CASESTUDY

STARLINK
TRUSTED SECURITY ADVISOR

StarLink streamlines the security framework of one of the largest media organizations in the region.

OVERVIEW integrated

One of the largest news organizations was in dire need of safeguarding its network. They were well aware of the problems that could cause breaches in their security and wanted to take stringent action to ensure their information was not compromised at any step of the time. Working with a leading partner, StarLink Security Consultants assessed the network, and provided an integrated solution to the organization by identifying and addressing their security challenges.

THE CHALLENGE

Detailed analysis of their existing network revealed the possible loopholes that could cause a breach in the network.

The customer had traditional firewalls which did not have the fine-grained intelligence to distinguish one kind of web traffic from another and enforce business policies. So it was either all or nothing. We further understood that

1. The firewall couldn't identify applications regardless of port, protocol, evasive technique, or SSL encryption. Neither could the firewall accurately identify users and subsequently use identity information as an attribute for policy control. Also, there was no integrated intrusion prevention capabilities.
2. Another problem was that their anti-virus softwares couldn't keep up with the malware authors that were continuously modifying their execution code. This resulted in waste of time ensuring the latest signatures across multiple endpoints were being maintained. Additionally keeping a blacklist of known malware signatures was a reactive approach and did not provide protection against zero day vulnerabilities.
3. There was no admin control over the application execution and installation.
4. The company did not have a platform to monitor and manage mobile devices and the applications installed on it, keeping malware at bay in private and public networks.
5. The company did not have a platform to monitor and analyze the internal network for the traffic between the virtual environments. And if a virtual machine was compromised by malicious code or security breach it would affect the other virtual machines on the same host.

THE SOLUTION

As a Value Added Distributor, StarLink analyzed each situation and advised solutions that could address all the problems and with their strong bandwidth of strategic channel partners helped implement these solutions.

As a solution to traditional firewalls that do not have the intelligence to filter web traffic, StarLink suggested a next generation firewall software which provided both standard first-generation firewall capabilities and application awareness, full stack visibility and granular control, ability to incorporate information from outside the firewall such as directory-based policy, blacklists and white lists. This firewall could also identify unknown malware, zero-day exploits and advanced persistent threats in a cloud based virtual execution environment.

We also included an upgrade path for future information feeds, security threats, and SSL decryption to enable identify undesirable encrypted applications.

To prevent, detect and respond to cyber threats that evade traditional security defenses, StarLink provided a leading cyber security solution that combined a trust based and policy driven approach to application control with real-time threat intelligence.

It also provided a unique solution that enabled SOC and IR teams to prepare for a breach through continuous endpoint recording, customized detection, live response, remediation and rapid attack recovery with threat banning.

To prevent any threats via mobile, a leading Mobile Threat prevention software was used. StarLink ensured threats were identified and stopped through a way that didn't rely on signatures, which are known to be powerless against today's constantly changing threats. This solution offered real-time visibility of threats on mobile devices, displays play-by-play analysis of suspicious apps, to provide and index of pre-analyzed apps, and generate threat assessments for custom apps. This dynamic analysis approach that was taken made mobile threat prevention resilient to obfuscation, code manipulation, evasion techniques and ensured it identified known and unknown threats that other defenses miss. Basically the solution provided real-time visibility into threats on mobile devices.

To monitor and analyze the internal network for the traffic between the virtual environments, a solution was implemented to tap into the virtual adaptors of these hosts. This helps in application performance monitoring and trouble-shooting or to find a compromised virtual machine and isolate it.

CONCLUSION

The security framework that StarLink designed and implemented through their channel partners helped fortify their organization's network.

The design included four products which comprised of next generation firewall that distinguishes one kind of web traffic from another, advanced threat protection system that enforces business policies, a threat management platform that provides granular visibility into mobile devices and applications installed on it and a method to tap into the traffic between a virtual machines to monitor and troubleshoot performance.

This enabled visibility, analysis and control, achieved comprehensive coverage, reduced complexity of the network and its administration which reduced operational costs and aligned their business with their IT.