SOLUTION BRIEF

Guardicore

Guardicore Centra™ and Check Point vSEC Strengthen Cloud Application and Workload Security

Together Guardicore and Check Point Software Technologies protect critical applications and workloads in public and private cloud infrastructures

Traditional perimeter protections designed to keep threats outside of the network are not optimized to secure IaaS environments. Today's threats target the enterprise's most lucrative assets, which are increasingly being migrated or deployed in public and private clouds. Once an attack gets past the perimeter, it propagates laterally and unless detected, it can move unimpeded. A new security model is required, one that can provide deep visibility and control of east-west traffic flows, actively detect and respond to ongoing threats and provide stronger security controls.

When deployed alongside Check Point vSEC, the Guardicore Centra™ Security Platform provides detection, analysis and real-time response to advanced persistent threats, insider threats and malware propagation. The joint solution provides process level visibility into applications and workloads, control of east-west traffic through micro-segmentation and real time breach detection and response. This allows security teams to discover, visualize, and respond to activity and threats inside the cloud infrastructure.

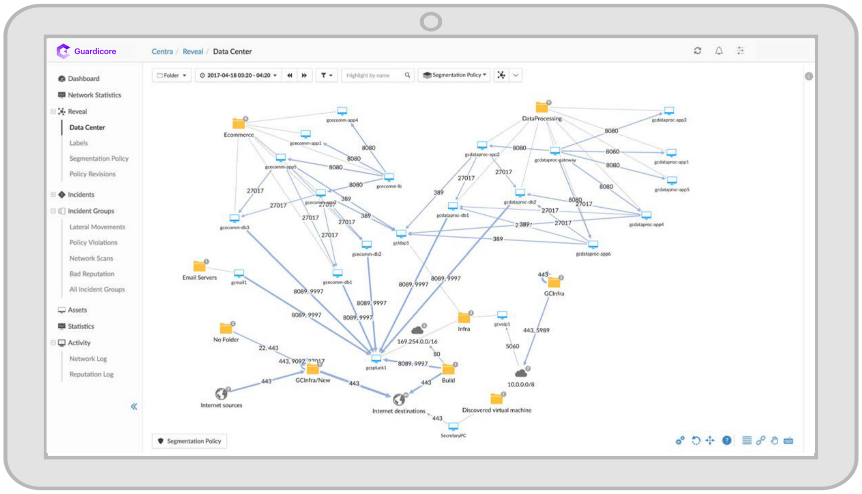
Solution Benefits

- **Context-Rich Network and Application-Layer Visibility Into East-West Traffic Flows**
  Security teams gain insights beyond standard source and destination information provided by service providers and internal gateways and can use those insights to harden application configurations, develop stronger security policies, and provide rich contextual information.
- **Detect and Respond to Breaches Faster and More Efficiently**
  Deploy multiple breach detection capabilities including dynamic deception, reputation analysis and segmentation policies for both internal and external facing subnets which deliver a complete picture of the attackers footprint and methods with IOCs automatically exported to the Check Point SmartDashboard for quarantine and remediation.
- **Develop Application-Aware Segmentation Policies**
  Simplifies the process of creating intra-subnet or intravirtual machine segmentation policies by incorporating application-layer flow data to help define granular security policies and then monitor those policies for variations and suspicious activity.

Context-Rich Network and Application-Layer Visibility Into East-West Traffic Flows

With network and process-level visibility into east-west traffic flows, security teams gain insights beyond standard source and destination information provided by service providers and gateways and can use those insights to harden application configurations, develop stronger security policies and provide rich contextual information for analyzing breaches.

Guardicore Reveal, a key component of the Guardicore Centra Security Platform, provides network and process-level visibility into applications and workloads combined with granular policy definition to discover, visualize, control and monitor activity inside the data center.
Once installed, Guardicore Reveal automatically generates a comprehensive visual map of all activity inside the cloud infrastructure, correlating process-level activity with network events, allowing administrators to get a quick and visual view of all workloads.



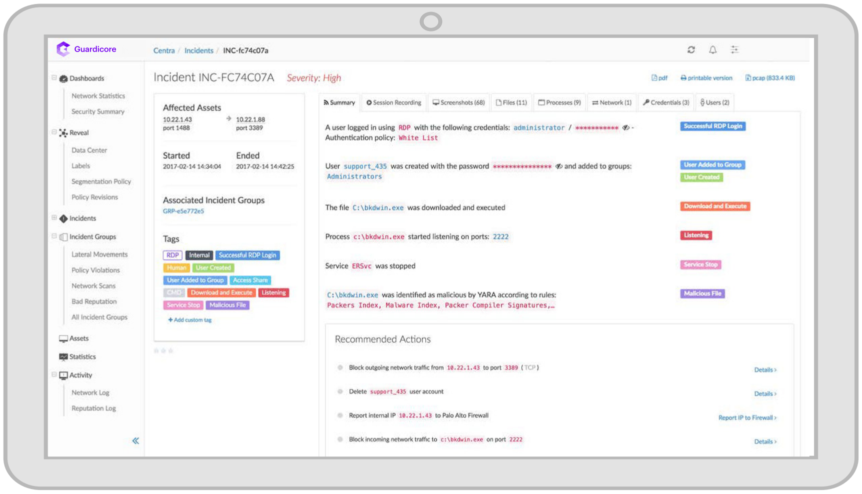
Guardicore Reveal provides a comprehensive visual map of all applications, workloads and communications.

