for bringing CARTA to risk management. The ultimate accountability for protecting the enterprise's information resources and, by implication, its business processes and outcomes, rests with the business owners of the information resources. The resource owners must have the authority to make the data-driven, risk-based decisions required to fulfill their accountability. Expecting the security team to make these decisions on acceptable levels of trust and risk on behalf of the business will hamper adoption of a CARTA strategic approach.

In the spirit of DevOps (which tore down the walls between development and operations, as shown in Figure 4), we need to apply this collaborative approach to risk management. We must embrace a mindset of "RiskOps" or "Risk<Build>Ops" with a goal of tearing down the walls between business leaders and operational risk-based visibility and impacts (see Figure 6).

**TABLE 3**

Proactive and Reactive Digital Business Risk Assessments

| Security Discipline | Proactive Risk Discovery | Reactive Risk Discovery |
|---|---|---|
| Risk Management | • What new digital business initiatives are planned?<br>• What are existing digital initiatives with a low threshold of reputation risk?<br>• What new regulatory requirements am I subject to, and what is the internal political appetite to meet them?<br>• What are the cyber risks to this?<br>• How serious are these cyber risks?<br>• How valuable is the new initiative (revenue, cost, liability)?<br>• What new business opportunities are available if I accept more risk?<br>• What commitments to shareholders or other stakeholders need to be back-traced to digital-business-related risk decision making? | • What is my overall risk posture across all BUs, partners, projects and infrastructure?<br>• Where are areas of high risk?<br>• Where am I out of compliance, and how much does it matter?<br>• What assets/services are at risk, and what value do they represent?<br>• What security controls are missing, and what risk does this represent? |

Source: Gartner (April 2018)

Providing risk visibility and the shift to data-driven risk decision making in the hands of BU and product owners completes our vision of a CARTA strategic approach. Security and risk management must become a set of intertwined, continuous, and adaptive processes (see Note 6). With CARTA, our governance and planning process creates a risk-aware mindset and becomes data-driven. Working with the business units, we define acceptable levels of trust and risk that translate into the guiderails of security policies. These policies and acceptable risk levels flow throughout our security infrastructure, changing:

- How we build and acquire new IT-enabled services
- How we assess and evaluate new digital business ecosystem partners
- How we protect and enable runtime access to our systems and data

When security decisions are made, they are constantly assessed to ensure that risk/trust are balanced to a level of risk that the business — not IT — finds appropriate.

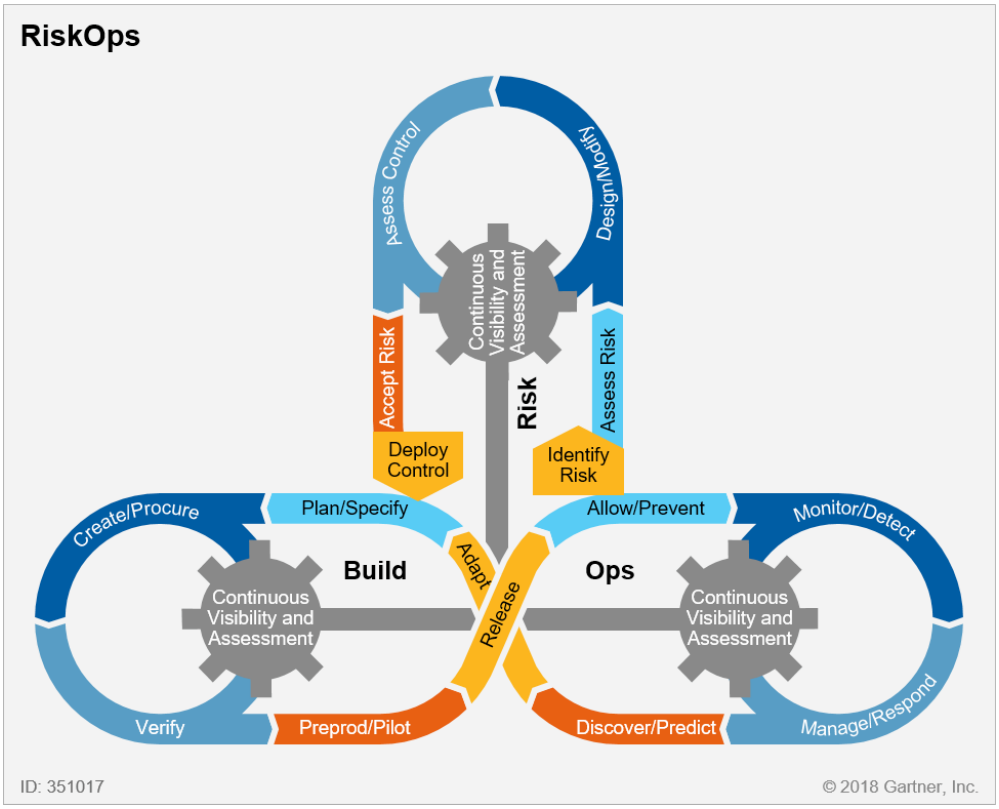
At runtime, we are constantly checking what we observe against what we expect, bringing the concepts of continuous monitoring, continuous assessment and continuous improvement to security protection and risk management. If excessive risk is detected at runtime, this visibility can be surface first through the SOC and ultimately to the business owner if needed. Risk is not avoided; it is monitored, assessed, balanced with trust, communicated and adapted to acceptable levels — continuously. This is the embodiment of a CARTA strategic approach.

