

Gartner.

Licensed for Distribution

This research note is restricted to the personal use of Ilan Afriat (ilanaf@cyber.gov.il).

2020 Planning Guide for Security and Risk Management

Published 7 October 2019 - ID G00407409 - 55 min read

By Analysts [Ramon Krikken](#), [Mario de Boer](#), [Joerg Fritsch](#), [Patrick Hevesi](#), [Anna Belak](#), [Augusto Barros](#), [Michael Isbitski](#), [Mike Wonham](#), [Mark Judd](#), [Jon Amato](#), [Richard Bartley](#), [Frank Catucci](#), [Thomas Lintemuth](#), [Michael Kranawetter](#), [Dennis Xu](#), [Michael Clark](#)

Initiatives: [Technology, Information and Resilience Risk for Technical Professionals](#) **and 4 more**

The security landscape is ever-changing, but control selection and implementation are becoming particularly challenging. Security and risk management technical professionals must understand major security trends to continue practicing strong planning and execution of security initiatives in 2020.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- [2020 Planning Guide Overview: Building Skills for Digital Transformation](#)

Overview

Key Findings

- Security teams find it difficult to keep up with change. Evolving risk, compliance, business and IT landscapes create new exposures. And the increasingly large and puzzling security product landscape makes it a major challenge to pick an effective and cost-efficient mix of controls.
- Advanced technologies enable quicker detection of and response to incidents. However, they cannot compensate for immature practices or a lack of skilled personnel. These technologies often demand advanced skills – in-house or outsourced – to use and manage them.
- Deploying security in multicloud and across diverse environments remains challenging. But the evolving capabilities in and around these solutions now often allow implementation of adequate infrastructure, application and data security through native and add-on controls.

- Increased availability of multifunction and orchestrating security tools leads to challenges when addressing technical issues. Strategic approaches to cloud, mobile and data security are evermore important to balance cost and functionality, but come with risk of “analysis paralysis.”

Recommendations

Technical professionals responsible for security and risk management should:

- Address high-exposure risk areas and security hygiene controls first. Ensure that current or newly internet-exposed assets – such as through cloud email migration – are protected. Concurrently, implement baseline security controls that broadly reduce security risk.
- Establish security architecture as a foundational practice. Augment existing risk management and control frameworks with architecture models that factor in capabilities, maturity, and threats and attacks. Use these models for global and project-based gap assessments and roadmaps.
- Avoid buying products, whether dedicated or multifunction platforms, solely because of tactical problems in a single area. Instead, take a step back and define a plan that includes solutions and vendors that fit the organization’s longer-term security architecture, IT and business needs.

Security and Risk Management Trends

Gartner Welcomes Your Feedback

We strive to continuously improve the quality and relevance of our research. If you would like to provide feedback on this document, please visit [Gartner GTP Paper \(https://surveys.gartner.com/s/gtppaperfeedback?ID1=105\)](https://surveys.gartner.com/s/gtppaperfeedback?ID1=105) to fill out a short survey. Your valuable input will help us deliver better content and service in the future.

Cybersecurity has long been a major concern for organizations, and security teams have found it challenging to keep up with the changing threat, risk, compliance, business and IT landscapes. Data is being used in more places, for more business purposes and by more partners in the digital business ecosystem. Applications and APIs are expanding to make more business functionality accessible, and cloud makes critical applications, such as email and content sharing, accessible to a wide range of attackers. ¹ In addition to data breaches ² and ransomware, ³ abuse and fraud are an increasing threat. Each threat corresponds with one or more security practices, which are illustrated in Figure 1. These practices provide a way of grouping controls that supports threat analysis, tool selection and architectural processes (see Figure 1).

Figure 1. 2020 Key Planning Considerations for Security and Risk Management

2020 Key Planning Considerations for Security and Risk Management

Major Changes in Compliance and Risk Impact Security Program and Roadmap

- Evangelize pragmatic approaches to risk
- Triage high-exposure risk areas
- Improve third-party assessment and control

Security Solution Architecture Is Increasingly Driven by Integrated Platform Approaches

- Create a security capability model
- Use threat and attack models
- Evaluate integrated cybersecurity platforms

Ecosystems Cement the Need for Data-Centric Security Architecture and Application Security

- Create discovery, visibility and control
- Design flexible security for data and analytics
- Enhance application and API security practices



Effective Security Monitoring and Response Depend on Automation and Analytics

- Develop and enhance incident response
- Focus on activity and access monitoring
- Assess machine learning and deception

Containers, DevSecOps, Hybrid Cloud and Multicloud Transform Infrastructure Security

- Embrace DevSecOps for automation
- Modernize network, workload, data security
- Emphasize visibility, monitoring, management

Mobile Devices, Things, Agents & SaaS Drive Need for Native Security & Security Add-Ons

- Implement endpoint threat and data protection
- Design mobile security with cloud AppSec
- Factor IoT devices, agents into security plans

Source: Gartner
ID: 407409

Clients are at many different levels of security maturity, which is why the planning considerations for 2020 cover many security controls within each practice. Each practice has basic hygiene controls, such as firewalls and compliance management, and more advanced options, usually selected based on specific risk and organizational capability. Many of last year's recommendations remain, thus providing a steady foundation for building maturity. None of the past few years' security concerns has gone away. 2020 will continue to bring increased exposure due to expansion of digital business ecosystems (digitalization), further convergence of IT and operational technology (OT), increased presence of the Internet of Things (IoT), and more widespread adoption of third-party services. Additionally, even in the face of changes in the compliance and risk landscapes, organizations have to remain pragmatic and continue advancing their security programs and architecture initiatives based on a solid security baseline. Teams with members from different organizational areas and with varied domain expertise will be necessary to help enable a streamlined triage, assessment and decision-making process for control selection.

However, recent trends show many security teams will need to slightly shift focus in order to keep up with attacks and changes in the security solution landscape — although for some, this small shift will represent a major effort. New or significantly enhanced areas for 2020 include:

- Planning for including a data-centric security architecture (DCSA) approach in the security strategy and roadmap

- Strengthening security architecture in light of the emergence of integrated cybersecurity platform solutions from major vendors
- Addition of new or updated security technology categories for:
 - Security orchestration, automation and response (SOAR)
 - Data access governance (DAG)
 - Expanded cloud security platforms:
 - Cloud access security broker (CASB)
 - Cloud workload protection platform (CWPP)
 - Cloud security posture management (CSPM)
 - Zero-trust network access (ZTNA)
 - Remote browser isolation (RBI) used in context of CASB and ZTNA

The subsequent sections describe the following key security and risk management trends, which will broadly affect organizations in many industries, geographies and sizes:

- Major changes in the global compliance and risk landscapes will continue to impact security program and roadmap planning.
- Security monitoring and response will continue to depend on automation and analytics delivered through internal skills and managed services.
- Security solution architecture will be increasingly driven by integrated cybersecurity platform approaches.
- Containers, DevSecOps, hybrid cloud and multicloud will transform infrastructure security architecture and management.
- Ecosystems will cement the need for data-centric security architecture and application security.
- Mobile devices, things, intelligent agents and SaaS will drive expansion of native security capabilities and add-ons.

The relative importance of each of the trends and its related planning considerations will depend on an organization's current maturity in digital business and IT, as well as its security posture. The Setting Priorities section at the end of this Planning Guide provides additional guidance on how to approach planning:

1. Triage high-exposure risk areas and basic controls first.
2. Use security architecture as foundational practice.
3. Engage nonsecurity stakeholders early and often.

However, not all aspects of security and risk management can be addressed in this Planning Guide. The focus is on advising IT security professionals, with a heavy bent toward security architecture and technical practices. In particular, the following areas are out of scope:

- Industry-specific security and risk practices and technologies, such as those for OT and electronic payments
- Audit and compliance practices and technologies, as well as integrated risk management (IRM) platforms and tools
- Business continuity and disaster recovery (BC/DR) practices and technologies

Major Changes in the Global Compliance and Risk Landscapes Will Continue to Impact Security Program and Roadmap Planning

According to Gartner surveys and client feedback, security remains a top concern for business and IT leaders. This is partly due to the high level of visibility gained: Cybersecurity is highly visible in the media because of privacy concerns, destructive attacks such as ransomware and an increasingly noticeable effect of cybersecurity on geopolitics. The number of security regulations, usually but not always in the form of geography- or industry-specific compliance mandates related to protecting personally identifiable information (PII), is also still increasing. Uncertainty remains about how to effectively comply with regulatory mandates that leave ambiguity on which controls to use, or what the consequences of failure to comply will be. Small incidents may have a big fallout, and this increases the pressure on security teams. Improving business visibility and involvement in compliance and planning remains a primary condition for success.

Privacy and data breaches are top of mind. However, distributed denial of service (DDoS), extortion and fraud attacks also still prevalent, with highly visible and high-impact attacks affecting public-sector and private-sector organizations alike. Common attacks include ransomware, business email compromise, and credential phishing and stuffing. A particular challenge is increased exposure to attackers – for example, by the move to cloud-based services, which often makes previously firewalled users and administrative functions accessible via the internet. Because many traditional security controls don't encompass these newer environments, it is easy for an organization to incorrectly use or configure them, or miss their existence altogether. Such exposure can lead to devastating ransomware attacks, often accomplished through a difficult-to-detect slow attack that causes significant losses to the organization. Even newer technologies, such as increased use of robotic process automation (RPA) and the emergence of artificial intelligence (AI) and machine learning (ML) in business processes and applications, are largely uncharted cybersecurity territory.

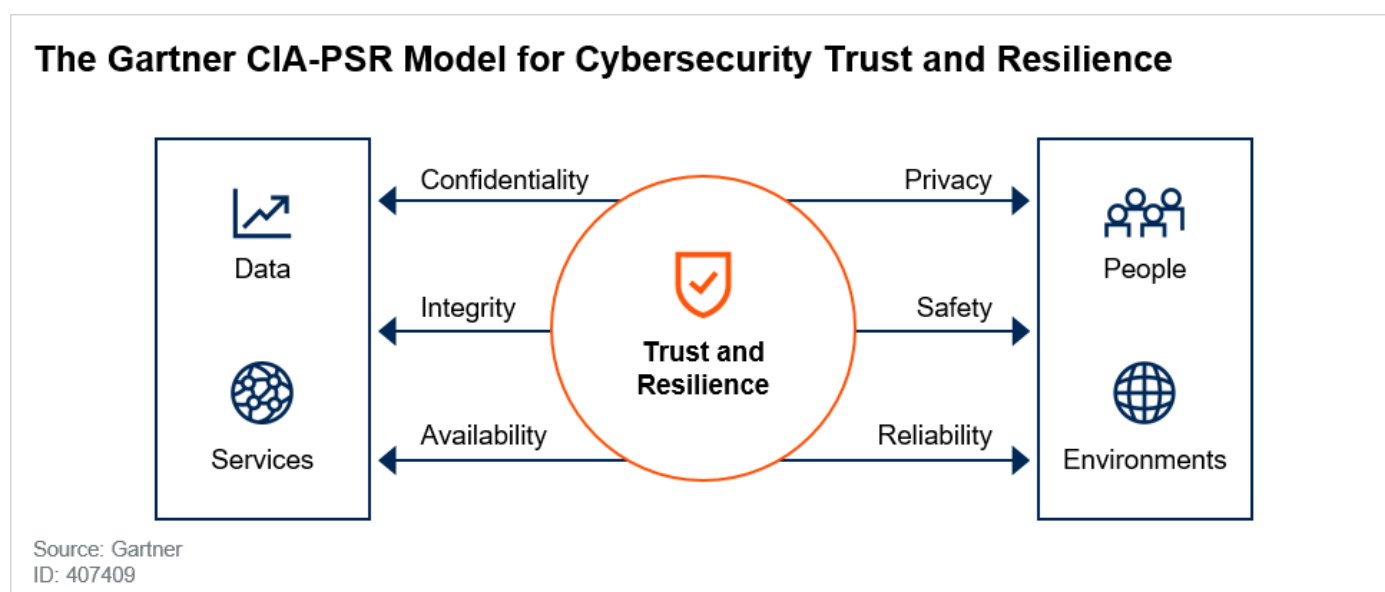
In addition, security teams are aware that they need to act as business enablers, but still often remain excluded from the start of a project. Faced with project time constraints, security teams – especially those with few resources – find it easier to follow a compliance and audit checklist than to spend time on effective risk analysis and control selection. Third-party security assessments, which are often driven by compliance requirements, and third-party risk management are proving particularly time-consuming. But even just creating visibility into use of third-party services is a challenge for security teams. Continuing the last few years' trend, security personnel are still hard to hire and retain, with some industry estimates of up to 3 million cybersecurity job openings during 2018. ⁴

