Gartner Top 9 Security and Risk Trends for 2020

CISOs should understand these trends to practice strong planning and execution of security initiatives.

The shortage of technical security staff, the rapid migration to cloud computing, regulatory compliance requirements and the unrelenting evolution of threats continue to be the most significant ongoing major security challenges.

However, responding to COVID-19 remains the biggest challenge for most security organizations in 2020.

“The pandemic, and its resulting changes to the business world, accelerated digitalization of business processes, endpoint mobility and the expansion of cloud computing in most organizations, revealing legacy thinking and technologies,” said Peter Firstbrook, VP Analyst, Gartner, during the virtual Gartner Security and Risk Management Summit, 2020.

COVID-19 refocused security teams on the value of cloud delivered security and operational tools that don’t require a LAN connection to function, reviewing remote access policies and tools, migration to cloud data centers and SaaS applications, and securing new digitization efforts to minimize person-to-person interactions.

Gartner has identified nine annual top trends that are the response by leading organizations to these longer-term external trends. These top trends highlight strategic shifts in the security ecosystem that aren’t yet widely recognized, but are expected to have broad industry impact and significant potential for disruption.

Trend No. 1: Extended detection and response capabilities emerge to improve accuracy and productivity

Extended detection and response (XDR) solutions are emerging that automatically collect and correlate data from multiple security products to improve threat detection and provide an incident response capability. For example, an attack that caused alerts on email, endpoint and network can be combined into a single incident. The primary goals of an XDR solution are to increase detection accuracy and improve security operations efficiency and productivity.

“Centralization and normalization of data also helps improve detection by combining softer signals from more components to detect events that might otherwise be ignored,” said Firstbrook.

Trend No. 2: Security process automation emerges to eliminate repetitive tasks

The shortage of skilled security practitioners and the availability of automation within security tools have driven the use of more security process automation. This technology automates computer-centric security operations tasks based on predefined rules and templates.

Automated security tasks can be performed much faster, in a scalable way and with fewer errors. However, there are diminishing returns to building and maintaining automation. SRM leaders must invest in automation projects that help to eliminate repetitive tasks that consume a lot of time, leaving more time to focus on more critical security functions.

Trend No. 3: AI creates new security responsibilities for protecting digital business initiatives

AI, and especially machine learning (ML), continues to automate and augment human decision making across a broad set of use cases in security and digital business. However, these technologies require security expertise to address three key challenges: Protect AI-powered digital business systems, leverage AI with packaged security products to enhance security defense and anticipate nefarious use of AI by attackers.

Trend No. 4: Enterprise-level chief security officers (CSOs) emerge to bring together multiple security-oriented silos

In 2019, incidents, threats and vulnerability disclosures outside of traditional enterprise IT systems increased, and pushed leading organizations to rethink security across the cyber and physical worlds. Emerging threats such as ransomware attacks on business processes, potential siegeware attacks on building management systems, GPS spoofing and continuing OT/IOT system vulnerabilities straddle the cyber-physical world. Organizations primarily focused on information-security-centric efforts are not equipped to deal with the effect of security failures on physical safety.

As a result, leading organizations that deploy cyber-physical systems are implementing enterprise-level CSOs to bring together multiple security-oriented silos both for defensive purposes and, in some cases, to be a business enabler. The CSO can aggregate IT security, OT security, physical security, supply chain security, product management security, and health, safety and environmental programs into a centralized organization and governance model.

Trend No 5. Privacy is becoming a discipline of its own

No longer "just a part of" compliance, legal or auditing, privacy is becoming an increasingly influential, defined discipline of its own, affecting almost all aspects of an organization.

As a rapidly growing stand-alone discipline, privacy needs to be more integrated throughout the organization. Specifically, the privacy discipline co-directs the corporate strategy, and as such needs to closely align with security, IT/OT/IoT, procurement, HR, legal, governance and more.

Trend No. 6: New "digital trust and safety" teams focus on maintaining the integrity of all interactions where consumer meets the brand

Consumers interact with brands through an increasing variety of touchpoints, from social media to retail. How secure the consumer feels within that touchpoint is a business differentiator. Security for these touchpoints is often managed by discrete

groups, with specific business units focusing on areas they run. However, companies are increasingly moving toward cross-functional trust and safety teams to oversee all the interactions, ensuring a standard level of safety across each space where consumers interact with the business.

Trend No. 7: Network security transforms from the focus on LAN-based appliance models to SASE

Cloud-delivered security services are growing increasingly popular with the evolution of remote office technology. Secure access service edge (SASE) technology allows organizations to better protect mobile workers and cloud applications by routing traffic through a cloud-based security stack, versus backhauling the traffic so it flows through a physical security system in a data center.

Trend No. 8: A full life cycle approach for protection of the dynamic requirements of cloud-native applications

Many organizations use the same security product on end-user-facing endpoints as they did for server workloads, a technique that often continued on during “lift and shift” cloud migrations. But cloud-native applications require different rules and techniques, leading to the development of cloud workload protection (CWPP). But as the applications grow increasingly dynamic, the security options need to shift as well. Combining CWPP with the emerging cloud security posture management (CSPM) accounts for all evolution in security needs.

Trend No. 9: Zero-trust network access technology begins to replace VPNs

The COVID pandemic has highlighted many of the problems with traditional VPNs. Emerging zero-trust network access (ZTNA) enables enterprises to control remote access to specific applications. This is a more secure option, as it “hides” applications from the internet — ZTNA only communicates to the ZTNA service provider, and can only be accessed via the ZTNA provider’s cloud service.

This reduces the risk of an attacker piggybacking on the VPN connection to attack other applications. Full-scale ZTNA adoption does require enterprises to have an accurate mapping of which users need access to what applications, which will slow adoption.

This article has been updated from the original, created on June 22, 2020, to reflect new events, conditions and research.