SOLUTION BRIEF

Guardicore

Protect Critical Assets in the Financial Sector

Guardicore reduces the attack surface and streamlines compliance for financial applications in any environment

Financial institutions have long been the targets for cybercrime, but attackers continue to use more sophisticated tools and tactics in attempt to gain access to valuable financial assets and data. Cyberattacks cost financial services firms more than firms in any other industry, averaging 50% more than all others combined.

At the same time, the threat landscape for financial institutions continues to transform. The explosion of digital financial services combined with cloud computing initiatives and new application delivery models has expanded the attack surface that criminals can exploit. In response to these threats, financial institutions are increasingly adopting Zero Trust strategies and active defense measures to protect critical financial systems like SWIFT payments infrastructure, and cardholder data environments (CDE) to reduce the attack surface and meet data protection and other compliance requirements.

Micro-segmentation as a Foundation for Zero Trust

A Zero Trust architecture abolishes the idea of a trusted network inside a defined corporate perimeter. At the core of Zero Trust is the application of "microperimeters" of control around sensitive data assets. Financial institutions can reduce the attack surface of critical financial systems and prevent the exfiltration of sensitive data by applying micro-segmentation for fine-grained access control.

Guardicore protects financial institutions' core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our Centra Security Platform is a comprehensive data center and cloud security solution that delivers the simplest and most intuitive way to apply micro-segmentation controls to reduce the attack surface and detect and control breaches within east-west traffic. It provides deep visibility into application dependencies and flows and enforcement of network and individual process-level policies to isolate and segment critical applications and infrastructure. And it provides complete coverage of financial systems wherever they reside, protecting workloads that span on-premises, legacy systems, VMs, containers and deployments in public cloud IaaS including Amazon Web Services, Microsoft Azure and Google Cloud Platform.

Highlights

- **Total Visibility**
  Visually map application dependencies and flows across financial systems.
- **Reduce Risk to Critical Assets**
  Apply micro-segmentation policies to reduce the attack surface and limit exposure to crown jewel applications.
- **Meet Compliance Mandates**
  Quickly map and separate compliance-related systems and infrastructure such as SWIFT and PCI.
- **Reduce the Cost of Breaches**
  Detect active breaches earlier, preventing financial data exfiltration and reducing mitigation costs.
- **Simplify Security Management**
  Apply and enforce security policies consistently for any financial application.
- **Secure Anywhere**
  Secure applications wherever they run – public/private or hybrid environments, including legacy systems.

Reduce Risk and Achieve Compliance

Financial services organizations can leverage Guardicore visualization and micro-segmentation to comply with regulations like the Payment Card Industry Data Security Standard (PCI DSS) and ensure the protection of local SWIFT infrastructure and other financial systems. With Guardicore Centra you can:

- Map, secure and validate compliance of covered systems
- Isolate specific applications and their components from the rest of the network
- Restrict connections between untrusted networks and any system components
- Detect and prevent anomalous activity into and within trusted environments

Apply Security Consistently Across Heterogeneous Environments

Financial applications and networks often span multiple, heterogeneous systems and infrastructure. Guardicore Centra provides a single point of control to manage security policies across heterogeneous environments. With Guardicore Centra you can:

- Consistently enforce micro-segmentation policy for any workload in any environment
- Centralize security management for on-premises, legacy systems, VMs, containers and public cloud
- Automatically apply existing policies to new assets with no manual intervention
- Securely migrate workloads to new infrastructure without creating service disruptions and "orphan" assets and connections

Respond to Active Breaches and Security Events Faster

When the integrity of financial systems and data are at risk, time is of the essence. Guardicore compliments its visualization and micro-segmentation with breach detection and response capabilities that streamline incident investigation and reduce dwell time. With Guardicore Centra you can:

- Quickly identify unauthorized lateral movement inside data center networks
- Block suspicious connections without downtime for critical applications
- Reduce incident investigation time leveraging in-context, high-fidelity security incidents
- Identify threats based on suspicious domain names, IP addresses and file hashes associated with known malicious activity

Santander

"Guardicore enables us to enhance our overall data center security strategy and help our IT security team to avoid today's advanced threats."

- Marino Aguiar, CIO, Santander Brasil

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