Planning Considerations

Evangelize a Pragmatic Approach to Cybersecurity Risk and Compliance

Ensure that risk assessments are aligned to well-understood business objectives. Invest time upfront to establish and document assessment objectives in business language, and prioritize the assessment activities around these objectives. The assessment must not only encompass risks relating to data breaches and privacy, but also account for other security objectives (see Figure 2 for the Confidentiality, Integrity and Availability-Privacy, Safety and Reliability [CIA-PSR] Model for Cybersecurity Trust and Resilience). Communicating security and risk means tailoring metrics and messages to different audiences and stakeholders, such as practitioners, IT managers, business managers and executive management. All need related, but different, views – in forms such as metrics, explanations and recommendations – that flow from the combination of operations, risk assessment, threat assessment, controls assessment and incident management processes.

Figure 2. The Gartner CIA-PSR Model for Cybersecurity Trust and Resilience



Work to build realistic expectations around risks, and around the performance and effectiveness of controls. First, cybersecurity risks must be viewed in the light of a larger enterprise risk framework in order to understand broader trade-offs and impacts. Second, you must have a pragmatic view of the cybersecurity risks themselves in order to avoid a narrow and intense risk focus. Use industry data to see what's dangerous today: open cloud file shares,

account takeovers and business email compromise, to name a few. Use “what-if” scenarios to select and also eliminate control choices. Full network encryption protects your organization from the slim chance of network sniffing, but also impedes security monitoring. Taking a pragmatic view on risks helps spend money more wisely and limits negative impact from overly burdensome security controls.

Conduct portfolio risk assessments to challenge current security patterns that no longer match the threat-and-attack or IT landscapes, and advocate for their replacement or deprecation. For example, recommend multifactor authentication and user monitoring instead of passwords, or utilize native security controls in cloud services rather than “forklifting” on-premises security technologies into the cloud. But make sure to not just drop well-established compliance controls such as password rotation, even if they are ineffective for current attacks or risks – this leads to challenges with respect to audits and regulatory examinations. It takes a while for “best practices” to change.

Related research:

- [“Build Once, Use Many Times: Use Privacy Engineering to Support a Data-Centric Security Architecture”](https://www.gartner.com/document/code/430106?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/430106?ref=authbody&refval=3970104)
- [“Developing Metrics for Security Operational Performance”](https://www.gartner.com/document/code/432923?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/432923?ref=authbody&refval=3970104)
- [“Best Practices for Successful IT Risk Assessment”](https://www.gartner.com/document/code/439861?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/439861?ref=authbody&refval=3970104)

Triage High-Exposure Risk Areas, and Practice Basic Security Hygiene

Performing in-depth risk and gap assessments is a time-consuming process, and it doesn’t always lead to good prioritization. When prioritizing what are believed to be the highest-value assets first, organizations may unwittingly leave the door open for an easy compromise with damaging results. Pay specific attention to users, applications, systems and data that are highly exposed – cloud-based email being a prime example – in order to make sure trivially executed attacks are mitigated. Concurrent with high-exposure risk triaging, implement basic security hygiene through a set of control types – such as vulnerability management and malware protection – that provide the baseline defense expected in almost any organization. Security hygiene also involves optimizing existing investments by maximizing the effectiveness of native security controls and enhancing existing add-on security tools.

Good practices that follow from high-exposure risk triage and basic security hygiene include:

- Building a reliable asset management process; knowing what you have to protect and who is responsible for it is a key element for many security controls.

- Removing users' local administrative privileges on endpoints, and protecting their access to the most sensitive business applications, including email, from account compromise.
- Implementing strong authentication for all privileged users, such as database administrators (DBAs) and cloud infrastructure administrators, and logging their activity.
- Optimizing phishing and malware protection options in endpoint protection platforms (EPPs), secure web gateways (SWG), secure email gateways (SEGs) and other technologies that are in use.

Do not blindly accept basic controls just because they were considered effective in the past. For example, although still necessary for compliance purposes, periodic user password rotation has questionable efficacy because passwords are often stolen instead of guessed or cracked. Unless required by compliance mandates, these ineffective controls should be avoided to create room and budget for more effective ones, such as protecting login services from brute-force attacks. In reality, compliance practices should also be revisited, but that is a slow process at best.

Related research:

- ["Building the Foundations for Effective Security Hygiene"](https://www.gartner.com/document/code/368951?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/368951?ref=authbody&refval=3970104>)
- ["Creating Security Standards: Context, Structure and Must-Have Content"](https://www.gartner.com/document/code/363608?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/363608?ref=authbody&refval=3970104>)
- ["How to Build an Effective Malware Protection Architecture"](https://www.gartner.com/document/code/366440?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/366440?ref=authbody&refval=3970104>)

Improve the Effectiveness of Third-Party Assessments and Control Selection

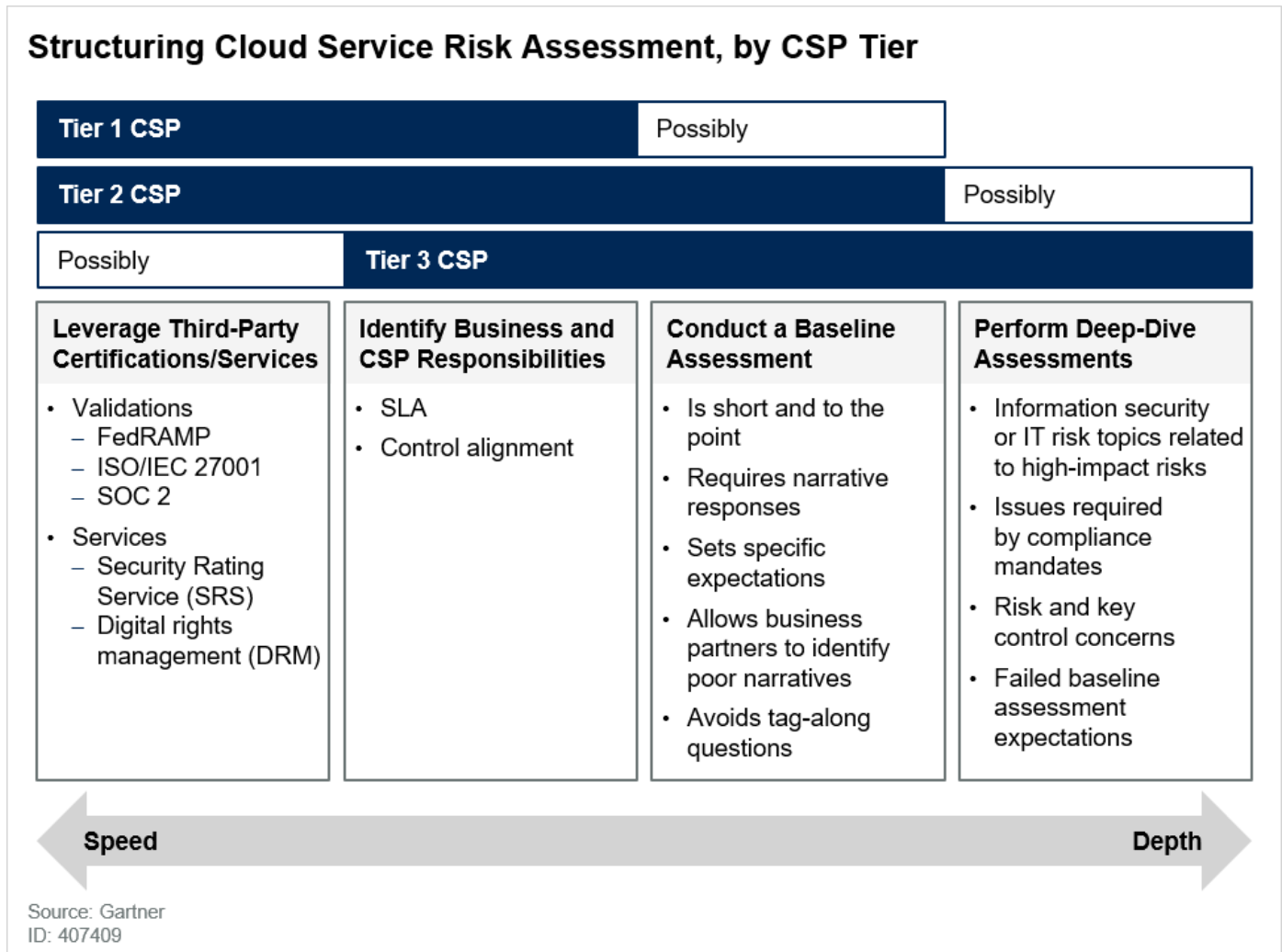
Organizations are adopting more third-party services, and therefore, scaling third-party assessments has become a critical concern. To be able to keep up, especially when continuous assessment is needed, security teams should take several actions as part of their procurement and contracting processes (see Figure 3):

- Adjust the depth and frequency of the assessment based on a provider tiering mechanism.
- Leverage CASB tools or similar functionality to perform shallow cloud provider and application risk assessment triaging at scale.
- Leverage security rating services (aka digital-risk rating services) and external assessments to reduce in-depth assessment effort.
- Clearly define the cloud service provider (CSP)'s responsibilities, compare them against those of the organization, and determine what process and technical control gaps remain.

- Look for adequate controls instead of controls that are equivalent to on-premises controls, and make sure to understand the providers’ capabilities.

This approach ensures that teams do not spend undue amounts of time assessing mature, well-secured Tier 1 providers, but still allows enough due diligence to assess other providers.

Figure 3. Cloud Service Risk Assessment



Use the assessment to identify gaps in provider security capabilities that fall into the organization’s area of responsibility – for example, user reporting or data backup. Determine whether these gaps can be filled with add-on controls. Accepting a provider’s built-in controls and supplementing them with third-party add-ons is often necessary anyway to ensure that security scales in a multiprovider world. This approach helps reduce lock-in and one-offs, though it does not work in every situation. If a provider does not have sufficient internal controls to provide baseline security, no amount of add-on security can compensate.

