Addressing Insider Threats, Cyber Attacks & Data Security

Insider threats, whether executed through accidental or malicious intent, continue to plaque organizations big and small. Banks today remain highly vulnerable to these attacks, and as a result, are now looking at innovative new approaches and technologies to regain a position of strength. From a reference architecture standpoint two interesting models have emerged in the last few of years – Forrester's Zero Trust Architecture, and Gartner's Adaptive Security Architecture.

Forrester's Zero Trust Architecture is based on the simple premise that individuals and their machines can no longer be trusted. Not to say that all individuals have to be looked at with a skeptical eye. It's a reality of our times as we recognize the likelihood and ease with which credentials are captured by malicious actors then used as part of an orchestrated campaign. Utilizing the latest in network-based security tools such as a "next-generation based firewall" (NGFW), Forrester defines a model that identifies crucial data, the applications that link to that data, and the users and endpoints that ultimately have access. Once that's determined, a tight perimeter is established with regular monitoring and enforcement to ensure only those who should have access to that data actually do. And everyone else is forcefully kept out through the application control mechanisms built into today's NGFW.

Gartner's Adaptive Security Model takes this another step further and outlines the requirements that the overall technology supporting the architecture must fulfill. Specifically, the network and endpoint security technologies protecting the data must be able to predict, detect, prevent and respond to all threats in real time. This includes threats that have never been seen before in the wild, or use advanced obfuscation techniques to try and avoid detection. Achieving this requires a level of integration and automation that is only now emerging at the endpoint. This crucial step serves and the final frontier in an evolution that's been fueled by a massive amount of R&D investment that's been made in IT security over the last 4-5 years specifically. This innovation has brought us the NGFW, network-based sandboxing, improved web security, and new endpoint detection and response (EDR) capabilities to quickly identify compromised hosts. But is it enough?

SentinelOne has recently been honored by Gartner as a 'visionary' in their annual Endpoint Protection Platform Magic Quadrant. This recognition is due to SentinelOne's unique integration that brings together the detection, prevention and remediation of advanced, targeted threats in real time. At the core of SentinelOne's platform lies a behavioral-based detection engine that closely monitors all system processes, combined with machine learning, to quickly identify and route out malicious patterns. Once these patterns are detected SentinelOne initiates an automated set of mitigation actions to kill all malicious processes and quarantine the endpoint to prevent any potential for exfiltration or lateral movement. SentinelOne's platform maps directly to Gartner's Adaptive Security Architecture and provides a powerful tool in a layered network and endpoint security defense model. SentinelOne also compliments Forrester's Zero Trust architecture by ensuring insider threats can be quickly contained before an actor can achieve their objectives, even within a secure zone.

Scott Gainey
CMO

SentinelOne

Contact Info

www.sentinelone.com
855 868 3733

Scott Gainey is responsible for SentinelOne's global marketing organization. Prior to SentinelOne, Scott was VP of Marketing at Palo Alto Networks responsible for product and solutions marketing, communities, and demand generation. Scott brings nearly 20 years of high-tech business-to-business marketing experience while serving in various leadership positions at Cisco, Xsigo Systems, NetApp, Veritas and Sun Microsystems. SentinelOne is transforming endpoint security to protect organizations from advanced cyber threats that have rendered anti-virus obsolete. The company uses Dynamic Execution Inspection to detect and protect devices against targeted malware and zero-day attacks in real time. SentinelOne was formed by an elite team of cyber security and defense experts from Check Point, IBM, Intel, Israel Defense Forces, McAfee, and Palo Alto Networks.