TEC
Communications

CASE STUDY - EMAIL SECURITY

THE BENEFIT / RESULTS

The Customer's Director of Infrastructure was extremely happy with the results, stating "with Cisco Email Security, we added features that allowed us to get more granular on how and when we quarantine email. We saw a decrease in unwanted spam messages right away, and have heightened confidence in the solution going forward."

With Cisco's superior Spam filter, Customer admins and users noticed little (if any) spam from the first day of implementation, leading to less risk and greater efficiency. Cisco's Email Security (CES) solution caught more spam, allowed for increased granularity, minimized false positives, and provided greater protection to users. Additionally, Cisco Advanced Malware Protection (AMP)'s 24/7 file monitoring identifies malware before it can damage networks. TEC achieved what it sent out to accomplish for the Customer: leverage IT to make its operations easier, faster, and safer with minimized inefficiency and downtime.

CUSTOMER PROFILE

Our Customer is a Cleveland-based 100+-employee company which has been a leader for over 75 years in the specialty clothing manufacturing industry.

THE SITUATIONAL ANALYSIS

The Customer's email system was outfitted with a spam filter with basic features. Over time, an increasing number of spam messages and phishing emails (designed to look legitimate and placed strategically to entice opening) broke through the filter. Not only were the messages affecting the efficiency of the Customer's business, but they also threatened to carry malicious links that could put the company in danger of a data breach.

THE NEED

With sensitive, proprietary business information circulating throughout the company on a daily basis, it was of critical importance to ensure that the Customer's data stayed within the organization and not accidentally exposed to those outside the company. Secondly, it was imperative to safeguard employees from an increasing number of malicious emails. Upon TEC's consultation with the Customer regarding its IT story, it became evident that they needed a solution that could accomplish both goals and continue to process legitimate emails reliably.

THE SOLUTION

As part of Cisco's Email Security (CES) solution, TEC implemented a bundle of features to protect against email threats, including: antispam, graymail detection, antivirus solution, outbreak filters, and forged email detection. Additionally, Advanced Malware Protection (AMP) was added to enhance malware detection and blocking capabilities with file reputation scoring and blocking, sandboxing, and file retrospection for continuous threat analysis.

THE OBJECTIVES / INTENDED OUTCOMES

TEC's topline goal was to provide the Customer with an email security solution that:

♦ Allows the filtering and blocking of suspicious or malicious content, links and attachments
♦ Analyzes messages for sensitive and proprietary material prior to leaving the organization
♦ Sets custom policies based on other criteria that protected the Customer's business

THE EXECUTION

To implement the solution, TEC:

♦ Created a Whitelist and Blacklist
♦ Customized content filters
♦ Built Outbreak filters
♦ Enabled End User Spam Quarantine
♦ Integrated Spam Quarantine with Active Directory (AD)
♦ Defined Virus and Outbreak policies
♦ Set up Hot Address Table
♦ Made DNS entry changes
♦ Verified Mailflow
♦ Conducted knowledge transfer

The biggest challenge involved integrating the End User Spam Quarantine with AD. While troubleshooting this integration, TEC did not see any requests from the Email Security Appliance hit the outside of the firewall. Additionally, after go-live, nearly every email was being sent to the users' Spam Quarantine — even test emails that were confirmed as 'clean.' After some modifications, the solution worked according to goal.

Want to learn more about TEC's Cybersecurity solutions, so YOUR business is sufficiently protected from a growing number of threats?
Go to www.tec4it.com/cyber-security, or we're just a phone call away at (440) 333-5903!

CISCO Partner
Premier Certified

CISCO
Advanced Collaboration Architecture Specialization