Related research:

- [“Performing Effective Security Risk Assessments of Public Cloud Deployments”](https://www.gartner.com/document/code/366336?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/366336?ref=authbody&refval=3970104>)

Security Monitoring and Response Will Continue to Depend on Automation and Analytics Delivered Through Internal Skills and Managed Services

Increasing the use of detection and response capabilities is still gaining importance because attackers are finding gaps in, and ways around, properly implemented preventive controls. Security monitoring technologies have seen great evolution and adoption, with security information and event management (SIEM), in particular, still acting as a central component of monitoring and response capabilities. As with many other technologies that gather and analyze data, the driver of evolution in security monitoring is “analytics for security,” including the use of AI techniques, mostly machine learning. The goal is to move beyond static rules and limited correlation – which are time-consuming and difficult to create and manage – to more data sources, machine learning and advanced visualizations.

Security monitoring technologies, however, offer too many options, and a single solution for collecting, storing and analyzing all security data has not yet emerged. SIEM is often a main monitoring hub, especially because these solutions have expanded to include new capabilities such as user and entity behavior analytics (UEBA). This is no surprise, because good monitoring solutions are tuned to the specific events, context and architecture that they monitor. With that specificity and individual effectiveness comes a proliferation of monitoring approaches, even to the point where multiple monitoring solutions essentially cover the same thing but can't replace each other. For example, CASB solutions offer UEBA functionality, but mainly for cloud-based use cases. It therefore remains unlikely that all aspects of monitoring will be managed and viewed from a single solution, let alone a single console.

In addition, organizations continue to struggle with staffing and skills for security monitoring. Especially for traditional solutions like SIEM, security monitoring is time-intensive – not only in actual monitoring of operations, but also in maintenance of content such as correlation rules. Even when security monitoring is heavily automated, staffing is an issue when reviewing events and reports. In advanced security operations, additional staff members are needed to perform security analysis, in functions such as threat hunting and threat intelligence operations. But people with these more specialized skills are especially hard to find, which makes scaling a major challenge. The emergence of managed services, such as managed detection and response (MDR), shows how security service providers are working to help organizations address this issue. In addition, increased automation – both integrated into existing tools, and in the form of security orchestration, automation and response (SOAR) tools – helps scale existing security operations staff.

Planning Considerations

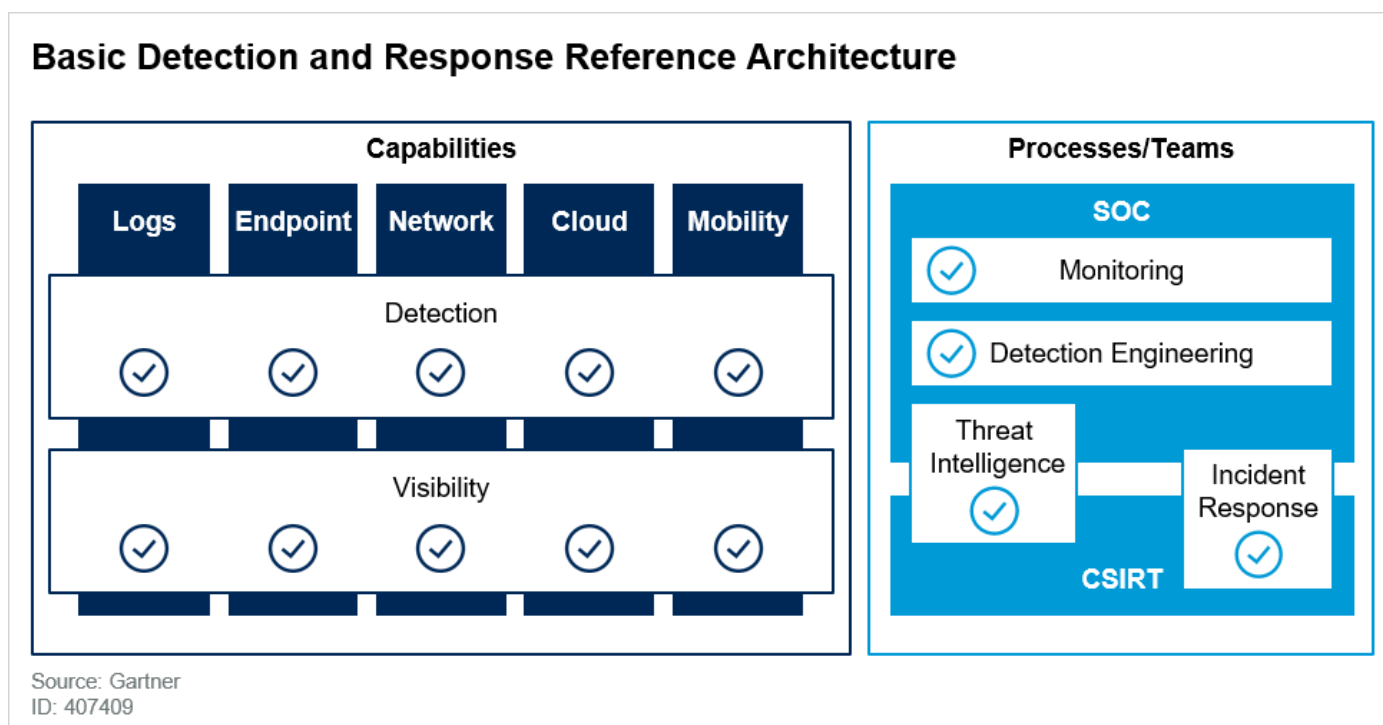
Develop and Enhance Incident Response and Security Monitoring Capabilities

From a process perspective, perform ongoing incident response (IR) planning activities. Preparing for IR is typically one of the more cost-effective security measures an organization can take, because well-planned IR reduces incident impacts and costs. Using the right combination of processes, tools and people, an organization can start to grow its IR maturity from ad hoc practices with few tools to continuous incident response with dedicated teams.

Concurrently, practice the incident response plan, and test recovery and continuity plans that relate to cyberattacks – a single ransomware incident may otherwise leave the organization without IT systems and data.

On the technology side, start with a gap assessment (for example, against the model shown in Figure 4). Ensure collection and reporting of common event types, and coverage of critical and exposed assets. These events include login and access activity for critical systems and applications, antivirus (AV) alerts, large outbound data transfers, and remote-access anomalies. Be sure to evaluate the out-of-the-box threat intelligence data that comes with existing security products for inclusion. Then, implement a use-case-driven approach to manage detection content and rules. Additional technologies such as endpoint detection and response (EDR) and network traffic analysis (NTA) tools will be a necessity for higher-maturity and high-threat environments, and can also be consumed as a managed service. However, security teams should not buy more monitoring than they can manage.

Figure 4. Basic Detection and Response Reference Architecture



Some organizations will be able to use these technologies and practices to build a security operations center (SOC). Others will need to outsource commodity security monitoring and/or detection and response to third parties. Monitoring is time-consuming, and it requires specific security skills, but orchestration and automation – including through the use of SOAR tools – reduce the operational burden. Being able to reduce the amount of time a security team spends on commodity monitoring frees that team up for more customized monitoring activities such as user activity monitoring, or for other tasks such as threat hunting. General monitoring, such as firewall and intrusion detection system (IDS) event triage, can be handled by outsourced providers, as long as a well-documented handoff and escalation procedure exists.

Related research:

- [“How to Plan, Design, Operate and Evolve a SOC”](https://www.gartner.com/document/code/366326?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/366326?ref=authbody&refval=3970104>)
- [“How to Start Your Threat Detection and Response Practice”](https://www.gartner.com/document/code/349155?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/349155?ref=authbody&refval=3970104>)
- [“How to Work With an MSSP to Improve Security”](https://www.gartner.com/document/code/343485?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/343485?ref=authbody&refval=3970104>)
- [“How to Implement a Computer Security Incident Response Program”](https://www.gartner.com/document/code/441567?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/441567?ref=authbody&refval=3970104>)

Increase Focus on User Activity and Access Monitoring in Systems and Applications

Attackers must perform privileged operations or access resources to achieve their goal, such as stealing a database or disabling an application. For example, DDoS must access network or workload resources in order to overload them. Even ransomware, which isn't a data-stealing attack, must access files to encrypt them, and business email compromise requires access to users' mailboxes. In theory, all attacks – including insider attacks, which do not have to cross the perimeter or use malware – can be caught by monitoring for such activity. Though it is neither the earliest attack detection method nor the easiest one to implement and manage, user activity monitoring is extremely valuable, even if only for post hoc forensic analysis. Analytics won't provide a “silver bullet.” However, the profiling and anomaly detection capabilities found in some products will help with alerting and, possibly, blocking.

For infrastructure, logging and monitoring of privileged activity are key, especially when the lines between compute, storage, network, database, application and security administration are often blurred. At the application level, it's important to emphasize monitoring over strict access control because even authorized access will be abused. For example, a healthcare worker may illegitimately access medical records. Because of how most applications are designed, this type of monitoring can usually be instrumented in one or more places, such as in a database, a web proxy or an application. At a minimum, monitoring must enable reporting and post-hoc investigations of events. These capabilities pave the way for adding real-time analytics, alerting and enforcement later on. IAM, CASB, UEBA, and the emerging zero-trust network access (ZTNA) solutions are good starting points for covering a significant spectrum of user access monitoring. Deception technologies can also be used to cover gaps in the coverage of more traditional tools.

Related research:

- [“How to Secure Cloud Applications Using Cloud Access Security Brokers”](https://www.gartner.com/document/code/393383?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/393383?ref=authbody&refval=3970104>)
- [“A Comparison of Remote Network Access Products for Enterprise Endpoints”](https://www.gartner.com/document/code/380285?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/380285?ref=authbody&refval=3970104>)

Investigate Deception and Machine Learning to Improve the Accuracy of Monitoring

Gartner clients have been reporting good results from deploying deception technologies, primarily to improve threat detection. These technologies work by introducing monitored “trap” items that are designed to lure an attacker into accessing them. A “deception for better detection” model provides a way for the organization to benefit from these early tools, despite their immaturity. Such tools are not targeted solely at sophisticated clients; some deception vendors focus on mainstream clients suffering from alert fatigue. Other good reasons to invest in deception technologies include working around limitations from privacy regulations, monitoring coverage for the environment or having very specific data targets, such as high-technology intellectual property.

