AKAMAI CUSTOMER STORY

Breach Remediation Company Leverages Akamai in Ransomware Response and Recovery

Comprehensive network visibility

Segmentation across IT infrastructures

Response to ransomware threats

The customer

A U.S.-based breach remediation services company was engaged by a global equipment manufacturer after a major security incident.

The challenge

Fast-spreading ransomware

After a successful propagating malware attack that impacted business operations, the global manufacturer began working with the breach remediation services company to restore and improve security in its environment. The attack, initiated from an employee's laptop, had quickly spread and impacted most operating locations in addition to penetrating the organization's backup servers.

Selecting a solution

Initial containment methods, such as applying internet access restriction rules across firewalls, were slow to contain the rapidly worsening breach. The complexity of the environment and the reality of networking in a distributed enterprise made implementing and enforcing restriction rules with firewalls a slow and ineffective process.

Additionally, visibility into legacy machines was a significant issue for the incident responders responsible for investigating and containing the breach. Seeing the urgency and need to accelerate segmentation before the lateral spread impacted even more assets, the breach remediation service provider recommended Akamai Guardicore Segmentation.

Breach Remediation Company

Industry
Information Technology

Solution
Akamai Guardicore Segmentation

Key impacts

- Mitigates spread of ransomware via lateral movement
- Provides granular visibility into network flows
- Secures modern and legacy machines
- Enables fast incident response

Akamai

Akamai Guardicore Segmentation benefits

Instant visibility

Within three hours, the breach remediation services organization swiftly provisioned Akamai agents across more than 3,000 company servers. And just minutes after deployment, granular visibility into networking and communications flows began to emerge, giving the incident response team the context and accurate data they needed to investigate the breach and validate containment.

Fast time to policy

Shortly after achieving much-needed visibility, teams took action to segment critical assets from the broader environment. Two crucial production applications, responsible for the only functioning manufacturing line, were quickly identified and secured. Using Akamai Guardicore Segmentation, a policy was immediately introduced that restricted connections from infected subnets and parts of the data center to the applications — a task that would have taken weeks with legacy firewalls.

A simple query also revealed that legacy machines connected to the internet, bypassing legacy firewalls, attempted containment restrictions. After discovering noncompliant communication, the team created policies that effectively restricted internet access for all servers, including legacy machines, within minutes.

Preventing lateral movement during recovery

During the next part of the recovery process, the team recreated the manufacturer's application clusters, baking in Akamai agents. They configured an initial policy that blocked all incoming connections and used Akamai Guardicore Segmentation to identify dependencies. Then, communications were allowlisted on a need-to-have basis, only after validating the requirements and understanding the context. This approach allowed the team to recover and bring the applications impacted by the ransomware attack back online without the risk of reinfection.

Future protection

Akamai Guardicore Segmentation enabled the breach remediation services company to demonstrate significant added value for its customer, the manufacturer, while helping it recover from the ransomware attack. This opened up the opportunity for the services company to increase revenue, expand its footprint, and better help clients realize IT and security goals.

The internal data center segmentation introduced during the phased recovery significantly reduced the attack surface. Today, the organization's security posture has improved, and the impact of any future breach has been greatly reduced.

> [Akamai] allowed us within four hours to stop the attack from spreading and restore downed production lines in a 'sterile' network segment without modifying any underlying networking. All during ongoing IR investigation and containment.
>
> CISO at Breach Remediation Company

Please visit akamai.com/guardicore for more information.