SOLUTION BRIEF

Guardicore

Multi-Method Breach Detection Spotlight: Using Segmentation Policies for Data Center Breach Detection

With data center breaches showing no signs of abating, it's time for security teams to focus more attention on the heart of the data center, where applications are talking to each other and performing mission-critical functions. As more and more organizations increasingly distribute data center assets across multiple, virtualized environments, perimeter defenses are no longer adequate. Security administrators need an efficient means of securing internal east-west traffic from attacks that have succeeded in breaching perimeter defenses.

Firewalling Hits a Wall

Firewalls have traditionally been used to secure communications in-and-out of data centers. However, placing firewalls at the core of the data center is problematic. Unable to adapt to massive amounts of east-west traffic, they can be a bottleneck to performance. Firewalling at the server level consumes large amounts of compute resources from the host, which is already highly taxed. It also requires deploying multiple solutions to span the many different types and brands of operating systems in the data center.

Until now, implementing security policies at the process level has been a challenge as well. That's because it requires visibility into all applications and processes running on the server. It further demands an understanding of how processes should function together within the application and the data center. Without those insights, process-level security policies can have negative results.

To protect data center assets while simultaneously improving breach detection and response, security teams need the means to:

- Visualize all the applications and processes running in their data centers
- Implement security policies at a granular level without impeding critical processes
- Detect unauthorized communications that may indicate a breach

Multiple Detection Methods Detect Breaches Faster

- **Dynamic Deception**
  A redirection architecture and dynamically generated live environments engages attackers and identifies their methods without disrupting data center performance
- **Policy-Based Detection**
  Security policies at the network and process levels enable instant recognition of unauthorized communications and non-compliant traffic.
- **Reputation Analysis**
  Detects suspicious domain names, IP addresses and file hashes within traffic flows providing comprehensive breach detection.

Corner Your Adversaries with Multiple Detection Methods

Policy-based detection is just one of several methods the Guardicore Centra Security Platform uses to improve real-time breach detection and response. Working in conjunction with each other, these complementary methods also include:

- 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.
- Reputation analysis, which leverages Guardicore's global network of threat sensors and intelligence feeds to identify negative processes and suspicious IP addresses, domain names or file hashes associated with threats.

Deploying these three methods simultaneously forms a strong security net, virtually ensuring that any live breach in the data center is caught, mitigated and contained for in-depth investigation.

Learn more about Guardicore's comprehensive data center breach detection capabilities at www.guardicore.com

Guardicore

Time for Defense to Go on Offense: Policy-Based Detection With Guardicore

Policy-based detection can help security teams more quickly detect, confirm and contain threats to prevent damage and minimize losses. These granular security controls do double duty, preventing an intruder from gaining malicious access to an application or process while simultaneously alerting administrators to the intruder's presence.

The segmentation policies capabilities within the Guardicore Centra™ Security Platform enable security administrators to:

- Generate a comprehensive visual map of all applications and activity inside the data center, 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.

Guardicore Centra detects a potential breach via a segmentation policy violation involving an unauthorized process attempting to communicate on an authorized port between two permitted hosts.

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