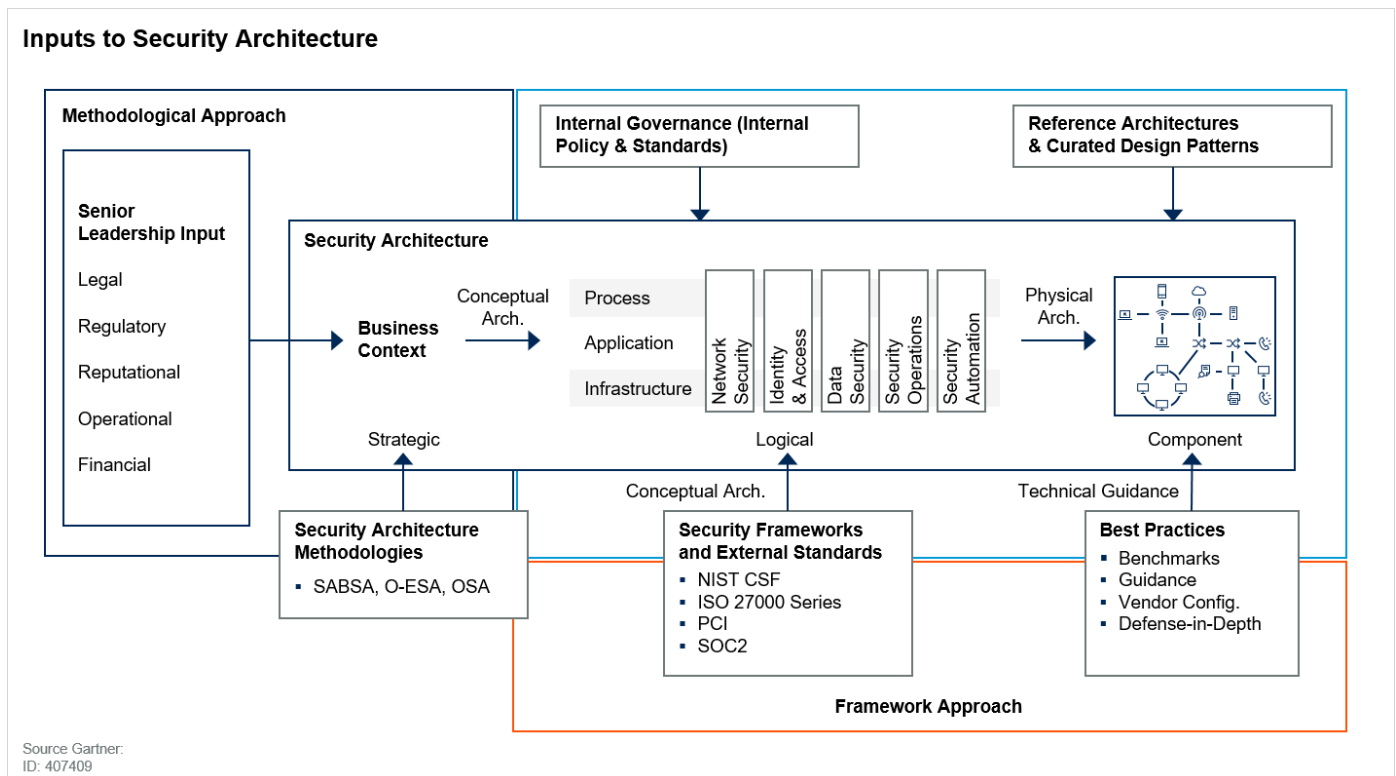
Related research:

- [“Assessing the Impact of Machine Learning on Security”](https://www.gartner.com/document/code/377363?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/377363?ref=authbody&refval=3970104>)
- [“Applying Deception Technologies and Techniques to Improve Threat Detection and Response”](https://www.gartner.com/document/code/373461?ref=authbody&refval=3970104) (<https://www.gartner.com/document/code/373461?ref=authbody&refval=3970104>)
- [“Solution Comparison for Six Threat Deception Platforms”](https://www.gartner.com/document/code/373459?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/373459?ref=authbody&refval=3970104>)

Security Solution Architecture Will Be Increasingly Driven by Integrated Cybersecurity Platform Approaches

Many security teams find it difficult to perform gap assessments and build security roadmaps. One of their greatest challenges is that it is becoming increasingly difficult to clearly understand what security features and applicability the products have. Some are niche “widgets” that offer singular capabilities or coverage, and others are broader “platforms.” In both cases, the difficulty is figuring out where and how they can be fit together in order to provide the right capabilities in the right places – like playing the Tetris puzzle game. A key exercise is to determine how the platform and best-of-breed capabilities fit together as part of the security architecture process (see Figure 5). The “shape” of product features inevitably leads to gaps and overlaps, and these need to be identified early so they will be properly addressed. Particularly when trying to plan for the near-term future, it’s not just the current shape that matters, but also predicting what the future vendor product roadmaps will look like. In the current business climate, new startups, organic product expansion and acquisitions happen at a fast pace.

Figure 5. Inputs to Security Architecture



Security architecture is implicit in various control frameworks and “top” lists, such as the ISO/IEC 27000 series and Center for Internet Security (CIS) Controls, but they do not provide security teams with enough structure for detailed roadmap planning. This is in part because they do not always reflect the evolution in business, IT or security controls. Using security architecture methodologies, such as SABSA, helps organizations capture business security objectives and use them as a foundation to build requirements and create system-engineered architectures. These map to some enterprise security architecture frameworks, but not all organizations use them or have an enterprise architecture function. Organizations that already use one of the architecture or control frameworks may want or need to supplement them with additional security architecture models and processes in order to close gaps and align with business needs.

A related issue in deploying security controls is supporting their proper management; effort required for configuration, ongoing tuning and working with the outputs from controls varies greatly. Similarly, organizations can choose the levels of effort they want to put into executing security processes, such as risk assessment or incident response (IR). The availability of in-house and outsourced security talent is a limiting factor.

Planning Considerations

Create a Security Capability Model as a Security Architecture Foundation

The starting point of any architecture is business requirements, which – through risk assessment – drive the requirement for security capabilities. Use security capabilities and layers as a technology architecture starting point. Adopt security control categorizations from existing models, such as Identify, Protect, Detect, Respond and Recover from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Do the same for

an asset classification or layering model – such as Physical, Network, Repository, Application and Data – and make sure to also account for asset diversity. This includes user endpoints versus server endpoints, IoT devices, and cloud versus data center. In 2020, Gartner will publish security architecture documents focusing on different technology areas, such as cloud computing, to help define these dimensions.

Related research:

- [“Improve Your Security With Security Architecture”](https://www.gartner.com/document/code/373511?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/373511?ref=authbody&refval=3970104>)
- [“A Guidance Framework for Establishing Your Approach to Security Architecture”](https://www.gartner.com/document/code/385515?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/385515?ref=authbody&refval=3970104>)
- [“Solution Path for Implementing Threat Detection and Incident Response”](https://www.gartner.com/document/code/366328?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/366328?ref=authbody&refval=3970104>)
- [“Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services”](https://www.gartner.com/document/code/361411?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/361411?ref=authbody&refval=3970104>)

Use Threat and Attack Models to Refine Gap Assessment and Control Selection

Use threats and attacks as another dimension in security architecture. Build with a list of possible attacks, prioritize ones that are paths of least resistance, and also identify which attack paths arrive at the same outcome. This ensures that security architecture and control design match the threats and attacks that various types of assets may be exposed to. In addition to having too little protection for an asset, a lack of threat focus easily leads to implementing protection for attacks that can't be realized, or for which an easier alternative attack path exists. Unfortunately, a unified threat and attack model does not exist.

Organizations should look to adopt existing attack models, such as:

- Gartner Attack Chain
- MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)
- The Lockheed Martin Cyber Kill Chain
- More specific models defined in other Gartner coverage

Similarly, take advantage of existing threat and vulnerability models, such as the Open Web Application Security Project (OWASP), or those built into threat modeling and risk management tools. In 2020, Gartner will publish additional documents to refine threat and attack models.

Related research:

- [“How to Develop and Maintain Security Monitoring Use Cases”](https://www.gartner.com/document/code/338758?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/338758?ref=authbody&refval=3970104>)

- [“How to Build an Effective Malware Protection Architecture”](https://www.gartner.com/document/code/366440?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/366440?ref=authbody&refval=3970104>)

Plan for Deciding Between Integrated Cybersecurity Solutions and Best-of-Breed Solutions

Large security and cloud vendors are building out integrated cybersecurity solutions that aim to implement single-console, integrated machine learning, orchestration and automation on a single platform that supports third-party integration. These platforms are built over time, expanding with new types of capabilities and integrations as client needs arise. For example, some vendors started with stand-alone secure web gateway and enterprise data loss prevention (DLP), then acquired CASB, followed by acquisition of ZTNA and RBI, and then integrated them into a single platform. Other vendors started as a content delivery network (CDN), and then added DDoS, web application firewall (WAF) and bot mitigation features, while others started with endpoint protection and added email and gateway offerings aligned with large threat intelligence. Organizations should look at their incumbent vendors and create a mapping of platform capabilities to their own security architecture and roadmap.

However, vendors do not provide a complete security portfolio – a “true” single integrated cybersecurity platform will likely not emerge any time soon. A platform firmly focused on end users and collaboration likely does not have a database monitoring agent; conversely, an application security platform will likely not have a CASB. Large cloud providers provide overlapping capabilities with the security platform vendors and products, which complicates selection. And even if an integrated platform provides a security function, it may not be capable enough to fulfill a specific use case. As such, organizations will continue to have to assess platform versus best-of-breed approaches, as well as a multiplatform approach.

Related research:

- [“Understanding and Implementing Security in Office 365: Exchange Online, SharePoint Online, OneDrive for Business and Teams”](https://www.gartner.com/document/code/349107?ref=authbody&refval=3970104) (<https://www.gartner.com/document/code/349107?ref=authbody&refval=3970104>)

Containers, DevSecOps, Hybrid Cloud and Multicloud Will Transform Infrastructure Security Architecture and Management

Weaknesses in the security of privileged operations and entitlements for IT infrastructure have resulted in damaging security incidents. For example, misconfigurations of resource permissions, roles and credentials for applications have been used to compromise and subsequently access sensitive customer information in data stores. Unsecured cloud administrator credentials have been used to wipe an entire organization’s systems and data. Understanding existing security posture and having visibility of all assets in the cloud are critical to being able to protect against these attacks.

In addition, basic security hygiene issues, such as missing patches and misconfiguration, are still playing a major role in attacks. Moving to virtualization, container and cloud technologies

helps streamline and automate infrastructure security practices. However, it adds complexity and also introduces new opportunities for mistakes because security and IT teams don't always immediately understand new exposures and new ways of implementing controls.

Conceptually, traditional implementations of network zoning and network perimeter security are still valuable as "early deny" approaches. However, businesses move to these new environments to provide easy flexibility and scalability – which conventional network security tools will limit. Security should focus on addressing lateral attacker movement in the infrastructure and cover attacks that happen at the application layer. Moreover, the notion of what is and what isn't infrastructure security is also changing, due to the following factors:

- **DevOps:** More organizations are adopting DevOps practices, including "infrastructure as code" (IaC) or "infrastructure automation" approaches, which cause the notion of "infrastructure" to be more fluid than before.
- **New technologies:** Software and cloud providers are offering new products that create additional types of storage, networks and compute. One example is serverless computing technologies, which abstract away infrastructure control and don't have the same level of maturity in security features.

Extending existing on-premises security tools is a possibility, but often a mistake. These tools were not designed for cloud implementations, and may not work correctly or focus on the right attack vectors or attack types. Many of the more proven virtualized infrastructure technologies, including those from leading cloud IaaS providers, now have security capabilities that are considered equivalent to, or better than, the security capabilities of the average organization. For a growing number of use cases, these cloud-based security controls are strong enough to replace physically separated and on-premises data center systems, respectively. Some technologies – such as containers, software-defined networking (SDN) and platform as a service (PaaS) – are still less defined in terms of security capabilities and strength. Organizations often use multiple platform and container solutions, which compounds the problem. However, their adoption is on the rise, and security controls such as CWPP and container security products have emerged. Their automation and orchestration have a strong potential to increase security by enabling standardization and deeper layered defenses, and by allowing workloads to be accessed more frequently.

Management – in particular, as it relates to monitoring and enforcement of privileged operations – remains a weak spot for many infrastructure technologies. Vendors in the IAM and security spaces, such as privileged access management (PAM) vendors and CASBs, have been working to improve this situation. They are developing capabilities that enable better monitoring and analytics, as well as better policy enforcement of privileged user activity, both in the data center and in the cloud. In conjunction, infrastructure and application technologies are increasingly offering security and nonsecurity management and monitoring APIs, thus allowing more effective and seamless integration with third-party technologies. Cloud security posture management tools integrate with infrastructure cloud providers to provide risk identification,

visibility into deployment configuration as well as policy enforcement to help manage complex deployments – even across multiple clouds.

