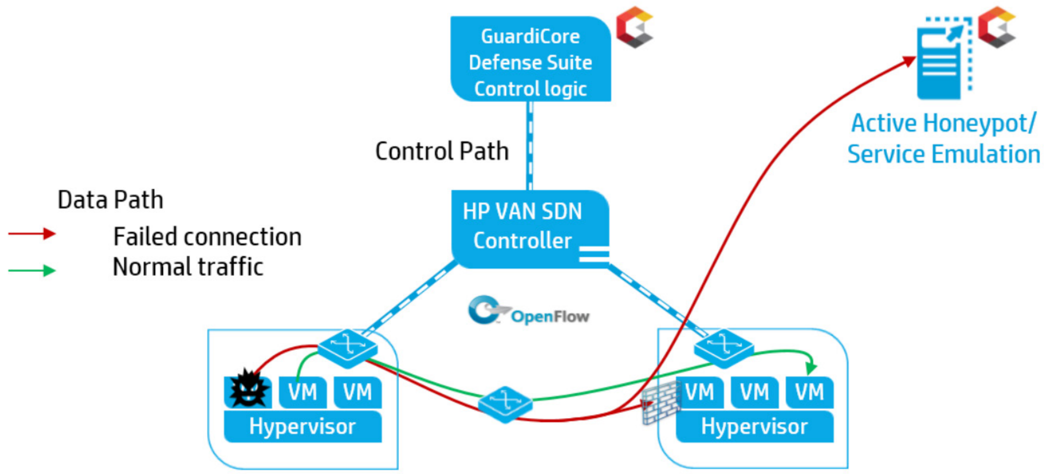
Solution brief

Data center security redefined

GuardiCore Defense Suite, powered by the HP VAN SDN Controller

Stop attacks from within the data center with an Active Honeypot.



Benefits

- Stop insider attacks
- Stop APTs and prevent malware from spreading
- Save costs with reduced manual investigation, early prevention, and automatic policy enhancement & enforcement

> "GuardiCore is focused on providing innovative layers of defense for Data Centers and cloud networks. Working with the HP VAN SDN Controller, we are able to leverage the full value of SDN and offer our customers a reliable solution."

- Ariel Zeitlin, Chief Technology Officer GuardiCore

Overview

Protect your data center from within

GuardiCore is focused on protecting data centers, the heart of organizational business logic and its sensitive data. The explosion of East-West traffic limits the use of advanced security techniques such as Sandboxing, Emulation, IDS and IPS inside data centers, while user-owned virtual machines limit the effectiveness of endpoint security in data centers.

Using SDN and leveraging the HP VAN SDN Controller platform, GuardiCore is set to bring a new breed of network defense to data centers, creating a new kill-chain for different components, or building blocks of an Advanced Persistent Threats (APTs) inside data centers. The first exposed part of GuardiCore's Defense Suite, the Active Honeypot, goes after active network mapping, a critical component of APTs, in data centers.

Today, data centers' most effective defense tools are peripheral, designed to keep attackers out. APTs need only one mistake in order to get inside the data center. Once inside the data center they are very hard to detect.

Currently, security inside data centers relies mostly on separation policy, or 'closed doors', by means such as firewalls, VLAN separation and Access Control Lists. While closed doors are a good practice, some doors must be kept open to allow normal business operation.

When attackers get inside data centers, they typically land in an arbitrary server, and start by mapping the network and trying to connect to and infect other servers. In many cases such attempts will be blocked by an existing separation policy or simply reach a closed port on target machines. But attacker will keep trying and eventually find an open door of vulnerability to exploit and propagate.

The GuardiCore Active Honeypot represents a new breed of network security tools. Blocked and failed connections are dynamically and seamlessly re-routed, without the attacker's awareness, to perform deep investigation, exposing the true intention of the connection attempt and reliably identifying and mitigating a malicious attack in real time.

Why GuardiCore & HP

GuardiCore—Pioneer in network security for data centers

The GuardiCore Active Honeypot, combined with the HP Software-defined Networking (SDN) Architecture, adds a new layer of defense by efficiently preventing targeted attacks from within the data center at an early stage, before they are able to cause significant damage. Attacks are not only prevented, but are also investigated to create and implement more advanced security policies.

HP Open SDN Architecture
The HP SDN architecture spans the infrastructure, control and application software layers, making the network easier to manage with maximum agility.

The HP Virtual Application Network (VAN) SDN Controller platform, paired with network infrastructure supporting the industry standard OpenFlow protocol, provides centralized control of a programmable, end-to-end network designed to dynamically adjust to your evolving business needs. The platform's reliability, consistent APIs and rich features, empower applications, such as GuardiCore Defense Suite, to deliver greater network efficiency, plus more advanced security, Quality of Service management, and rapid application or service delivery.

How it works

The GuardiCore Active Honeypot detects connections that were blocked by an existing security policy inside a data center. This detection is done in real-time and is enabled by the network-wide visibility exposed by the HP VAN SDN Controller. The detected blocked connections are then "revived" by GuardiCore Defense Suite, via the HP VAN SDN Controller, and are kept alive artificially by dynamically re-routing the connection to the Active Honeypot. The Active Honeypot is an isolated and highly monitored environment that provides the service the suspicious connection was looking for.

This re-routing occurs in real-time and without the suspect's awareness since the connection request is not just blocked. Simply blocking the connection would allow an attacker to seek other entry points. Instead, the Active Honeypot allows for continued monitoring to learn from the actions taken had entry actually been granted.

Deep analysis exposes the true intention of the connection attempt and reliably identifies a malicious attack. Based on the analysis, further actions are automatically taken to contain the attack and enhance security policies to proactively prevent future attacks.

SDN makes a difference

The GuardiCore Active Honeypot, with the HP VAN SDN Controller, utilizes dynamic programmability and end-to-end network visibility to provide a way to understand what would have happened had a blocked connection succeeded. This enables you to detect attacks on the network at a very early stage and fundamentally changes the way network security and forensics are done. All without reducing the existing separations among the internal networks and servers.

GuardiCore Defense Suite, through the HP VAN SDN Controller, also leverages the complete SDN architecture to automatically implement smart network responses based on the investigative analysis as well as automatically implement enhanced security policies to prevent future attacks.

Summary

The GuardiCore Defense Suite's Active Honeypot, paired with the HP VAN SDN Controller and SDN infrastructure, adds a new layer of internal, in-depth defense to address the problem of internal data center vulnerability as well as builds additional intelligence to enhance security policies.

The automated, dynamic programmability of the network delivers much greater data center and network security while also saving administrative and investigation costs. You are ultimately able to protect your data center both inside and out.

Learn more at
hp.com/sdn
guardicore.com

Contact us
sdnalliancesteam@hp.com

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document