GuardiCore
Securing the Software Defined Data Center

Technical Brief

# Internal Data Center Security and Breach Detection for VMware NSX

## BENEFITS

**Breach Detection**
Discovers attacks that are invisible to standard security products.

**Total Visibility**
Unparalleled visibility into activity inside the data center.

**Total Scalability**
Scales to any traffic load inside the hypervisor or server and throughout the entire data center.

**Rapid Analysis and Response**
Attack analysis and detection of attacker's footprint provides complete and detailed insight into the breach details.

**Remediation**
Identifies the source of attack and attacker tools; Quarantine of infected files and machines.

**Lower Cost of Ownership**
Simplifies protection and management by reducing the time it takes to detect a breach and respond to it.

**Flexible Deployment Options**
Tight integration with Software Defined Data Center controllers and orchestration components, public clouds and bare-metal environments.

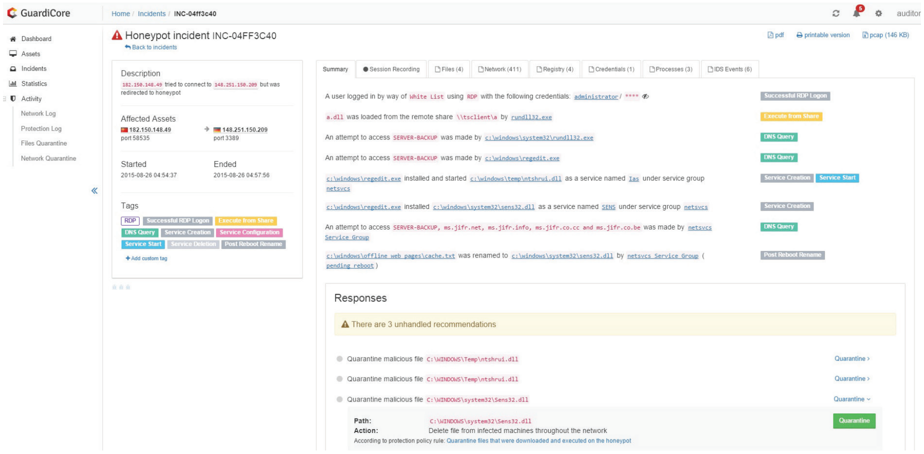
## Perimeter-Based Security Approach for Data Centers Has Proven Inadequate

Data centers are home to critical corporate data and business processes, making them a lucrative target for cyber attacks. Once inside a data center, intruders are very hard to detect and respond to. According to multiple researches, it typically takes many months to discover a breach, detect its source and remediate.

The GuardiCore Data Center Security Suite helps address this interior data center security challenge by providing visibility into data center activity, scaling cutting-edge security techniques to keep pace with east-west traffic rates. Using multiple detection methods, it exposes attackers, provides quick insights into the nature of the attack and responds to it in real time. Distributed per hypervisor or server, the Suite offers full coverage of all traffic inside data centers and scales to very large network sizes and traffic rates, with low impact on hypervisor/server performance.

## What GuardiCore Does

GuardiCore detects humans as well as APTs and bots at the stage of lateral movement. Gaining attack footprint, GuirdiCore provides the ability to search for the full spread of the breach and automate mitigation and remediation of infected servers. GuardiCore monitors all the connections inside the data center using multiple detection methods. Centralized management performs semantic analysis of suspicious activity and alerts on any deviation from authorized and expected behavior.



Honeypot incident INC-04FF3C40
Back to incidents

Description
182.150.148.49 tried to connect to 148.251.150.209 but was redirected to honeypot

Affected Assets
182.150.148.49 port 58535 → 148.251.150.209 port 3389

Started 2015-08-26 04:54:37
Ended 2015-08-26 04:57:56

Tags

A user logged in by way of White List using RDP with the following credentials: administrator / ****

a.dll was loaded from the remote share \\tsclient\a by rundll32.exe

An attempt to access SERVER-BACKUP was made by c:\windows\system32\rundll32.exe

An attempt to access SERVER-BACKUP was made by c:\windows\regedit.exe

c:\windows\regedit.exe installed and started c:\windows\temp\ntshrui.dll as a service named Ias under service group netsvcs

c:\windows\regedit.exe installed c:\windows\system32\sens32.dll as a service named SENS under service group netsvcs

An attempt to access SERVER-BACKUP, ms.jifr.net, ms.jifr.info, ms.jifr.co.cc and ms.jifr.co.be was made by netsvcs Service Group

c:\windows\offline web pages\cache.txt was renamed to c:\windows\system32\sens32.dll by netsvcs Service Group ( pending reboot )

Responses

There are 3 unhandled recommendations

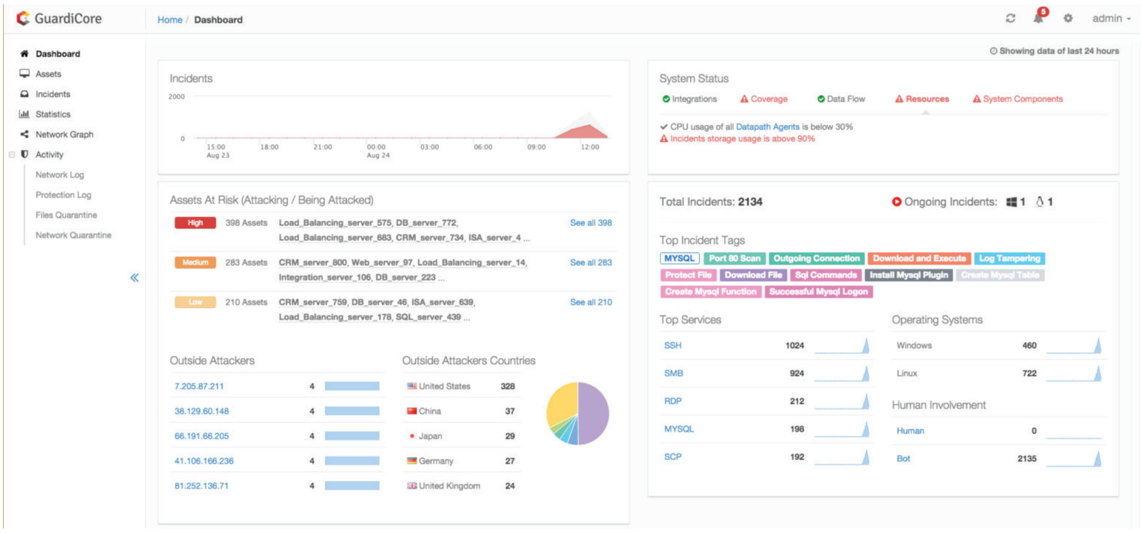
Quarantine malicious file C:\WINDOWS\Temp\ntshrui.dll

Quarantine malicious file C:\WINDOWS\Temp\ntshrui.dll

Quarantine malicious file C:\WINDOWS\system32\Sens32.dll

Path: C:\WINDOWS\system32\Sens32.dll
Action: Delete file from infected machines throughout the network
According to protection policy rule: Quarantine files that were downloaded and executed on the honeypot

Semantic Analysis of Attacks



Showing data of last 24 hours

✓ CPU usage of all Datapath Agents is below 30%

⚠ Incidents storage usage is above 90%

Assets At Risk (Attacking / Being Attacked)

| | | | |
|---|---|---|---|
| High | 398 Assets | Load_Balancing_server_575, DB_server_772, Load_Balancing_server_683, CRM_server_734, ISA_server_4 ... | See all 398 |
| Medium | 283 Assets | CRM_server_800, Web_server_97, Load_Balancing_server_14, Integration_server_106, DB_server_223 ... | See all 283 |
| Low | 210 Assets | CRM_server_759, DB_server_46, ISA_server_639, Load_Balancing_server_178, SQL_server_439 ... | See all 210 |

Outside Attackers

| | |
|---|---|
| 7.205.87.211 | 4 |
| 38.129.60.148 | 4 |
| 66.191.66.205 | 4 |
| 41.106.166.236 | 4 |
| 81.252.136.71 | 4 |

Outside Attackers Countries

| | |
|---|---|
| United States | 328 |
| China | 37 |
| Japan | 29 |
| Germany | 27 |
| United Kingdom | 24 |

Total Incidents: **2134**

Ongoing Incidents: 1 1

Top Incident Tags

MYSQL, Port 80 Scan, Outgoing Connection, Download and Execute, Log Tampering, Protect File, Download File, Sql Commands, Install Mysql Plugin, Create Mysql Table, Create Mysql Function, Successful Mysql Logon

Top Services

| | |
|---|---|
| SSH | 1024 |
| SMB | 924 |
| RDP | 212 |
| MYSQL | 198 |
| SCP | 192 |

Operating Systems

| | |
|---|---|
| Windows | 460 |
| Linux | 722 |

Human Involvement

| | |
|---|---|
| Human | 0 |
| Bot | 2135 |

The Security Suite Dashboard

## Designed to Protect the Software Defined Data Center

GuardiCore Data Center Security Suite for VMware NSX provides detection, analysis and real-time response to advanced persistent threats (APTs), insider threats and malware propagation inside data centers and clouds. Integrated with the hypervisor and the virtual switch, it leverages NSX programmability to inspect east-west traffic within the VMware-deployed data center. The Data Center Security Suite transparently enforces security at the hypervisor level and between virtual machines. The Suite identifies the attacker's footprint, automatically quarantines infected machines for remediation, and provides comprehensive visibility into virtual network traffic trends and threats.