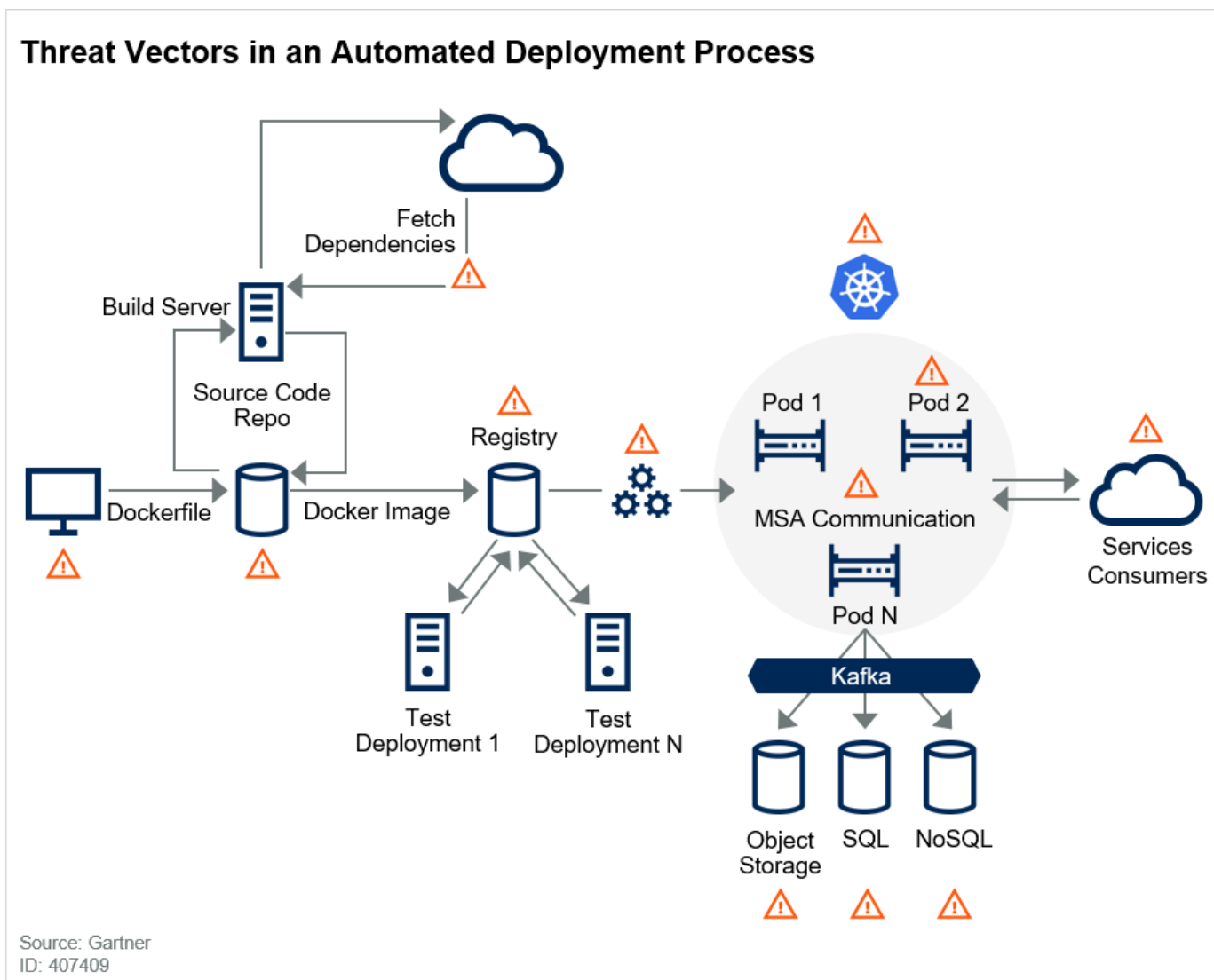
DevOps and DevSecOps blur the boundaries between infrastructure and applications, and data security is partially implemented at the infrastructure layer. Security teams will find that trends and considerations relating to infrastructure security go hand in hand with those relating to application and data security. Infrastructure as code, in particular, creates new risk and opportunities. Runtime application security controls that become part of the workload or network infrastructure, as well as some forms of data-at-rest encryption, are good examples of this. These items are partially or fully discussed in the next section.

Planning Considerations

Embrace DevSecOps to Enable Standardization and Automation of Security Across Infrastructure

Align security and DevOps practices for a holistic DevSecOps approach. Security should become an integral part of processes and automation, and in turn, it should take full advantage of the strengths of these processes and automation. Aside from supporting an inherently more agile environment, this approach ensures that security is consistent and repeatable. It also ensures a focus on the building blocks – such as workflow definitions, scripts, recipes and images – rather than on every single operation and instantiation. Understanding how to harden, as well as how to support, security in a diverse ecosystem of virtualization, cloud, container, serverless and database environments is key. As an example, Figure 6 shows an automated deployment process for container-based applications, with threats indicated by the orange triangles.

Figure 6. Threat Vectors in an Automated Deployment Process



Not all of the technology stacks will come with sufficient built-in security. In these cases, organizations will need to instrument them with security via third-party components, such as container security products, CWPPs or runtime application self-protection (RASP) technologies. In a DevOps environment, organizations will also need to shift their vulnerability assessment practices to not just scan workloads after they go live – scanning of container images during build or prior to instantiation, for example, is a good practice. And they need to tightly integrate security testing into the development pipeline. Security APIs make such instrumentation easier, and organizations should ask their vendors to offer these APIs if they are not yet available.

Related research:

- “Container Security – From Image Analysis to Network Segmentation, Options Are Maturing” (<https://www.gartner.com/document/code/366118?ref=authbody&refval=3970104>)
- “Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services” (<https://www.gartner.com/document/code/361411?ref=authbody&refval=3970104>)
- “Structuring Application Security Practices and Tools to Support DevOps and DevSecOps” (<https://www.gartner.com/document/code/337322?ref=authbody&refval=3970104>)

Modernize Network, Workload and Data Security, and Embrace Native Infrastructure Security Capabilities

Plan to secure a diverse set of workloads in a “network of secure systems” fashion. In this approach, various network security boundaries exist – some for policy enforcement and some just for visibility. These boundaries grow to accommodate load and/or shrink to the host level or smaller via microsegmentation concepts. SDN approaches will be needed to enable agility in private cloud environments. External network perimeters need to become more dynamic, and the concept of a traditional demilitarized zone (DMZ) slowly disappears. Especially as more applications become API-based and cloud-delivered, basic filtering at the network boundary should be combined with cloud-based security services such as DDoS protection, bot mitigation, WAFs and iPaaS.

Embrace intrinsic security measures rather than relying on legacy technology designed for platforms without these features. In IaaS, look to native features such as security groups in Amazon Web Services (AWS), network security groups in Microsoft Azure and firewall rules in Google Cloud Platform. Security groups provide for basic network separation and filtering scenarios, and in some cases are getting more advanced with the addition of network tags to control and limit based on applications or application groups. Microsegmentation technologies should be evaluated when increased visibility or enhanced security is required. This is especially true when developing a cohesive view across multiple IaaS providers or when visibility at the container level is required. The ability to use or integrate monitoring/visibility mechanisms is key. Start with security groups and augment with microsegmentation as compliance requirements or the outcomes of a risk assessment dictate.

For workload and data security, combine built-in or add-on encryption for storage or databases as a baseline compliance control, with CWPP, container security or even RASP as a workload security add-on. CWPP solutions provide multifunctional control – including workload-specific protection and network security – for IaaS environments. In serverless and other xPaaS environments, first determine built-in capabilities for securing data and the integrity of the workload. Certain risks, such as a host compromise, will be the provider’s responsibility to address. But security will still be scant in these environments. Look to manage and monitor security at the code level, or use instrumentable components.

Related research:

- [“Container Security – From Image Analysis to Network Segmentation, Options Are Maturing”](https://www.gartner.com/document/code/366118?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/366118?ref=authbody&refval=3970104)
- [“Improve Your Cloud Security With Cloud Workload Protection Platforms”](https://www.gartner.com/document/code/383229?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/383229?ref=authbody&refval=3970104)
- [“Using Native IaaS Workload Security Capabilities in Amazon Web Services, Microsoft Azure and Google Cloud Platform”](https://www.gartner.com/document/code/373510?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/373510?ref=authbody&refval=3970104)

- [“Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services”](https://www.gartner.com/document/code/361411?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/361411?ref=authbody&refval=3970104)
- [“Comparing Security Controls and Paradigms in AWS, Google Cloud Platform and Microsoft Azure”](https://www.gartner.com/document/code/343562?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/343562?ref=authbody&refval=3970104)
- [“Implementing Cloud Security Monitoring and Compliance Using Amazon Web Services”](https://www.gartner.com/document/code/351316?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/351316?ref=authbody&refval=3970104)
- [“Solution Comparison for Microsegmentation Products”](https://www.gartner.com/document/code/377627?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/377627?ref=authbody&refval=3970104)
- [“Decision Point for Postmodern Security Zones”](https://www.gartner.com/document/code/337220?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/337220?ref=authbody&refval=3970104)

Emphasize Visibility, Monitoring and Management for Privileged Accounts and Operations

Consider the effect that the choice of system and application accounts has on the ability to isolate workloads and their data. In the extreme, an organization should use entirely separate administrative domains to run individual applications by having separate master accounts on a cloud service. But more often, the number of accounts, their specific capabilities and their permissions should be chosen to complement workload- and network-based separation. They should be used to isolate applications and data that belong to different risk categories or compliance domains, and in particular to isolate backup and disaster recovery resources.

Compensate for risk from the consolidation of administrative roles, especially in cloud and virtualized environments. Privileged operations security is important for protecting against not only insider threats, but also external threats that use compromised insider access. Use strong authentication and authorization, including advanced management of credentials and secrets, for privileged accounts and operations. Adaptive access control, especially if it includes user endpoint and behavioral profiling, provides additional protection from misuse and credential theft.

Logging and monitoring of privileged activity are also key because the lines between compute, storage, network, database, application and security administration are often blurred. At a minimum, monitoring must enable reporting and post hoc investigations of events. These capabilities pave the way for adding real-time analytics, alerting and enforcement later on. Privileged user management, identity analytics, CASB and UEBA tools all play a role in providing continuous monitoring and analytics of user activity. Many other products, such as container security, CWPP and CSPM, are a potential source of events for other tools such as cloud-based SIEM, but many also implement their own security analytics.

Related research:

- [“Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services”](https://www.gartner.com/document/code/361411?ref=authbody&refval=3970104) (https://www.gartner.com/document/code/361411?ref=authbody&refval=3970104)

- “Comparing Security Controls and Paradigms in AWS, Google Cloud Platform and Microsoft Azure” (<https://www.gartner.com/document/code/343562?ref=authbody&refval=3970104>)
- “How to Secure Cloud Applications Using Cloud Access Security Brokers” (<https://www.gartner.com/document/code/393383?ref=authbody&refval=3970104>)
- “Solution Comparison for Cloud Access Security Brokers” (<https://www.gartner.com/document/code/377717?ref=authbody&refval=3970104>)
- “Implementing Cloud Security Monitoring and Compliance Using Amazon Web Services” (<https://www.gartner.com/document/code/351316?ref=authbody&refval=3970104>)
- “Best Practices for Securing Continuous Delivery Systems and Artifacts” (<https://www.gartner.com/document/code/386385?ref=authbody&refval=3970104>)

Ecosystems Will Cement the Need for Data-Centric Security Architecture and Application Security

Data is proliferating, both within and outside of the organizations that collect and initially take responsibility for protecting it. At the same time, the regulatory obligations placed on organizations to govern that data – for example, privacy regulations to protect the individual – are multiplying. Privacy regulations especially are rarely technically prescriptive, and sometimes appear contradictory or at least highly nuanced. However, Gartner does see consistencies that support a more simplified strategy.

