Gartner Publishes Top 10 Security Projects for 2019

Devolutions

GARTNER HAS PUBLISHED ITS TOP 10 SECURITY PROJECTS FOR 2019

Gartner has published its **Top 10 Security Projects for 2019**. These 10 security projects represent initiatives Gartner believes all organizations that have already implemented fundamental security measures should adopt ASAP to increase business impact, and to reduce risk.

1. Privileged Access Management (PAM)

The 2018 Global Data Risk Report revealed that 88% of companies with more than 1 million folders do not have appropriate access limitations, while 58% of companies have more than 100,000 folders accessible to all employees. What's more, a separate survey of IT professionals conducted by Centrify found that nearly two-thirds of all breaches involve access to privileged accounts. Gartner advises that PAM projects should include both nonhuman and human systems accounts, and they should support a mix of cloud, on-premises and hybrid environments, along with APIs for automation.

Current PAM solutions in the marketplace are expensive, and most small and midsize businesses (SMBs) cannot justify the cost. For the relatively few SMBs that can afford a PAM solution, they typically lack the in-house technical expertise to understand the differences between core and non-essential requirements. At Devolutions, we are on a mission to change this, and **we plan on launching a robust PAM platform specifically designed for SMBs by November 2019.** Learn more here.

2. CARTA-Driven Vulnerability Management

Continuous Adaptive Risk and Trust Assessment (CARTA) guides security teams to constantly adjust their approach to security, since attempting to stay on top of all possible vulnerabilities is simply not possible. Gartner advises organizations that adopt CARTA to start by establishing the value of IT assets and their associated risks, and clearly understanding network typology and changes to infrastructure. This latter requirement is an important but difficult challenge. A recent survey has shown that only 64% of IT decision-makers have visibility across their entire software portfolio, and only 66% believe that their software is current.

3. Detection and Response

Detection and response capabilities embrace several integrated aspects, including tools that monitor behavior, people, data access, data utilization, and infrastructure technologies (i.e. networks and endpoints). Gartner advises organizations to ask the following key questions:

- How are we gathering and storing data to support our detection and response capabilities?
- Does the technology we have (or are planning to procure and implement) support a wide range of detection and response features, and the ability to utilize indicators of compromise?
- Are we testing vendors that claim to have AI or machine-learning capabilities?

While effective threat detection and response is critical for closing the gap between the speed of compromise and the speed of discovery, it is also getting tougher. According to ESG research, 76% of cybersecurity professionals say that threat detection and response is harder today than it was two years ago, primarily due to a maze of disconnected point tools.

4. Cloud Access Security Broker (CASB)

A CASB is a security policy enforcement point, which is positioned between cloud service consumers and cloud service providers to generate visibility. It essentially functions as a gatekeeper that enables organizations to extend security policies beyond their own infrastructure. Gartner advises organizations to start by conducting cloud application discovery to reveal shadow IT, which are IT projects that are managed outside of — and without the knowledge of — the IT department. After this, organizations should determine what level of control they need for each SaaS application, and enter into short-term agreements with cloud-based services that promise to discover and secure sensitive data.

5. Cloud Security Posture Management (CSPM)

Through 2023, 99% of all cloud security failures will be the customers' fault. CSPM dramatically reduces customer-driven mistakes, mismanagement or misconfiguration, while also reducing the problem of "alert fatigue" that many of today's SecOps teams struggle with. Gartner advises organizations who use a single IaaS platform to tap their current vendor and see if they have CSPM offerings. If not, then many cloud-based CSPM options are available, including those provided by CASBs.

6. Business Email Compromise (BEC)

According to the FBI Internet Crime Report, losses attributed to BECs reached a staggering $1.3 billion in 2018 — more than double that of 2017. To avoid getting victimized, Gartner advises organizations to correct process breakdowns, increase technical controls, integrate customizable machine learning options with email security systems, deploy endpoint protections, and provide security awareness training. This latter directive is especially important, given that 70% of employees still don't understand privacy and security best practices.

7. Dark Data Discovery

Dark data is information that organizations organically create and passively store through normal business operations. While this information is low value to the organization, it may pose a risk if accessed and exploited by hackers or other bad actors. Gartner advises organizations to target dark data that lives in multiple silos and choose vendors that offer a wide data repository support for systems that store sensitive data.

8. Security Incident Report

According to the 2018 SANS Incident Response Survey, one-third of participants admitted they didn't know how many security incidents they failed to respond to, and 15% said they didn't know if some security incidents resulted in data breaches. A robust Security Incident Report process improves visibility, awareness, and response capabilities. Gartner advises organizations to assess whether their current response plan could be improved, and to explore the viability of establishing an Incident Response Retainer (IRR) with a vendor that will build a program around their specific needs and budget.

9. Container Security

Container security is designed to protect the container pipeline and application, along with the container deployment environment and infrastructure. Gartner advises organizations to ensure that their container security project integrates with common developer tools and CI/CD pipeline, and to leverage APIs in order to support multiple security tools. Organizations should start by scanning for known vulnerabilities, and then move into runtime production.

10. Security Rating Services (SRS)

SRSs deliver ongoing, real-time scoring for internal assessments, procurement, partnerships and M&A activities. Gartner cautions organizations that SRSs can only supplement visibility, since they highlight key services. They don't provide a 360-degree view of the entire digital ecosystem.