Solution Brief

SECB Autonomous XDR

EDR MOVES TO XDR: TODAY'S FUTURE OF DETECTION AND RESPONSE

Extending the security of endpoint protection

Endpoint protection platforms (EPP) and endpoint detection and response (EDR) have become extremely important components of corporate cybersecurity strategies. As they evolved from antivirus software, endpoint security solutions have provided enterprises with an additional layer of security that includes advanced, comprehensive measures around threat detection and response, device management, data loss prevention (DLP) and more. However, due to the changing threat landscape, the gap between what is needed and what EDR solutions can deliver appears to be widening. Beyond the gaps, the cost and complexity associated with EDR solutions prevent many enterprises from even considering them. Likewise, due to its singular focus on the endpoint, EDR software often fails to detect threats that penetrate via unconventional attack vectors, leaving endpoints unprotected and enterprise management unconvinced of its value.

Mind the multi-vector gap in EDR

Cyberattacks are becoming more sophisticated every day, fueled by increasingly connected networks that broaden the attack surface and create new opportunities for entry. As attack vectors multiply, many enterprises address each vector with a best-in-class solution to protect those specific vulnerabilities. Today, security teams have many solutions in place, including EDR, but lack a unified way to manage their numerous security systems. As a result, security data is collected and analyzed in siloes, creating gaps in what security teams can see and investigate.

Without an integrated, overall view of security events, multi-vector threats can continue to avoid detection as cybercriminals exploit the gaps between systems.

For example, in a script-based or fileless attack, bad actors use a legitimate application, such as MS PowerShell, to inject and run a malware script whenever PowerShell is open in memory. The same "Bypass" parameter in PowerShell that lets admins remotely execute commands can be used by cybercriminals to remotely download and run a script directly into memory, without copying the file to disk. Since the script leaves no trace of I/O activity, EDR cannot detect the threat. This is just one example of how fileless malware attacks can infect endpoints without leaving a trace (similar to in Stuxnet and UIWIX). To detect such threats, experts recommend looking for the occurrence of unusual commands in log files. Since PowerShell is typically used for specific operations, a few uncommon commands will stick out and often can be picked up by network traffic analysis solutions.

This is only one example proving the critical need to detect multi-vector threats by giving security teams an integrated view of security data. Otherwise, there will always be blind spots where threats can hide out and do great damage. It's time to make your EDR solution part of a unified and integrated XDR approach to cybersecurity.

The Tipping Point – from EDR to XDR

EDR is one of many solutions organizations have adopted to enhance their cybersecurity posture. Also popular are network traffic analysis (NTA) solutions that analyze network traffic communication patterns to detect anomalies and threats; as well as security information and event management (SIEM) systems that perform real-time analysis of security alerts generated by network applications and hardware.

Like EDR, these solutions are reactive, and they operate in siloes rather than across all attack vectors in the enterprise network. To effectively defend infrastructure and data from breach and misuse, organizations need to remove siloed barriers and adopt a unified, multi-vector solution to threat detection and response. To that end XDR solves this need and goes beyond current limitations.

XDR = eXtended detection & response

Security data from the enterprise network, cloud and endpoints streams into a single platform that enables unified threat visibility, analysis, and automated response across all security systems in the enterprise. The unified SecBI XDR approach provides a complete, real-time picture of multi-vector attacks and automates immediate investigation and immediate response.

By continuously collecting and analyzing real-time data and security alerts from EPP/EDR, security gateway, SIEM, and SOAR sources into a single platform, XDR paints the full scope of every serious incident. XDR telemetry automates rich data collection from remote points, automating and accelerating SOCs' ability to detect, investigate and respond quickly to stop attacks. The SecBI XDR leverages unsupervised machine learning (ML) to analyze, qualify, and rank security alerts in real time, automatically closing routine alerts, and advancing and prioritizing only those threats that require attention. By applying behavioral analytics, powered by ML, XDR profiles user and endpoint behavior to detect anomalies that could indicate a threat.

The SecBI XDR Platform

SecBI XDR platform optimizes an EPP/EDR solution by turning it into the nerve center of the enterprise SOC. The SecBI XDR platform synthesizes security alert data across the entire network and all its endpoint, network and mail gateways, and cloud security systems. From siloed data sources, it paints a unified and clear forensic picture of multi-vector attacks, automates investigation and speeds response. This automated system works to continuously monitor and react to network activity, so security teams don't have to.

SecBI's Autonomous Investigation™ technology discovers the full scope of an attack, including affected entities, kill chain and root cause. The technology automatically traces the attack across all stages, integrating related data and evidence collected from multiple data sources for easy understanding. SecBI analyzes all data in parallel, instead of sub-sampling like many Entity Behavior Analytics (UEBA) solutions do. As a result, SecBI detects a broader range of threats with greater accuracy.

Transform your cybersecurity operations with XDR now. Take the multiple sources of information in your network that remain untapped and underutilized, and pool them together in the SecBI XDR platform to increase SOC team productivity, reduce alert fatigue, and stay on top of evolving attacks.

The "X" reflects the extended cross product approach of using multiple sources for amplified threat detection and response capabilities.

Agent-less, Vendor-agnostic Platform

Allows enterprises to optimize their investment in current cyber-security tools and receive better and wider protection.

Built for easy & seamless integration

SecBI provides a wizard to easily add any REST API supporting product to the system within minutes and leverage all the relevant automations.

Visit

www.secbi.com/partners/

or write

partner@secbi.com

To become a SecBI XDR Technology Partner

SECBI
Autonomous XDR