Securing and enabling privacy compliance within data warehouses and big data and advanced analytics pipelines are of increasing concern among many clients. Data loss, exposure and integrity are the key threats in these environments, and can be seen to conflict directly with the needs of the business.

Applications have long been a major attack vector. “Traditional” security controls – such as firewalls, IDSs and intrusion prevention systems (IPSs) – are unable to comprehensively address application security problems. Coding errors that cause vulnerabilities, such as SQL injection, are still a common source of incidents, especially when exposed as well-known vulnerabilities in off-the-shelf software or open-source components (including through nested component dependencies). Design weaknesses – such as unlimited authentication attempts, lack of account takeover detection and lack of protection against automated attacks – are also increasingly used to abuse the business logic in applications and APIs. And the ever-widening adoption of mobile, IoT, PaaS, containers and microservices brings new challenges in terms of where and how application security can and should be implemented.

Externalization of security capabilities and runtime security controls now allow a greater focus on adaptive security models, both in terms of threat protection and access control. Code scanning, static data masking (SDM) and entitlements still play a key role, but making security decisions in a more late-binding manner is equally important. For threat protection, application delivery controllers (ADCs), WAFs, CDNs, API gateways, bot mitigation solutions and RASP

provide security for applications. On the access control side, identity and security technologies such as IAM as a service (IDaaS), CASB, UEBA, dynamic data masking (DDM) and SDP have evolved to make adaptive access control and monitoring possible.

DevOps and DevSecOps blur the boundaries between infrastructure and applications. Security teams will find that trends and considerations relating to infrastructure security go hand in hand with those relating to application and data security. Managing the security of the DevOps toolchain, workloads and secrets are clear examples. These items are discussed in the previous section.

Planning Considerations

Create Discovery, Visibility and Control for Access to Applications and Data

Discovery and visibility are key because it's increasingly important to know which data is where, and to get deep insight into how users and machines access various applications and data sources. Organizations are searching to understand not only how authorized applications and data are being used, but also which unsanctioned applications (aka "shadow IT") and data locations are being used. Several technologies help create such visibility, and to a high degree of detail. These include database audit and protection (DAP), data classification tools, file analysis tools, DLP, and CASBs, as well as nonsecurity tools such as data management and enterprise content management. This visibility then allows organizations to match data residency and usage to their defined policies and choose a path forward: allow, block or mitigate the risk of movement and usage through additional controls. However, organizations should be careful when implementing such controls without a formal or semiformal data security program, because they risk choosing a technology that negatively impacts the business or fails to meet security or user expectations.

Emphasize user activity, transaction and data access control and monitoring in application contexts. Adaptive authentication and authorization, as well as strong monitoring and auditing capabilities, are key in securing any sensitive and/or critical application. IAM technologies, including identity analytics, and security technologies such as CASBs, UEBA and DDM are able to effectively fill gaps in cloud applications, enable externalized capabilities for in-house applications and protect access to data stores. At a minimum, ensure that logging and monitoring covers privileged users and access to critical or sensitive data. Find the appropriate links between the various security technologies to maximize their benefits and to reduce duplicated management and operational effort.

Investigate the inherent capabilities of the cloud environment. SaaS providers have recognized the need to provide data-centric security controls and monitoring as well as authentication and CASB compatibility. API availability is becoming commonplace, and native SaaS security is improving on a continuous basis. It is not yet possible to use CSP native controls to the exclusion of all others – at least a CASB should be considered a requirement. But with the caveat that operational and regulatory considerations should be taken into account, some organizations will find that they get cost-efficient "good enough" security solutions within the cloud.

Overlay your core security architecture with a data-centric view (see Figure 7). This will provide an invaluable approach, especially when securing unstructured data. Focusing exclusively on component security can blindside the security practitioner to other threats arising from the use and movement of data. Use data classification and discovery tools to find the sensitive data in the organization and then work with the business users to track how that information moves. Build a data flow map to identify key risk areas and focus data-centric controls such as classification, enterprise digital rights management (EDRM) and DLP on those points. Applying these solutions to everything is expensive, slow to show benefits and can have serious business impact – therefore, a targeted approach is more effective.

Figure 7. Data-Centric Security Architecture Control Families

The Four Data-Centric Control Families With Examples of Commonly Implemented Controls

DCSA Control Families	Control Examples
Insight	<ul style="list-style-type: none"> • Data mapping • Data discovery • Data classification
Confidentiality	<ul style="list-style-type: none"> • Access control • Data masking and encryption • Enterprise digital rights management (EDRM) • Data loss prevention (DLP)
Monitoring and Response	<ul style="list-style-type: none"> • Security information and event management • Database activity monitoring
Third-Party Governance	<ul style="list-style-type: none"> • Contractual controls

Source: Gartner
ID: 407409

DLP remains the go-to data security control of choice for many organizations, but continues to have a multitude of problems. DLP functionality is found in many other tools than just the traditional enterprise-DLP system. Use the data-centric architecture approach to reduce the burden on DLP by building hygiene “upstream” in the data life cycle. Use a risk-based approach to decide where DLP is most important and identify where DLP is available within your existing controls. Decide whether “best in class” is necessary, or if “good enough” will suffice, given that there is often a significant operational impact in using the best tool for each environment. Evaluate the use of SaaS- and IaaS-native DLP when your prime risk is in that environment, but remember that these solutions will only operate within that scope, and are often less powerful than a more expensive system.

Related research:

- [“How to Successfully Design and Implement a Data-Centric Security Architecture”](https://www.gartner.com/document/code/390767?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/390767?ref=authbody&refval=3970104>)

- “Improving Data Security Governance Using Classification Tools”
(<https://www.gartner.com/document/code/337209?ref=authbody&refval=3970104>)
- “Securing the Big Data and Advanced Analytics Pipeline”
(<https://www.gartner.com/document/code/352648?ref=authbody&refval=3970104>)
- “How to Secure Cloud Applications Using Cloud Access Security Brokers”
(<https://www.gartner.com/document/code/393383?ref=authbody&refval=3970104>)

Design a Pragmatic and Flexible Approach for Data Stores and Data Analytics

Before picking specific controls, create the most complete picture possible of what data exists where and how it moves within the organization – discovery and classification are necessary to ensure you know what to protect. Even basic data flow modeling provides extremely useful insight about the highest risks and required controls. Use a data-centric security architecture approach to focus on information security, rather than system security.

Use encryption wisely because of its operational risk and management overhead. Match encryption to threats and attacks, as well as to other controls such as access control and monitoring. Also, consider the impact of encryption on integration and business continuity at higher layers. In general, broad encryption should be performed at the lowest possible layer. Although this approach only creates blanket protection for attacks on storage and systems, it still satisfies most compliance and contractual requirements relating to data-at-rest encryption.

Determine whether, and how much, data must be protected at the field level for use cases such as test data, analytics, data sharing and even some highly sensitive production data fields. Use data masking, field-level encryption or tokenization. Use field-level protection only to address specific threats, attacks or compliance mandates, and treat this type of protection as an extension of authorization mechanisms. Do not mask or encrypt everything at the field level – choose specific fields and files to protect. Pick when and where this protection is applied – at ingest time, in the data store, at data access or after the data is retrieved. Then, choose the right type of protection algorithm for each field. Ensure that you can meet security requirements while also maintaining sufficient utility of the data for specific applications, business processes and users. If needed, look to emerging privacy-enhancing techniques – such as differential privacy or secure multiparty computation – or trusted computing constructs, such as Intel Software Guard Extensions (SGX).

Advanced analytics – including AI techniques such as ML with deep learning – take center stage as enterprise functions become increasingly data-driven. Technical professionals frequently have difficulty designing security and privacy into a big data and advanced analytics platform, where data silos, data flows and entitlements are largely opaque. In addition to the currently dominating walled gardens or enclaves for advanced analytics, where data scientists are largely unrestricted, clients should evaluate more granular data-centric controls that address privacy, entitlement or visibility of data across many silos.

Blockchain continues to be on the radar of many clients. Gartner has observed the early use cases, which include registries of ownership, transaction settling and identity management. Currently, blockchain initiatives are consulting-heavy, and Gartner anticipates that more startups will come up with new products and paradigms based on blockchain technology. The market is, however, not there yet. After a decade of academic research, secure multiparty computation can finally be operationalized to further protect the computations required for encryption/decryption and encryption key management. Currently, several offerings are available that provide, for example, encryption as a service or encryption key management as a service with very high levels of privacy.

Related research:


- [“Securing the Big Data and Advanced Analytics Pipeline”](https://www.gartner.com/document/code/352648?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/352648?ref=authbody&refval=3970104>)
- [“Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization”](https://www.gartner.com/document/code/343738?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/343738?ref=authbody&refval=3970104>)
- [“Assessing the Impact of Machine Learning on Security”](https://www.gartner.com/document/code/377363?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/377363?ref=authbody&refval=3970104>)

Create or Enhance Application and API Security Practices and Architecture




Create integration and automation for security requirements and security testing within existing software development and acquisition processes, as well as in data management practices. Take advantage of, or push for adoption of, practices such as DevOps and continuous integration and continuous delivery (CI/CD). These practices are catalysts for smoother integration of security activities into the software life cycle, although these are practices that need to be secured as well. Also ensure that development environments and artifacts are secured, both from pure code development and application infrastructure perspectives. Following security best practices is key in securing these newer environments (see Figure 8).

Figure 8. Best Practices for Securing Continuous Delivery Systems and Artifacts

Best-Practice Framework


Best Practices for Securing Continuous Delivery Systems and Artifacts

After deploying developer tooling, version control, binary repositories and registries, and secrets management, DevOps teams should:

- 
Ensure Application Source Code Integrity
 - Enable VCS security features
 - Secure registries, managers and repositories
 - Audit source code for embedded secrets
- 
Secure Operating Environments
 - Harden IaC baselines
 - Use vetted images, and manage them centrally
 - Audit images and IaC for embedded secrets
- 
Secure the Application Build Pipeline
 - Enable CI/CD tooling security features
 - Limit pipeline push/pull to trusted sources
 - Verify asset compliance during instantiation
- 
Beware of Risks and Pitfalls
 - Neglecting to scan for embedded secrets
 - Omitting a strategy for cloud platforms
 - Overly restricting development environments

Source: Gartner
 VCS = version control system
 ID: 407409

Establish security architecture for client and server components. Having established design concepts, patterns and even actual solution sets allows security to accelerate projects by significantly reducing ad hoc risk analysis and mitigation. It reduces risk by reusing a small set of well-secured patterns and vetted components, and it makes developers' lives easier by reducing their need to write "security code." Good architecture practices also allow more consistent and stronger security by using security solutions outside of their silos. For example, organizations may be able to use CASBs, which are SaaS-focused, to front-end homegrown cloud applications. They can also use data-centric audit and protection (DCAP) wherever products aim to cross multiple data silos.

Take advantage of externalized security capabilities, such as those in WAFs, API gateways, CDNs, mobile app shielding, RASP and bot mitigation technologies. In addition to mitigating vulnerabilities, these externalized capabilities are ideally suited for certain security functions that are difficult to implement and maintain, that are less effective, or that lack flexibility when they are part of the application code. Examples of such functions include DDoS prevention, bot defense, malware-checking and device/user authentication.