*Additional research contributions by Ant Allan, Felix Gaehtgens and Khushbu Pratap.*

## Evidence

[1] Wikipedia, "Situation awareness."
[2] UL, "Cybersecurity" and CA Technologies, Veracode Community, "CA Veracode Verified."
[3] AWS, Amazon Macie.
[4] Oracle, "Oracle Identity SOC Solution."
[5] Symantec, Cloud Access Security Broker.

**FIGURE 6**
**CARTA-Inspired Risk Management: RiskOps**




Source: Gartner (April 2018)

[6] Nguyen A, Yosinski J, Clune J. "Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images." In Computer Vision and Pattern Recognition, IEEE, 2015.
[7] Wikipedia, "Blind men and an elephant."
[8] E.N. Crane, "Emergent Network Defense," The George Washington University, 2013.

## Note 1. "Shift Left"

Many vendors and some trade publications refer to this as "shifting left." While partially accurate, we want to be clear that the need to protect at runtime in operations (the right side of Figure 4) is equally as important. "Shift left" doesn't replace the need for runtime protection capabilities; it strengthens it.

## Note 2. Machine Learning in Data Protection and Application Security Testing

Data protection platforms, analytics and machine learning will be used to build models of what is sensitive and what is not by training against corpuses of data. In application development, where SAST tools have traditionally been plagued with false positives, the use of machine learning can be used to intelligently trim the results for developers (this is called "intelligent finding analytics," or IFA; see "Magic Quadrant for Application Security Testing").

## Note 3. AI

Gartner defined "big data" through the volume, variety and velocity of the data that organizations found themselves facing. This is especially true in information security, as we move to instrument more and more of the IT stack, including user behaviors and data flows. AI can be seen as converting such overwhelming information and data flows into granular insights on which AI-driven systems may take automated actions — in this case, the security operations analyst.

## Note 4. Sea Change in Security Controls to Software and Cloud Delivery

Examples of change include:

- The shift to software-based security controls over hardware
- The use of cloud access security brokers to gain visibility and control of sensitive information in cloud-based services
- The move toward cloud-based delivery of network security services, such as:
- Remote and mobile worker secure web gateway services
- Email protection
- CASB services
- Back-end detection and response analytics (and interenterprise visibility)
- Branch-office unified threat management services for direct-connect projects
- The adoption of software defined access perimeter solutions as replacements for legacy demilitarized zone (DMZ) and VPN architectures
- Cloud providers entering the security market directly with cloud-based monitoring of cloud workloads for indications of compromise, such as AWS GuardDuty and Microsoft Azure Security Center

## Note 5. Integrated Risk Management

Gartner defines "integrated risk management" as a set of practices and processes supported by a risk-aware culture and enabling technologies. It improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

## Note 6. Reimagining Security and Risk as Continuously Improving, Continuously Adapting Processes

Continuous and adaptive security decision making
Continuous and integrated risk management
Continuous application security testing
Continuous asset, entity and service discovery
Continuous authentication
Continuous authorization
Continuous compliance
Continuous data monitoring
Continuous exposure testing
Continuous identity trust assessment
Continuous monitoring and visibility
Continuous protection
Continuous risk assessment
Continuous risk discovery
Continuous risk-prioritized response
Continuous security posture assessment
Continuous trust assessment
Continuous vulnerability assessment (for example, see the U.S. Department of Homeland Security's page on Continuous Diagnostics and Mitigation [CDM])

# ABOUT FORCEPOINT

**Harnessing the best defense for your critical data and IP. Your people.**

Purpose-built and ready to protect, Forcepoint is driven by an understanding of human behavior and intent. Our innovative technology, decades of experience and clear vision help solve critical security issues to protect employees, business data and IP.

We offer a systems-oriented approach to insider threat detection and analytics, cloud-based user and application protection, next-gen network protection, data security and systems visibility. It's a new approach to cybersecurity never seen before. And as technology and users' needs evolve, we are constantly looking to expand our offerings while staying true to our core in protecting the human point.

Through our 20 years of frontline experience, proactive and context-based technologies, and data-centric, integrated solutions, Forcepoint enables better decision-making and more efficient security at the human point for more than 20,000 government organizations and enterprises world-wide.



FORCEPOINT forcepoint.com