CASESTUDY

STARLINK
TRUSTED SECURITY ADVISOR

StarLink fortifies the security network of one of the largest government organizations in KSA.

OVERVIEW

Being one of the largest government clients in KSA also increases the risks of security attacks. That is why it is important to continuously fortify the security network to avoid any breaches. It was then that the client looked to StarLink for support. Thus, StarLink and its leading channel partner assessed the situation and identified their security challenges.

THE CHALLENGE

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

1. Lack of security around the DNS infrastructure
2. Limited visibility on DHCP/DNS environment.
3. Lack of an automation from a network management perspective.
4. The email infrastructure wasn't secure as there wasn't any Anti-spam, Anti- malware, Anti-spyware, Anti-phisphing facilities to protect it.
5. There wasn't any protection from any advanced persistent threats coming through the web traffic and emails.
6. No mitigation or protection strategy from any kind of threat.
7. Although the organization was equipped to handle signature-based 'nuisance' malware with its traditional anti-virus solution, they were well-aware that they could not stop an advanced attack like those that hit other organizations. Fearing such an attack, the client wanted to take stringent steps to find a viable and effective solution.

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 protect the DNS infrastructure, StarLink implemented a DNS security to protect data and infrastructure internal and external to the enterprise. This helped defend against DNS, DDoS, stopped APTs and prevented data exfiltration via DNS, all without the need for end points agents as this combined enterprise grade DNS with automatic threat intelligence feed to provide protection and response against threats. It also enabled DNS to continue functioning even under attack and provided protection against new and evolving attacks automatically.

To tackle the problems of email security, StarLink implemented a solution which ensured dynamic content scanning, dynamic URL analysis as well as image scanning.

The sensitive data would be secured against external attacks and insider threats.

In addition, to secure the web, file and email security a Malware protection system was implemented which would allow the customer to gain visibility on all the aforementioned channels therefore being able to mitigate malware infection.

To equip the organization to safeguard itself from advanced malware attack, a solution was implemented which would continuously monitor and record all end points and server activity to prevent, detect and respond to cyber threats that could evade their traditional signature-based security defenses.

CONCLUSION

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

Now, they are well secured against targeted attacks on sensitive data and their critical network as well as from malware and zero day threats. Email security was upgraded and facilitated secure transmission and delivery of email through encryption. The implemented solution also gave real-time visibility into all activities, end points and servers enabling it to defend against DNS DDoS attacks or even the most advanced threats from infecting its systems. There was now integration of endpoint security and network security.