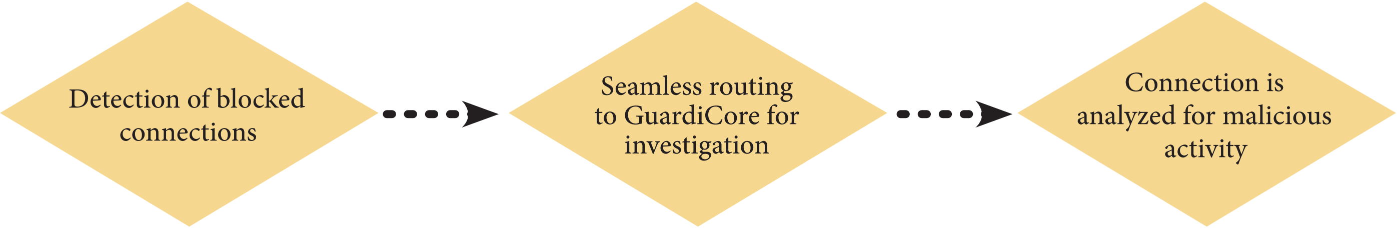
## How GuardiCore Data Center Security Suite Works

The GuardiCore Data Center Security Suite addresses the internal data center security challenges by detecting and examining connections and processes at the hypervisor level. The suite includes 3 main components:

1. A distributed light weight Secure Virtual Machine (SVM) is used for detection of suspicious activity, forwarding traffic of interest for analysis and remediation. The SVM uses multiple detection algorithms to identify suspicious activity and send relevant flows and process information to the analysis and inspection engine.
2. An analysis and inspection engine performs investigation of suspicious activity, determines if it is indeed malicious, understands its behavior and identifies the spread of the breach.
3. Centralized management component provides a single point of control for the system, UI for the administrator and integration with security management tools including SIEM and ticketing systems.

