EVOTEK

Email Security Gateway Health Check

Build a strong email gateway to ensure you aren't a prime target for cyber attackers

An Email Security Gateway Health Check and Assessment aims to tune the organization's email gateway and ensure its ongoing efficacy, configuration, and alignment with current email-borne threats. The scope of this assessment serves to identify vulnerabilities, mitigate email-based threats, protect sensitive information, ensure regulatory compliance, safeguard the organization's reputation, and drive continuous improvement in email security. Email can be the easiest entry point for bad actors and outside threats, if not properly monitored.

Business Challenge

Email poses significant security challenges for organizations due to several reasons. Email is a widely used communication channel, making it a prime target for cyber attackers. Most organizations can believe that email security is a "set it and forget it tool". Phishing attacks, where attackers impersonate trusted entities to deceive users into revealing sensitive information, are extremely prevalent through emails with malicious attachments and links delivering malware, ransomware, or initiating unauthorized access attempts. If the business does not understand the supplemental tools and processes that offset email security such as staff training and education or URL/Web Filtering, they can leave themselves open to various attacks.

A Proven Solution

Strong email security has strategic importance for senior leadership as they benefit from reduced risks associated with email-based attacks, such as financial loss, reputational damage, and legal consequences. EVOTEK's approach is comprised of a proprietary control set that aims to capture not only the email gateway solution itself but also performs a detailed look at ancillary tools that support the organization's email security goals and objectives. It streamlines IT and Security teams' efforts in managing spam, implementing security controls, monitoring for anomalies, and responding to incidents promptly. Most importantly, a robust email security program instills confidence in stakeholders and demonstrates a commitment to cybersecurity best practices.

A Big Catch in Preventing Email Threats

EVOTEK was able to assess the current operational details of a client's email gateway and discovered several misconfigurations, including whitelisting all sending domains and misconfigured DNS settings. From their findings, EVOTEK was able to quickly propose tuning and configuration level changes to ensure seamless operation of the tool and reduce email threats by over 70% in the next quarter.

Data Center   Network   Security   Cloud   Communications