Guardicore

CASE STUDY

Communications Infrastructure Provider
Stops Ransomware in its Tracks with Guardicore

This US communication infrastructure provider ensures businesses and residents stay connected in today's fast-paced world. It's responsible for an extensive network of cell towers and fiber networks that customers rely on in their daily lives.

The Challenges

Limited endpoint visibility and control

With over 6,000 laptops deployed across the organization, the IT security team had growing concerns over the fleet's risk to the broader IT environment. Additionally, ongoing issues with shadow IT activity by some of the company's power users needed to be addressed.

While some security measures had been put into place by the end user computing team, they were limited. None could granularly control system access for users or limit peer-to-peer communication to stop malware propagation effectively — the latter a significant concern at the organization.

To address these gaps, stakeholders wanted to improve the business's security posture by introducing a solution that would allow them to extend visibility and granular segmentation controls to employees' devices. This would also grant them the ability to observe and prevent unauthorized lateral movement.

Selecting a Solution

Security stakeholders had been considering the Guardicore Centra Platform for some time, interested in using it for multiple cybersecurity use cases. The organization decided on a phased approach to see great potential in the granular visibility and straightforward policy creation process.

Since Guardicore's software-defined segmentation policies aren't tied to the underlying infrastructure, the provider had the option to tackle any number of security initiatives. However, with the employee laptop fleet identified as high-risk, the team prioritized deploying Guardicore agents to its endpoints.

The Guardicore Centra Security Platform

Once the project began, the rollout of Guardicore's streamlined Windows agent to the organization's computers went quickly. This extended process-level visibility to user access and laptop activity.

INDUSTRY

Communications
Infrastructure Provider

HQ COUNTRY

USA

ENVIRONMENT

- Windows Fleet
- 6,000+ laptops

The IT security team was then able to create and manage security controls for these endpoints centrally, all based on accurate environment data. They then promptly set up several policies — including an alert around specific Microsoft Remote Desktop Protocol (RDP) activities, including failed login attempts.

Granular visibility in action

A short time after deployment, the policy configured to report unusual RDP-related activity delivered a flurry of alerts. It was quickly apparent a bad actor was attempting a brute force attack as failed login after failed login was observed.

The IT security team closely monitored the situation and, as attackers continued their assault, decided to make the call and block RDP on every endpoint with a Guardicore agent. In just a few clicks, they created and enforced a new segmentation policy that disabled RDP, stopping the attacker before a single endpoint was compromised.

Ransomware stopped in its tracks

During the post-mortem process, the security team quickly realized all indicators pointed to a major and well-known ransomware threat actor.

If the campaign had been successful, the attackers would likely have attempted to proceed with their usual tactics, encrypting anything in reach before issuing a ransom note. Due to the provider's organizational size and current trends, the bad actors' demands would have certainly exceeded $1 million. This would have come with significant added disruption and downtime if business-critical assets, such as the ERP system, had been compromised.

However, thanks to the fast-acting security team and Guardicore, there was no impact on the organization from the attempted attack.

Stopping shadow IT

In addition to stopping external threats, the team was also able to address internal challenges using the platform. Before Guardicore, the limited endpoint visibility made it easier for some users to circumvent official processes, executing activities on their own not compliant with the organization's official policies. The new insight and ability to enforce security controls on endpoints allowed IT security to curb shadow IT. This included preventing members of the DevOps organization from spinning up new resources on their own without going through official channels for authorization.

Expanding protection with Guardicore

For the communications infrastructure provider, protecting endpoints is only the beginning. Shortly, it plans to explore more new features and roll out Guardicore to its data center, secure its Citrix environment and apply third-party access controls for external vendors.

With the flexible nature of the platform, the team has the assurance that they can extend protection against advanced threats anywhere in the environment — no matter how their merger and acquisition strategy or digital transformation initiatives unfold in the future.

CHALLENGES

- Preventing Ransomware
- Stopping Shadow IT
- East-West Traffic Visibility

FEATURES USED

- Visibility
- Endpoint Segmentation

RESULTS

- Prevention of potential $1 million in losses
- Prevention of potential Shadow IT

Guardicore

About Guardicore
Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint.