PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH SYMANTEC PROXYSG®

Attivo Networks® has partnered with Symantec to provide advanced, real-time, in-network threat detection and improved automated incident response. With the joint solution, customers receive improved threat intelligence to isolate compromised systems based on suspicious activity. Organizations can reduce time and resources required to detect threats, analyze attacks, isolate attackers, and to remediate infected endpoints, ultimately decreasing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- End-point Deception Credentials Distribution

THE CHALLENGE

Cyberattackers have proven repeatedly that they can, and will, infiltrate the networks of even the most security-savvy organizations. Whether the attacker gets in using stolen credentials, a zero-day exploit, an email-based attack, or simply starts off with insider access, they will establish a foothold and move laterally through the network until they reach their intended target. Attackers have also proven that once inside they can evade the remaining security solutions and traverse the network undetected.

Quickly detecting and shutting down attackers that are already inside the network requires a new security approach that does not rely on typical measures, such as known signatures or attack pattern matching. Deception technology delivers this new approach, tricking attackers into revealing their presence, delivering high fidelity alerts to quickly and efficiently disrupt the attack. It can also capture valuable attack forensics and threat intelligence that organizations can use to bolster their defenses and make future attacks more difficult.

THE ATTIVO THREAT DEFEND PLATFORM AND SYMANTEC PROXYSG JOINT SOLUTION

Integrating the Attivo ThreatDefend™ Deception Platform with Symantec ProxySG is simple. In minutes, organizations can have an integrated adaptive security platform that provides effective, real-time, detection of cyberattackers, that can automatically block and isolate infected systems to effectively contain the attack, disrupt attacker command and control traffic, and stop data exfiltration. The integrated solution provides a real-time, non-disruptive way of detecting and blocking active threats inside the network, not giving an attacker the opportunity to reach their external assets or exfiltrate valuable company assets and information.

Automating threat identification has become critically important as lateral movement speeds increase for both live attackers and malware. Combining the Attivo Networks BOTSink® Engagement Server and the Symantec ProxySG provides automated, real-time, protection, detection, and identification capabilities that outperform systems that rely on manual intervention.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the Attivo Networks solution provides network, endpoint, and data deception across an organization. The system has proven highly effective in detecting threats from all vectors, including reconnaissance, stolen credentials, Man-in-the-Middle attacks, Active Directory compromise, ransomware, and insider threats.

The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers delivering decoys, lures, and breadcrumbs to an attacker, ThreatDirect® to extend deception into remote locations, the ThreatStrike® endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) to coordinate the entire deception suite. Together, these components create a comprehensive early detection and active defense platform against advanced cyber threats.

SUMMARY

The Attivo Networks ThreatDefend Platform plays a critical role in enabling an active defense with in-network threat detection and native integrations to dramatically accelerate incident response.

The ThreatDefend solution can identify compromised endpoints and automatically send validated alerts directly to the Symantec ProxySG. In turn, policies on the ProxySG can automatically isolate infected systems and reduce the attacker's ability to spread undetected. The time saved in automated isolation is critical to preventing lateral movement and data exfiltration. Where a strategy that depends upon manual intervention may work for low-severity alerts, high-severity attacks may not afford security teams time to react. Automation gives the advantage back to the security team and will help contain the attacker before they can exfiltrate data or cause mass damage.

The need for this integration is urgent. In a single year, over one billion sensitive records have been stolen with detrimental impact to individuals and enterprises. The resulting damage to the companies' reputations and balance sheets has reached into the billions of dollars. By implementing solutions that detect in-network threats early, automatically isolate them, and deliver ability to hunt for additional threats, organizations can mitigate the risk of large-scale breaches.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, ICS-SCADA, POS and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT SYMANTEC

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

www.symantec.com