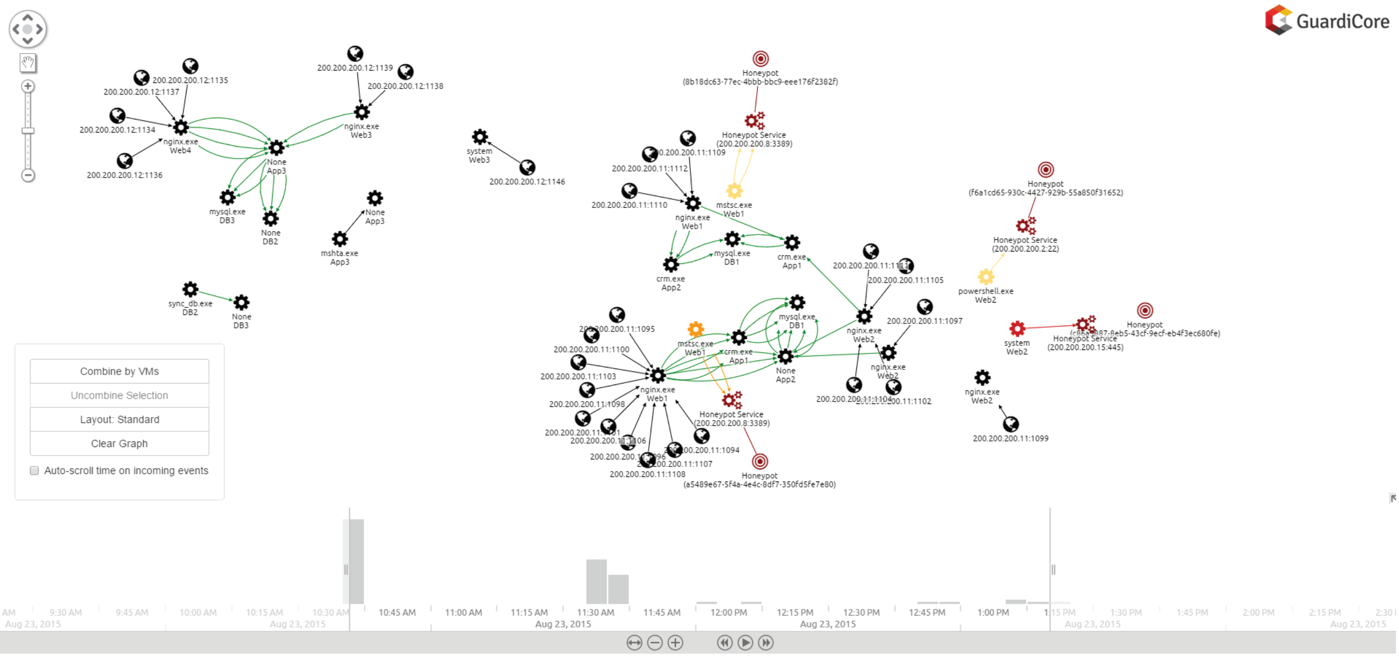
## Detection methods

One detection method tracks NSX or 3rd party firewall policy-violating connection attempts throughout the entire data center. Such connections might be a result of APT or bot’s lateral movement during the propagation phase. As such, any blocked attempt is considered a suspect attack that must be analyzed. GuardiCore Data Center Security Suite seamlessly keeps the connection alive, redirecting it to the analysis and inspection engine which provides the expected service in a highly monitored, instrumented environment. The analysis engine analyzes the suspect attack’s behavior and looks for signs of malicious actions such as exploitation, brute-force into management applications, password harvesting, manipulation of log files and upload of backdoors and attack tools. Any action by the attacker is recorded, and a detailed, actionable report is generated, containing deep forensic insights such as used credentials, exploits and uploaded tools.


Detection of blocked connections
Seamless routing to GuardiCore for investigation
Connection is analyzed for malicious activity

Using Blocked Connections for Activity Analysis

Another detection method is to examine the authorized processes that do not generate blocked connections. In other words, it does not violate any NSX micro segmentation policy. Using introspection into the hypervisor, GuardiCore is capable of monitoring the connection between any process, network flow and virtual machine and creating a baseline of approved activity. Any deviation from this baseline is considered a violation and the suspected process is automatically marked for further analysis. For example, in a real-world scenario, a web server process running on a specific VM is authorized by the NSX distributed firewall (DFW) to connect to the database process on a different VM. An attacker that is running a malicious process on the web server VM would be authorized to connect to the database VM. GuardiCore Data Center Security Suite would recognize the new process as malicious and alert the security administrator.



Identification of Malicious Activity Using Process Monitoring

## FEATURES

### Leveraging NSX capabilities

Using network programmability to scale east-west traffic inspection, introspection to collect rich context about every process and newly developed capabilities and integrated with NSX Orchestration API to provide fast and broad response.

### Micro-segmentation added functionality: block and investigate

Using built-in VMware NSX micro-segmentation, blocked connections are redirected and investigated.

### Breach detection and attack prevention

Deep analysis and forensics provide automatic detection of the attacker's tools, enabling search and remediation of the entire data center.

### Natural Language reporting with detailed forensics

Detailed information regarding the attacker's activity is provided in human-readable language alongside the most detailed technical analysis of the attack. Additional forensics evidence including IOC is provided.

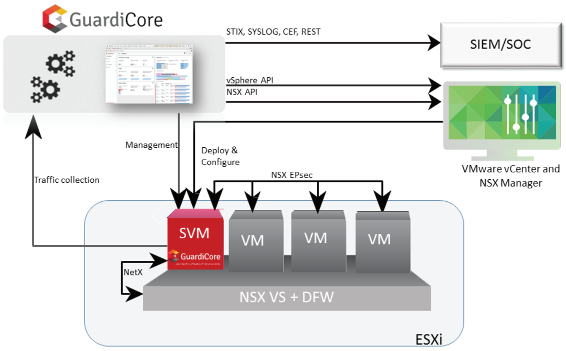
## GuardiCore Integration with VMware NSX

Integration with VMware NSX is performed using several VMware APIs for management, traffic inspection and introspection.
The deployment method uses a lightweight Linux SVM on each hypervisor which is automatically deployed on the hosts by NSX Manager after activation of GuardiCore service.
Using NSX-NetX API, GuardiCore identifies network connections that are violating security policies set by NSX Distributed Firewall (NSX-DFW). The connections are then redirected to GuardiCore analysis and inspection engine through dedicated VLAN/VxLAN/GRE interface, as desired by the user.

## Modes of Operations

The Data Center Security Suite has 3 main modes of operation:

1. Active Redirection mode: policy-violating traffic on protected hosts, on which an Inspect policy is enforced.
2. Passive Monitoring mode: policy-violating traffic on protected hosts, on which an Inspect policy is enforced and monitored by detection and response agents without performing active redirections to the analysis and inspection engine. Statistics regarding blocked connections are being collected and displayed in the User Interface. This mode allows measurement of expected frequency of redirection events before enabling the Active Redirection mode.
3. Disabled mode: Detection and Redirection agents are running, but are not inspecting or forwarding traffic to analysis.



NSX integration

## 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