AKAMAI CUSTOMER STORY

Large Financial Services Company Secures Remote Access with Akamai After Ransomware Attack

Comprehensive network visibility

Rapid time to policy

Secure remote workforce

The customer

A large financial services company based in Brazil.

The challenge

Increased remote access

Similar to many organizations, the COVID-19 pandemic led to increased remote access needs at this financial services provider, and much of the bank's IT staff transitioned to working from home on company-managed devices. As users began to access the data and applications they needed for their roles primarily off of the secure corporate network, the organization's attack surface rapidly grew.

Successful ransomware incident

Shortly after transitioning to a work-from-home model, a successful ransomware attack hit a critical Oracle Cloud database at the bank, which they would later discover originated from a VDI environment. Security and IT knew they needed to take swift action to limit the loss of sensitive financial data. Additionally, they understood if they could not determine and secure the original attack vector, there was a real risk of the ransomware spreading laterally to both the backup servers and the organization's production environment. If this happened, the bank was sure to be impacted by significant data and financial losses.

Selecting a solution

Akamai Guardicore Segmentation was already in wide use in other areas of the bank. Before the ransomware attack, the platform was responsible for managing and enforcing the segmentation policies of more than 23,000 servers with workloads spanning on-premises, virtual, bare-metal, and VDI infrastructure, as well as Azure and OpenShift container environments.

Large Financial Services Company

Industry
Financial Services

Solution
Akamai Guardicore Segmentation

Key impacts

- Mitigates spread of ransomware via lateral movement
- Provides granular visibility into network flows
- Protects remote access by segmenting VDI environments
- Enables fast incident response

Akamai

As a software-based segmentation solution, it had been used by the bank previously to realize several security and compliance initiatives, including managing administrator jump box access and Swift application segmentation. Knowing the platform's track record of providing excellent visibility and rapid time to policy, the response team quickly moved to leverage Akamai Guardicore Segmentation's features and tackle the breach.

Akamai Guardicore Segmentation benefits

Process-level visibility

Using the platform, the bank's response team investigated historical communication flows. They traced the ransomware's initial introduction to a database administrator's remote VDI connection communicating with an Oracle Cloud database.

Rapid time to policy

After identifying the attack vector, the team fast-tracked VDI segmentation, making it a top priority. The policy planning process began on a Saturday, using Akamai Guardicore Segmentation's visibility features to scope out potential policy needs. By the following Tuesday, the bank had enforceable policies in place for the more than 3,000 VDI connections to Oracle Cloud.

Ransomware recovery

The team deployed Akamai agents on the backup application and configured application ringfencing, defining — down to the process-level — what could communicate with the asset. It was then deployed in the breached area, blocking ransomware from propagating further, using global deny rules.

To reduce additional risk from remote worker access, policies were also set for the two VDI solutions used by call center employees, further preventing unauthorized lateral movement between endpoints at the bank.

Achieving segmentation policy enforcement in only three days allowed the financial services organization to drastically reduce the ransomware incident's impact and greatly improve remote access security moving forward.

Please visit akamai.com/guardicore for more information.

> The visibility provided by [Akamai Guardicore Segmentation] was like a bright beam of light that pushed back the darkness!
>
> Head of Infrastructure Security
> at Large Financial Services Company

 | Support | Published 06/23