Related research:

- [“Best Practices for Securing Continuous Delivery Systems and Artifacts”](https://www.gartner.com/document/code/386385?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/386385?ref=authbody&refval=3970104>)
- [“A Guidance Framework for Establishing and Maturing an Application Security Program”](https://www.gartner.com/document/code/366334?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/366334?ref=authbody&refval=3970104>)
- [“How to Integrate Application Security Testing Into a Software Development Life Cycle”](https://www.gartner.com/document/code/370366?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/370366?ref=authbody&refval=3970104>)
- [“Protecting Web Applications and APIs From Exploits and Abuse”](https://www.gartner.com/document/code/383318?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/383318?ref=authbody&refval=3970104>)
- [“Solution Comparison for Cloud-Based Web Application Firewall Services”](https://www.gartner.com/document/code/349064?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/349064?ref=authbody&refval=3970104>)

Mobile Devices, Things, Intelligent Agents and SaaS Will Drive Expansion of Native Security Capabilities and Add-Ons

User endpoints – PCs and mobile devices – remain a big target for malware, and are often the first foothold for further attacks. These attacks have moved on from only stealing sensitive information to much more commercially attractive attacks, such as ransomware and business email compromise. Popular modern mobile operating systems generally provide good isolation between different apps and their data. However, they can be compromised with low-level exploits delivered through mobile phishing, network or application attacks. Threats are not limited to phishing or malicious applications, but the user can accidentally give unwanted apps privileges that are too powerful. Behavioral analysis and EDR technologies on mobile and PC endpoints are required to block and/or detect more advanced malware and fileless attacks.

Security of PC and mobile endpoints is closely linked to cloud and collaboration technologies. Providing secure mobile access to collaborative cloud services, such as Microsoft Office 365 and Google’s G Suite, is a key consideration for many organizations. CASBs, themselves often cloud-based, play a role in providing insight into, and exerting control over, cloud usage and user activity. Security teams should stay informed about potential convergence and overlap in these solutions, especially as they relate to managing access. CASB and SDP clearly overlap functionally, but currently exist side-by-side to cover different assets – CASB covers SaaS applications, and SDP covers remote access to self-hosted applications in the cloud or on-premises.

In addition to growth in end-user endpoints, organizations also have to deal with a growing number of other devices that need access to their networks and agents that need to interface with applications and data. IoT devices are often not designed with enterprise security and manageability in mind – security is often weak by default, and configuration and patching are nontrivial. In addition, some of them are multihomed, combining a Wi-Fi or hardwired network connection with cellular communications, thus creating possible entry points onto the

enterprise network. Various intelligent agents, such as virtual personal assistants (VPAs) and RPA, take over human tasks, but their security is not yet well understood.

Planning Considerations

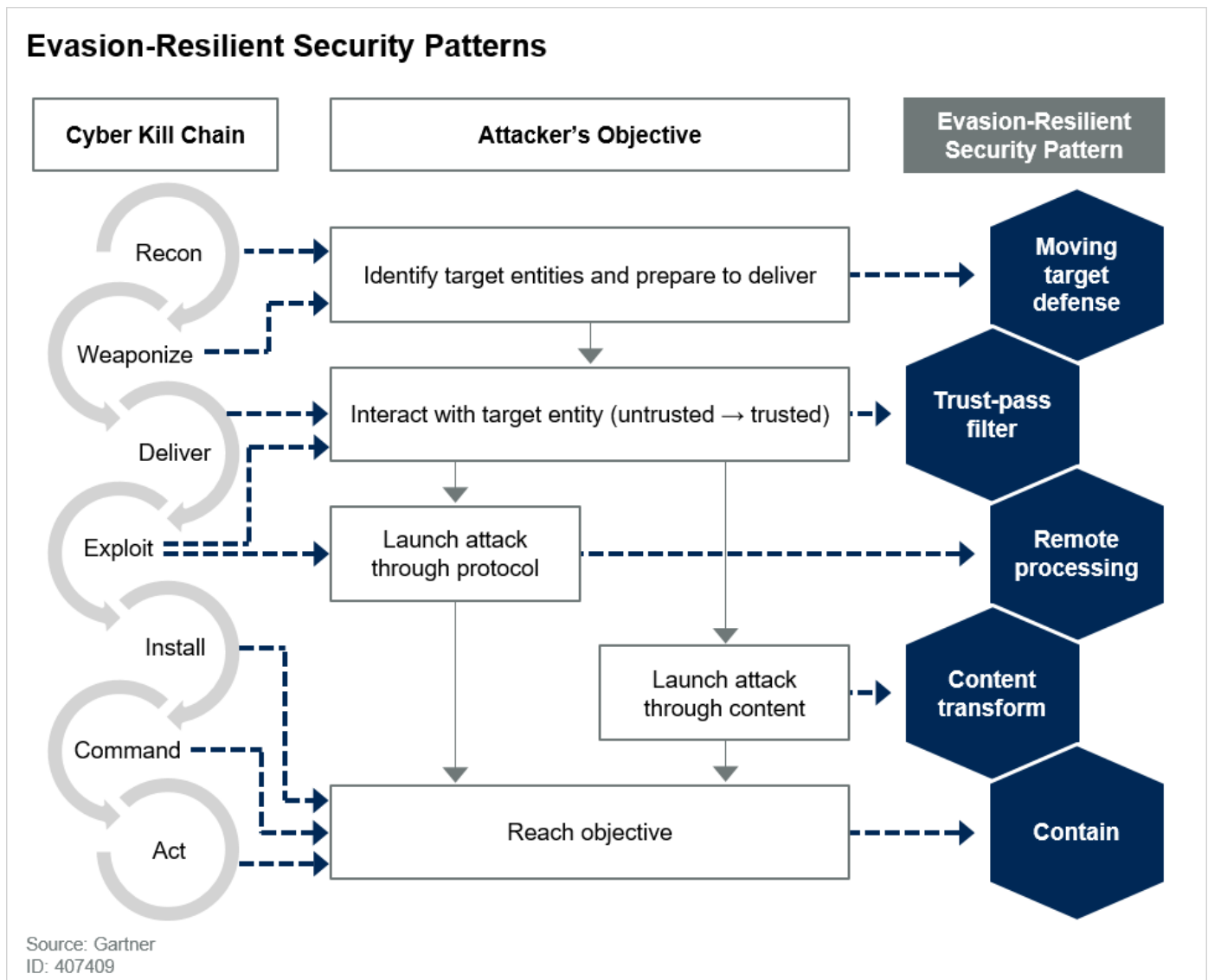
Implement Threat and Data Protection to Cover All Types of End-User Endpoints

Security architects must review their malware protection architectures across networks, client endpoints and server endpoints:

- Assess standard hygiene practices – including vulnerability and configuration management and data backup – across operating systems and applications.
- Audit configurations of security solutions to ensure that they are optimized and integrated for detection across networks and endpoints.
- Utilize one or more endpoint and mobile solutions to provide not only prevention capabilities, but also to provide detection and response capabilities that help reduce the time to recover from a successful malware attack. EDR and mobile threat defense (MTD) are examples of this.
- For high-risk or high-threat environments, consider technologies that sacrifice some user experience (UX) or solution complexity for increased security. Examples include remote browsing and content disarm and reconstruction (CDR) technologies. Look first for integrations with your existing solutions, such as SEG and SWG, before expanding to broader use cases.

Various technologies have matured and are used at large scale. These include exploit mitigation, malware detection and prevention, containment, behavior analysis, and EDR. Some technologies, such as CDR browsing, are emerging as preventative approaches (see Figure 9). Base your solution selection on proven detection quality, breadth of technologies included, user impact, administration, scalability and reliability, support, vendor viability, and cost.

Figure 9. Evasion-Resilient Security Patterns



Set standards for the minimum supported hardware and OS versions, and configure them securely. Use native device features, such as isolation, and maintain proper hardening and patching of operating systems and other software. Use third-party endpoint anti-malware and/or application controls where vendor-provided controls are proven insufficient. The market for EPP solutions is changing, and traditional vendors are no longer the obvious choice for some buyers. On mobile devices, MTD solutions provide application risk management, network protection and device protection beyond what is provided by the OS, unified endpoint management (UEM), enterprise mobile management (EMM) and mobile device management (MDM) alone. For consumerized mobile use cases, consider building security checks and device independence into apps. For example, build in kernel mode attack and jailbreak detection, software updateability and application shielding/runtime application self-protection by leveraging SDKs from MTD and mobile app security vendors.

Network protection of users and endpoints is still necessary, and their availability as cloud-based solutions simplifies deployment. SWGs and SEGs are critical for most organizations' malware and phishing defenses, and network sandboxing approaches have become common for better malware detection. Roaming users also need protection from other network attacks,

like rogue Wi-Fi access points, and MTD provides this capability. In addition, security awareness initiatives, like anti-phishing and anti-malware training, are usually required. Well-designed programs meaningfully increase awareness and thus render people less likely to make bad security decisions by accident or on purpose. Clarity, reinforcement and timeliness – such as sending a bulletin when a phishing email gets through the email filter – are key.

Related research:

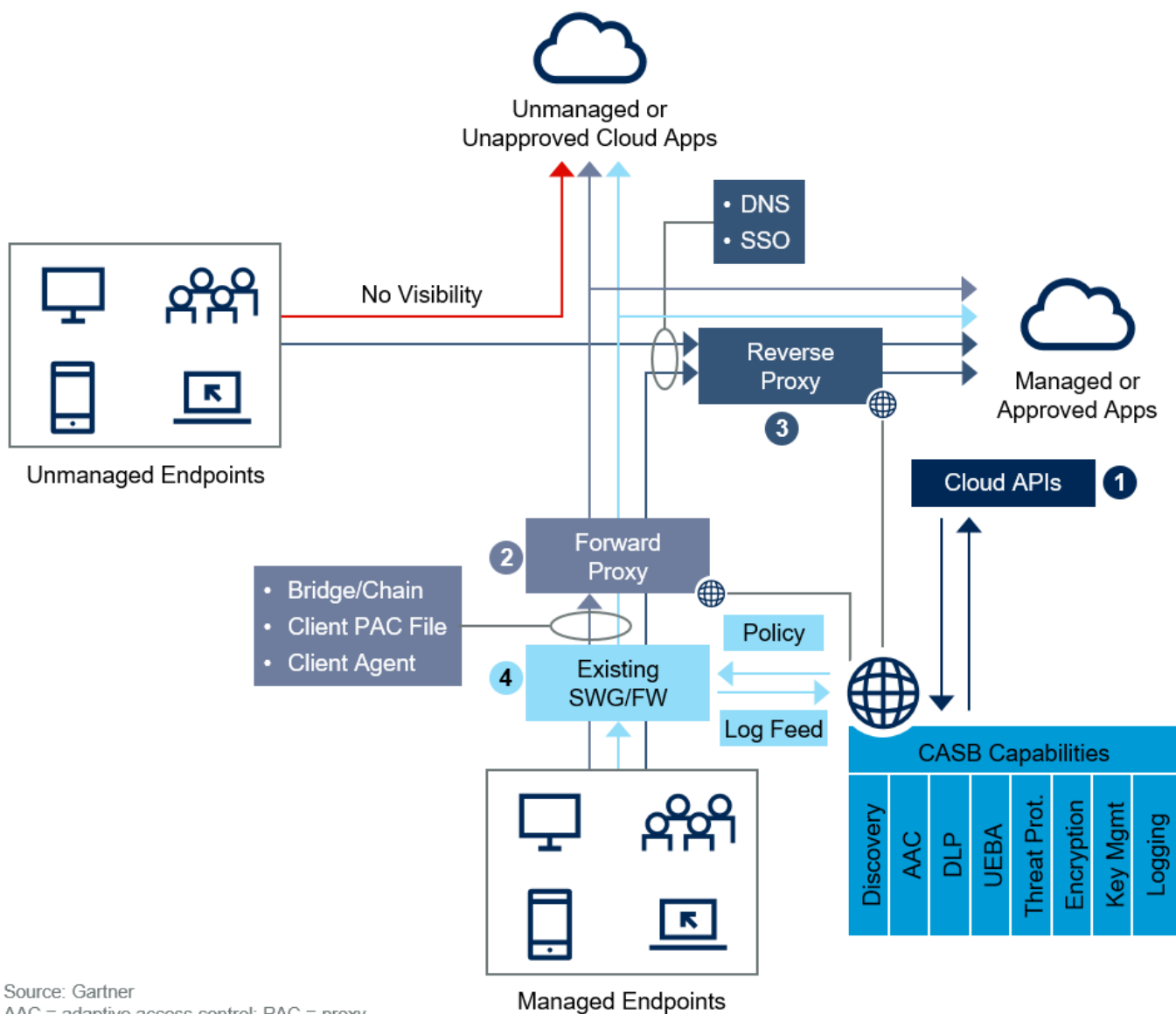
- [“Comparing Techniques for Endpoint Protection”](https://www.gartner.com/document/code/404264?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/404264?ref=authbody&refval=3970104>)
- [“Beyond Detection: 5 Core Security Patterns to Prevent Highly Evasive Attacks”](https://www.gartner.com/document/code/346997?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/346997?ref=authbody&refval=3970104>)
- [“Evaluation Criteria for Endpoint Protection Platforms”](https://www.gartner.com/document/code/346995?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/346995?ref=authbody&refval=3970104>)
- [“How to Build an Effective Malware Protection Architecture”](https://www.gartner.com/document/code/366440?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/366440?ref=authbody&refval=3970104>)
- [“Mobile OSs and Device Security: A Comparison of Platforms”](https://www.gartner.com/document/code/376865?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/376865?ref=authbody&refval=3970104>)
- [“Comparison of Mobile Threat Defense Solutions”](https://www.gartner.com/document/code/347528?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/347528?ref=authbody&refval=3970104>)
- [“Advance and Improve Your Mobile Security Strategy”](#)

