CHECK POINT + ATTIVO NETWORKS

REAL-TIME IN-NETWORK DETECTION, ANALYSIS AND AUTOMATED INCIDENT RESPONSE

Benefits

- Real-time threat detection
- Attack forensics and threat analysis
- Faster incident response
- Automatic or manual blocking

INSIGHTS

Organizations deploy a wide variety of point solutions to protect their critical assets from threats. While the network may seem airtight, gaps in security have consistently led to breaches in companies of every size across all industries. Amplifying this problem, many security devices do not communicate with each other – meaning alerts from one device are not sent to other devices to stop the same threat at different points in the network. This lack of communication leads to networks being susceptible to cyber-attacks. Together, Check Point and Attivo are closing this security gap with a simple and comprehensive solution to protect critical assets.

SOLUTION

The Attivo Networks® and Check Point® Software Technologies joint solution delivers a simple way to detect, analyze, and automatically block cyber-attacks. Customers can use the Attivo ThreatMatrix™ Deception and Response Platform to detect infected systems inside the network. The Attivo Deception Platform can automatically send infected IP addresses and attack signatures to the Check Point management server to block the infected system. Together, we reduce the risk of a breach and data loss by minimizing the time-to-detection and time-to-block threats inside the network.

BLOCK THREATS IN REAL-TIME

As cyber-attacks continue to increase in complexity and effectiveness, a modern combination of prevention and detection techniques can effectively protect critical assets in the network. Additionally, as prevention and detection tools gain more information on attacks and how to prevent them, a common thread of communication needs to exist to decrease the time to detect, block, and remediate attacks. This continuous communication will improve the performance of prevention systems as well as incident response, ultimately saving time and money.

The process begins with the ThreatMatrix Platform identifying a threat that has started to infect machines on the network. Once the threat has engaged with the deception platform, the attack is analyzed in a quarantined environment. Detailed attack forensics including signatures and attack patterns are relayed to the Check Point Next Generation Threat Prevention platform, reinforcing threat prevention capabilities and automating blocking to prevent exfiltration of data.

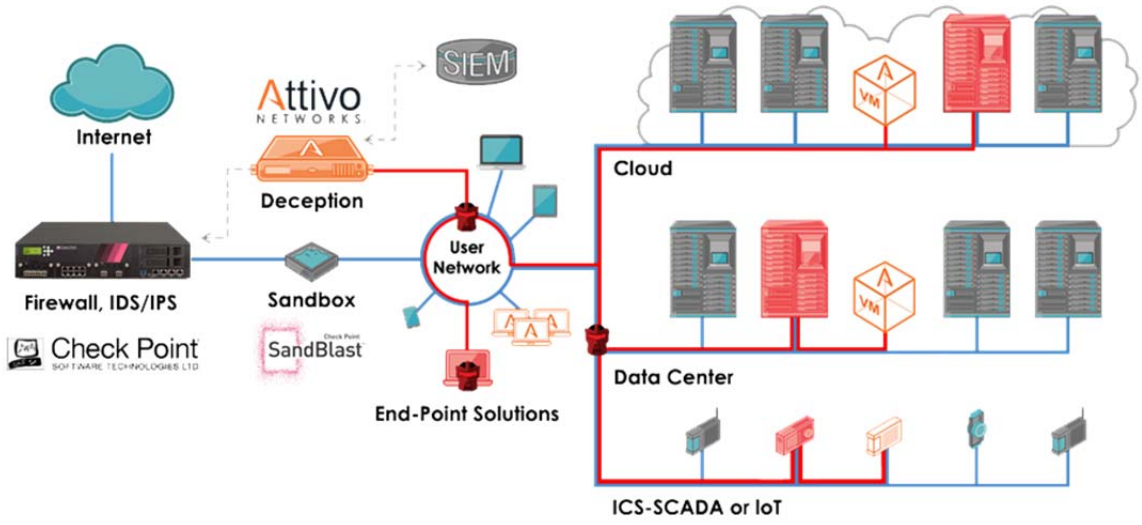
INCREASE ATTACK VISIBILITY

The deception platform – comprised of BOTsink Engagement Servers, ThreatStrike End-point Deception Suite, and Threat Matrix analysis engine – detects threats from multiple vectors including stolen credentials, ransomware, phishing, and insider attacks. Attacks are detected within user networks, data centers, clouds, IoT, and ICS-SCADA environments. Using deception, this solution lures and misdirects attackers trying to reach or compromise valuable company assets.

As hackers attempt to escalate privileges and find targeted assets, attacks are detected at any point of infection, from initial reconnaissance to lateral movements within the network. Once the hacker is engaged, the platform collects and correlates the full Techniques Tactics and Procedures (TTP) with associated forensics and reports via IOC, STIX, CSV, and PCAP formats. We share this information either manually or automatically with the Check Point Next Generation Threat Prevention platform to empower organizations with the information they need to stop the attack.

SUMMARY

Real-time detection and comprehensive incident response are critical to avoid a full network breach. By adding the Attivo Threat Matrix Deception and Response Platform to an organization's security suite, time to detection is improved, detailed attack forensics are gathered, and substantiated alerts are raised, ultimately improving a company's ability to defend against advanced cyber-attacks. Paired with the Check Point Next Generation Threat Prevention platform, customers fortify their incident response capabilities with automatic or manual blocking, detailed information for remediation, and prevention capabilities.



ABOUT CHECK POINT

Check Point Software Technologies Ltd. (https://www.checkpoint.com) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyber-attacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT ATTIVO NETWORKS

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

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com