SOLUTION BRIEF

Guardicore

Multi-Method Breach Detection Spotlight: Fooling and Foiling Attackers With Dynamic Deception

In spite of the massive investment in intrusion prevention technologies, data center breaches continue to occur at an alarming rate. And once attackers have gained entry into the data center, they are extremely nimble at eluding detection. In fact, according to the Verizon 2016 Breach Detection and Investigation Report, "time to compromise" has accelerated rapidly over the past decade, while "time to discover" has gotten much slower. And this "detection deficit" is a chief contributor to the skyrocketing cost of breaches.

That is why the next frontier of data center security is internal east-west traffic— the heart of the operation, where mission-critical applications that govern the business interact with each other. And where malicious intruders that have successfully breached the perimeter can dwell indefinitely.

Conventional Detection Methods Fall Short

Traditional detection methods that feed alerts into a threat tracking system or SIEM often generate a large amount of "noise" and false positives. They sound the alarm too quickly and scare attackers away, losing the opportunity to fully learn about the attack method and origin. Alternatively, placing traditional security solutions in the heart of the data center runs the risk of disrupting data center performance, with potentially catastrophic consequences.

IT security teams need a detection solution that enables them to:

- Detect breaches either on or as close to the target asset as possible
- Avoid disrupting data center performance
- Confirm and investigate an entire breach through a single vantage point to accelerate incident response

Multiple Detection Methods Detect Breaches Faster

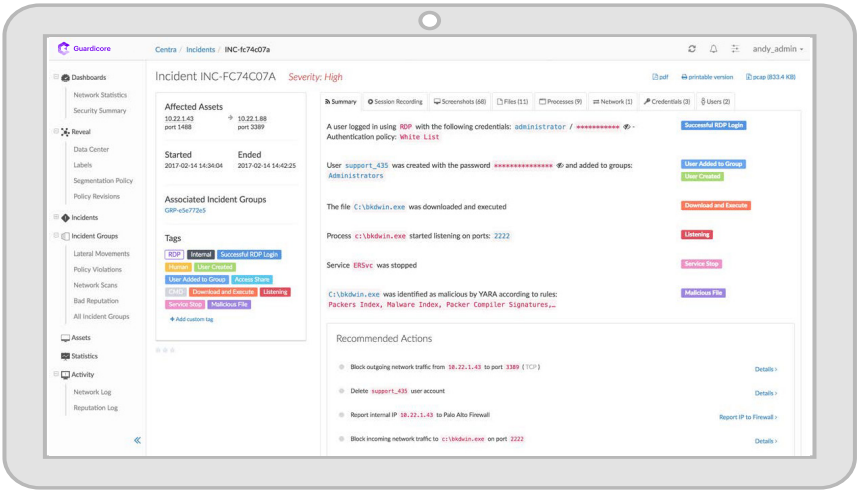
- **Dynamic Deception**
  A redirection architecture and dynamically generated live environments engages attackers and identifies their methods without disrupting data center performance.
- **Policy-Based Detection**
  Security policies at the network and process levels enable instant recognition of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

Time for Defense to Go on Offense: Dynamic Deception with Guardicore

Not all deception technologies are alike. Guardicore's patented high-interaction deception technology enables security teams to collect large amounts of data from suspicious actors—information that can be used to understand the attacker's methods, motives and even identity. High-interaction deception can also confirm genuine security incidents with higher fidelity and fewer false positives, which helps prioritize incidents and accelerate incident response.

Guardicore's dynamic deception component:

- Employs real servers, IP addresses, operating systems and services as decoys, instead of emulation
- Leverages lightweight agents designed to blend into the production environment with virtually no impact on data center processes
- Actively seeks out and engages with suspicious activity based on breach indicators such as blocked or filtered connection attempts
- Uses patented technology to reroute attacks out of the data center production environment, into a deception environment, thereby avoiding disruption
- Keeps the threat "alive" for in-depth analysis of the attack method and behavior



Guardicore Centra detects a lateral movement attempt, 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.

Guardicore

Corner Your Adversaries with Multiple Detection Methods

Dynamic deception 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:

- Policy-based detection, which uses segmentation policies to implement 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, 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**

About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security - for any application, in any IT environment.