Design Endpoint and Mobile Security to Align With Cloud Application Security

Many mobile apps interact with public cloud-based applications, and securing data on mobile devices has to include controlling cloud use from those devices. But perhaps more importantly, security for mobile device interaction with services will need to be hosted in the cloud to guarantee acceptable performance and latency. The cloud view on mobility also helps guide how security for cloud services should be designed. In other words, instead of designing mobile security and cloud security independently, you should approach security on a whole-system basis (see Figure 10).

Figure 10. Cloud Access Security Broker Architecture and Capabilities

Overview of CASB Capabilities and Four Architecture Integration Modes



Source: Gartner
 AAC = adaptive access control; PAC = proxy autoconfiguration; SSO = single sign-on
 ID: 407409

Technologies such as EPP, MTD, UEM and DLP provide device-based threat protection, data protection and user activity visibility. These device-based solutions can be factored into adaptive access control use cases provided by cloud-based technologies like CASBs. CASBs, in particular, provide organizations with a wide variety of integration methods and security capabilities (see Figure 10). For example, proxy-based CASBs serve as an in-line enforcement proxy or an out-of-band detection and response system. Organizations that have a large current or planned mobile and SaaS footprint should evaluate the capabilities that CASB would enable.

In addition to CASB, some vendors also offer ZTNA and RBI products to provide additional options for access to applications. Although ZTNA and CASB proxy approaches are very similar and could technically be combined, the former is often used for access to applications run by the organization itself, rather than to SaaS applications. As a new architecture pattern, RBI provides isolated access from unmanaged endpoints to trusted applications. This is the

opposite of the traditional use of RBI, which isolates trusted endpoints from untrusted websites and applications. Design of CASB, ZTNA, RBI or other network-based solutions has to account for interoperability with not only managed devices and browser-based access, but also unmanaged devices and the particulars of mobile apps.

Organizations leveraging SIEM as a hub for security monitoring activities benefit from these technologies to expand their detection and response capabilities. Direct integration of cloud and mobile environments into the SIEM is often challenging due to limitations in log content, complex log formats and log transport issues. The high volume of logs generated in cloud environments is also a strong reason to incorporate event collection and analytics in a decentralized manner, with alerts still being forwarded to the SIEM for centralized monitoring.

Related research:

- [“How to Secure Cloud Applications Using Cloud Access Security Brokers”](https://www.gartner.com/document/code/393383?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/393383?ref=authbody&refval=3970104>)
- [“Solution Comparison for Cloud Access Security Brokers”](https://www.gartner.com/document/code/377717?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/377717?ref=authbody&refval=3970104>)
- [“Understanding and Implementing Security in Office 365: Exchange Online, SharePoint Online, OneDrive for Business and Teams”](https://www.gartner.com/document/code/349107?ref=authbody&refval=3970104) (<https://www.gartner.com/document/code/349107?ref=authbody&refval=3970104>)
- [“Building an Effective DLP Program”](https://www.gartner.com/document/code/388932?ref=authbody&refval=3970104) (<https://www.gartner.com/document/code/388932?ref=authbody&refval=3970104>)
- [“A Comparison of Remote Network Access Products for Enterprise Endpoints”](https://www.gartner.com/document/code/380285?ref=authbody&refval=3970104)
(<https://www.gartner.com/document/code/380285?ref=authbody&refval=3970104>)

Setting Priorities

Most organizations do not have the time and budget to follow every suggested planning consideration, and Gartner clients occupy a wide spectrum of cybersecurity maturity and capability. Not all industries, geographies and organizational sizes will have the exact same security initiatives. In the previous three years' Planning Guides, priorities were constant and focused heavily on specific control approaches. This year:

1. **Triage high-exposure risk areas and basic controls first.** Security teams find themselves challenged to keep up with selecting critical controls in a changing world of IT and business. As part of implementing basic security hygiene, organizations should place great focus on assets that are highly exposed to external hackers. Email, client endpoints, privileged user accounts for cloud, and internet-exposed data stores, file shares and applications are easily misused or misconfigured. Attackers often identify and enumerate targets and weaknesses within these areas, which makes them common vectors for compromise. Creating visibility into, and protection within, these areas is of utmost importance.

2. **Use security architecture as foundational practice.** To assist in gap assessments and control roadmap planning, security teams must make use of security architecture practices. In addition to using risk management and control frameworks, making use of architecture models that account for capabilities, threats and attacks, and maturity helps provide a more comprehensive view. These practices should be used at the global level for planning security projects, but also at a project level to help map requirements into the existing security architecture.
3. **Engage nonsecurity stakeholders early and often.** Security teams must set aside time to engage with business stakeholders, and to engage with IT teams. Organizations as a whole need to set clear directions on their risk appetite, especially with ongoing changes in the cyberattack and regulatory landscapes. The cost of effective cybersecurity, especially now that talent is hard to find, must be factored into business decisions. As such, a pragmatic, evidence-based, integrated risk management approach with clear communication is critical to ensure that controls are chosen wisely and agreed upon by everyone. Establishing proper metrics and reporting effectiveness (or necessity for improvements) up the hierarchy is key to success.

Gartner believes these priorities will allow organizations to adopt and maintain an adaptive, risk-based approach to security.

Evidence

- ¹ ["Imperva Discloses Security Incident Impacting Cloud Firewall Users."](https://www.zdnet.com/article/imperva-discloses-security-incident-impacting-cloud-firewall-users/)
(<https://www.zdnet.com/article/imperva-discloses-security-incident-impacting-cloud-firewall-users/>) ZDNet.
- ² ["The Equifax Hack Exposed More Data Than Previously Reported."](https://fortune.com/2018/02/11/equifax-hack-exposed-extra-data/)
(<https://fortune.com/2018/02/11/equifax-hack-exposed-extra-data/>) Fortune.
- ³ ["How One Texas County Stopped a Ransomware Attack."](https://www.wsj.com/articles/how-one-texas-county-stopped-a-ransomware-attack-11567169059)
(<https://www.wsj.com/articles/how-one-texas-county-stopped-a-ransomware-attack-11567169059>) The Wall Street Journal.
- ⁴ ["Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens."](https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx)
(<https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx>) (ISC)².

Document Revision History

2019 Planning Guide for Security and Risk Management - 5 October 2018
(<https://www.gartner.com/document/code/361496?ref=dochist>)

2018 Planning Guide for Security and Risk Management - 29 September 2017
(<https://www.gartner.com/document/code/331855?ref=dochist>)

2017 Planning Guide for Security and Risk Management - 13 October 2016
(<https://www.gartner.com/document/code/312926?ref=dochist>)

2016 Planning Guide for Security and Risk Management - 2 October 2015

(<https://www.gartner.com/document/code/281219?ref=dochist>)

2015 Planning Guide for Security and Risk Management - 2 October 2014

(<https://www.gartner.com/document/code/264325?ref=dochist>)

2014 Planning Guide for Security and Risk Management - 3 October 2013

(<https://www.gartner.com/document/code/258041?ref=dochist>)

2013 Planning Guide: Security and Risk Management - 1 November 2012

(<https://www.gartner.com/document/code/245732?ref=dochist>)

2012 Planning Guide: Security and Risk Management - 1 November 2011

(<https://www.gartner.com/document/code/224667?ref=dochist>)

Recommended by the Authors

Building the Foundations for Effective Security Hygiene

(<https://www.gartner.com/document/3885867?ref=authbottomrec&refval=3970104>)

How to Start Your Threat Detection and Response Practice

(<https://www.gartner.com/document/3876789?ref=authbottomrec&refval=3970104>)

Improve Your Security With Security Architecture

(<https://www.gartner.com/document/3934016?ref=authbottomrec&refval=3970104>)

Best Practices for Securing Continuous Delivery Systems and Artifacts

(<https://www.gartner.com/document/3913430?ref=authbottomrec&refval=3970104>)

Build Once, Use Many Times: Use Privacy Engineering to Support a Data-Centric Security Architecture

(<https://www.gartner.com/document/3957235?ref=authbottomrec&refval=3970104>)

How to Secure Cloud Applications Using Cloud Access Security Brokers

(<https://www.gartner.com/document/3956344?ref=authbottomrec&refval=3970104>)

Recommended For You

Mitigating the Risk of Phishing When Technical Security Controls Fail

(<https://www.gartner.com/document/3905999?ref=algotbottomrec&refval=3970104>)

Creating Security Standards: Context, Structure and Must-Have Content

(<https://www.gartner.com/document/3913368?ref=algotbottomrec&refval=3970104>)

Threat-Oriented Approaches to Test Security in Production

(<https://www.gartner.com/document/3875509?ref=algotbottomrec&refval=3970104>)

Utilizing Breach and Attack Simulation Tools to Test and Improve Security

(<https://www.gartner.com/document/3875421?ref=algotbottomrec&refval=3970104>)

Building the Foundations for Effective Security Hygiene

(<https://www.gartner.com/document/3885867?ref=algotbottomrec&refval=3970104>)

© 2019 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

[About Gartner](#) [Careers](#) [Newsroom](#) [Policies](#) [Privacy Policy](#) [Contact Us](#) [Site Index](#) [Help](#) [Get the App](#)

© 2019 Gartner, Inc. and/or its Affiliates. All rights reserved.