CHECK POINT + GUARDICORE
DATA CENTER SECURITY

BENEFITS

- Unparalleled visibility into attacker activity inside the data center
- Detection of APT and malware propagation inside data centers (east-west traffic)
- Attack analysis and detection of attacker's footprint
- Automated incident response based on full understanding of the breach
- Reduced breach detection time
- Automated detection, quarantine and remediation of infected virtual machines

INSIGHTS

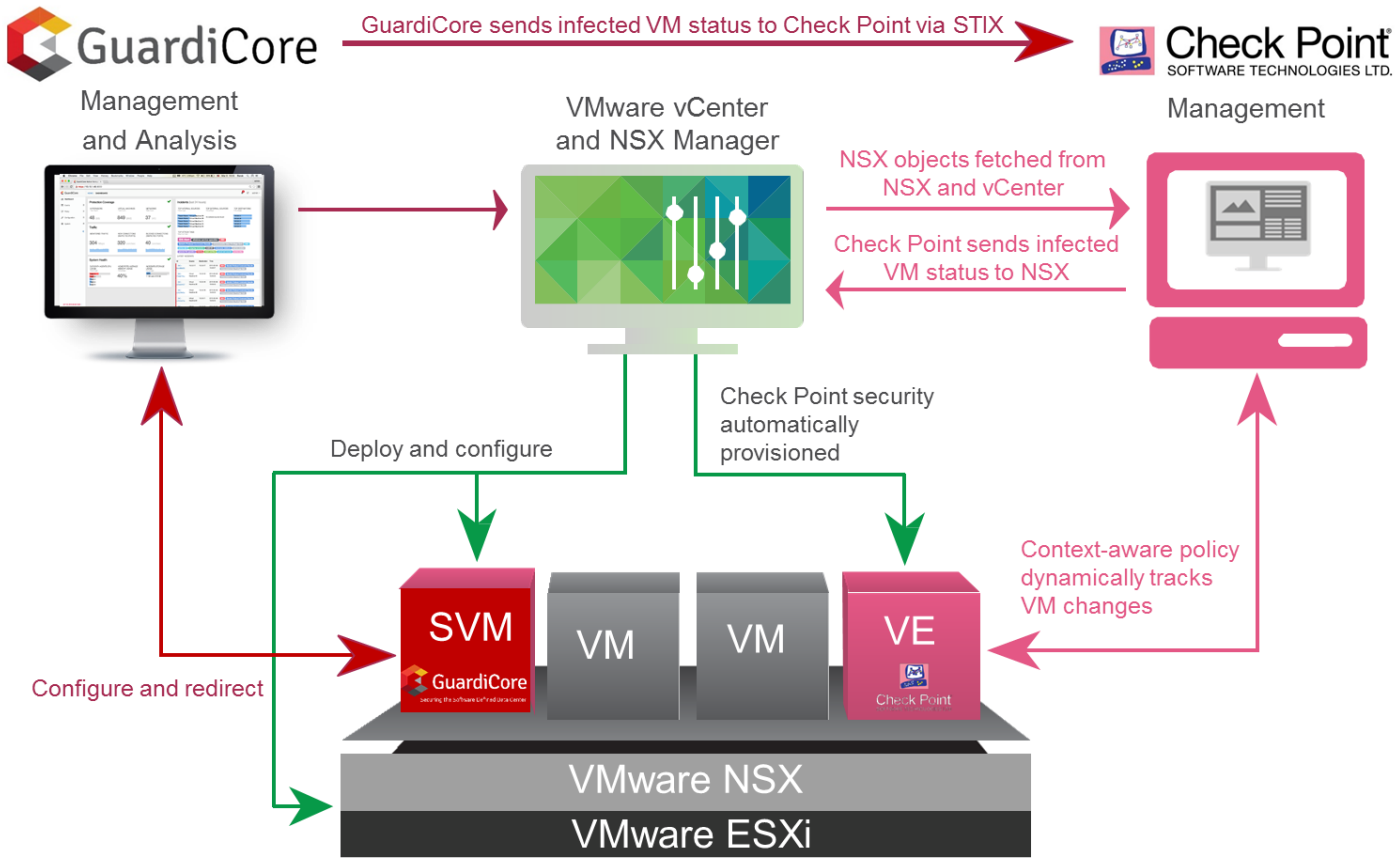
Cloud computing offers advantages over traditional data centers in availability, scalability and cost, but these virtualized environments also expose your company to whole new set of security challenges. When it comes to security, the focus has mainly been on protecting the perimeter, or north-south traffic, going into and out of the data center. There are few controls to secure east-west traffic inside the data center. This presents a security risk where threats can traverse unimpeded once inside the data center.

Intruders are hard to detect. It typically takes many months to discover a breach. Attackers will probe the network until they are able to use what is allowed by the security policy. In the early stage of an attack, APTs and insider threats are likely to generate blocked or failed connection attempts. Blocked traffic may indicate a breach or may be operational traffic. How does a security administrator determine when blocked traffic indicates a threat? When a threat is detected how long does it take to remediate the threat?

REAL-TIME DATA CENTER THREAT RESPONSE

Together Check Point and GuardiCore protect critical corporate data and business processes in the data center. GuardiCore identify attacks in real time and provides Indicators of Compromise (IOC) to Check Point using the STIX (Structured Threat Information Expression) API, allowing security administrators to block future attacks in the data center and at the perimeter.

The GuardiCore Data Center Security Suite analyzes APT and bot attacks, enabling an automated, real-time response. Blocked connection attempts are typically not inspected in real-time. GuardiCore understands that these blocked connection attempts may be the result of an APT or bot's lateral movement inside the data center. As such, any blocked attempt is considered a suspect attack, and seamlessly redirected to a Deception Engine, which provides the expected service in a highly monitored, instrumented environment. An Attack Semantics Engine analyzes the suspect attack's behavior and looks for signs of malicious actions such as exploitation, brute-force into management port, password harvesting, and manipulation of log files and upload of backdoors and attack tools. Any action by the attacker is recorded, and a detailed, readable and actionable report is generated.



GuardiCore Data Center Security Suite integration with Check Point vSec in a VMware SDDC

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyber-attacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT GUARDICORE

GuardiCore is a leader in internal data center security and breach detection. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber-attacks in their data centers. More information is available at www.guardicore.com.

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