Detect and Respond to Breaches Faster and More Efficiently

Security teams can deploy a combination of three distinct detection methods, centrally managed and distributed throughout the data center, to catch breaches more quickly—virtually in real time as they occur—which deliver a complete picture of an attacker's footprint and methods. These methods include:

- Patented dynamic deception, which employs real data center servers, IP addresses, operating systems and services as decoys that actively seek out suspicious activity at the first indication, engage with it and redirect it to a containment area for threat confirmation and investigation.
- Policy-based detection, which uses segmentation policies to implement network and application-level security controls around individual or groups of applications within the data center. Any policy violation, such as an unauthorized communication attempt, automatically triggers an alert to initiate an investigation.
- Reputation analysis, to identify negative processes and suspicious IP addresses, domain names or file hashes associated with threats.

The joint solution provides for the automatic export of indicators of compromise (IOC) for managed and unmanaged servers from Guardicore Centra to Check Point using the STIX (Structured Threat Information Expression) API. The IOC supplied by Guardicore are not generic but rather match threats detected within the Check Point vSEC environment. Armed with this information, security teams can identify attackers almost anywhere inside the public or private cloud infrastructure.



Incident INC-FC74C07A Severity: High

Affected Assets
10.22.1.43 port 1488 → 10.22.1.88 port 3389

Started 2017-02-14 14:34:04
Ended 2017-02-14 14:42:25

Associated Incident Groups
GRP-e5e772e5

Tags

A user logged in using RDP with the following credentials: administrator / *********** - Authentication policy: White List

User support_435 was created with the password *************** and added to groups: Administrators

The file C:\bkdwin.exe was downloaded and executed

Process c:\bkdwin.exe started listening on ports: 2222

Service ERSvc was stopped

C:\bkdwin.exe was identified as malicious by YARA according to rules: Packers Index, Malware Index, Packer Compiler Signatures,…

Recommended Actions

- Block outgoing network traffic from 10.22.1.43 to port 3389 (TCP)
- Delete support_435 user account
- Report internal IP 10.22.1.43 to Palo Alto Firewall
- Block incoming network traffic to c:\bkdwin.exe on port 2222

Guardicore Centra detects a lateral movement attempt between two internal servers, which is a strong indicator of a potential breach, and dynamically redirects suspicious traffic to the Guardicore deception environment for high-interaction engagement and analysis.

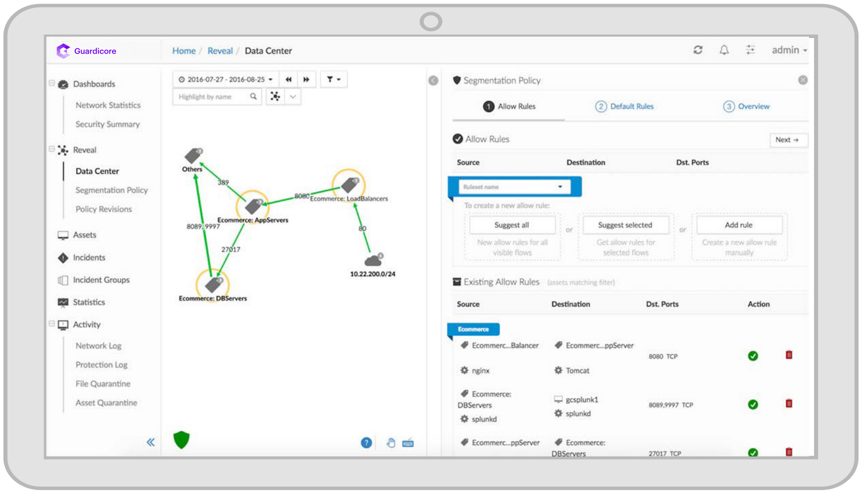
Develop Application-Aware Segmentation Policies

Guardicore Centra strengthens the process of creating intra-subnet or intra-virtual machine segmentation policies by incorporating application-layer flow data to define granular security policies and monitor those policies for variations and suspicious activity.

Using Reveal, a key component of the Guardicore Centra Security Platform, security teams can:

- Generate a comprehensive visual map of all applications and activity inside public and private clouds, allowing visibility into all workloads and a full understanding of application-layer communications.
- Filter and organize applications into groups and label them for the purpose of setting common security policies—for example, all applications related to a particular workflow or business function.
- Define and create rules governing authorized communications between applications.
- Test and refine those rules to ensure they are not disrupting normal, authorized traffic.

Any non-compliant traffic, unauthorized communication or other policy violation automatically triggers an alert indicating an intruder may be present. This in turn initiates the investigative process to confirm and contain the threat.



Source	Destination	Dst. Ports

Existing Allow Rules (assets matching filter)

Source	Destination	Dst. Ports	Action
Ecommerce			
Ecommerc...Balancer nginx	Ecommerc...ppServer Tomcat	8080 TCP	✓
Ecommerce: DBServers splunkd	gcsplunk1 splunkd	8089,9997 TCP	✓
Ecommerc...ppServer	Ecommerce: DBServers	27017 TCP	✓

Guardicore Reveal provides complete process-to-process visibility and segmentation policy management for public and private clouds, across multiple VMs and between assets (public or private).

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

Guardicore

v. 2.0