

EMAIL SECURITY-AS-A-SERVICE

"Stop email-based attacks in their tracks with Email Security-as-a-Service."

Email Security-as-a-Service (ESaaS) protects many email-based threats, such as spam, phishing, malware, and ransomware. It allows organizations to focus on their core business activities while ensuring that their email communications are secure and protected from cyber threats. ESaaS is important for all-sized businesses needing more resources or expertise to manage their email security infrastructure.

KEY FEATURES

- 85% organizations have encountered phishing emails at least once.
- 81% of malicious files are distributed by email.
- 1 in 239 email attachments are malicious!
- 1 in 415 Links in emails are malicious!

MANAGING EMAIL SOLUTION INHOUSE: A CHALLENGE ON MULTIPLE FACETS

Expertise

Implementation of Email security controls requires a high level of expertise. Small and medium-sized businesses may need more resources or expertise to manage their email security infrastructure, making detecting and preventing increasingly sophisticated email-based attacks difficult.

Time

Managing email security can be time-consuming, taking away resources that could be focused on other critical business activities. It is particularly true regarding monitoring and responding to email-based threats requiring constant 24x7 attention and analysis.

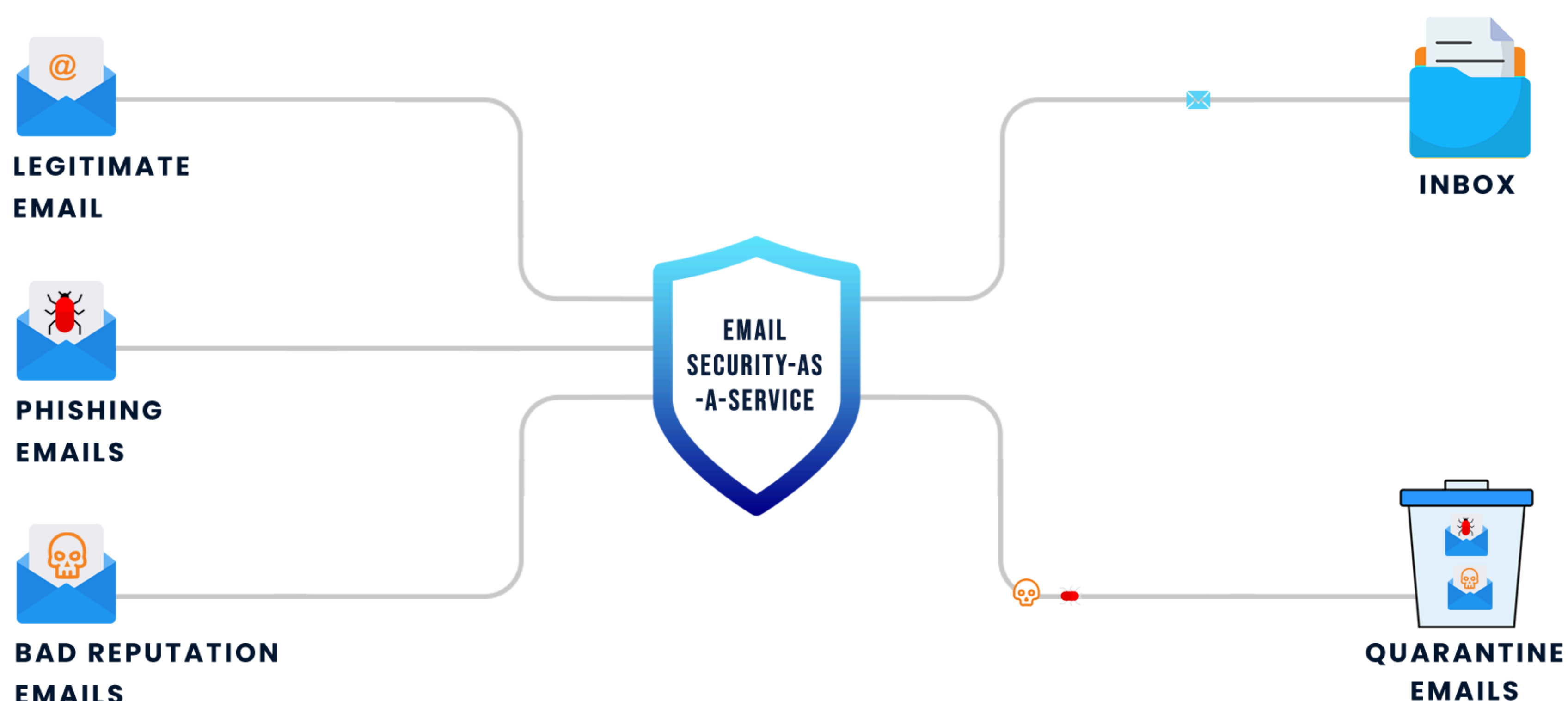
Evolving Threat Landscape

Email-based threats are constantly evolving and becoming more sophisticated, making it difficult for in-house teams to keep up with the latest attack techniques and prevention methods.

Cost

Building and maintaining an email security infrastructure can be expensive. It requires investing in solutions and ongoing upkeep and monitoring. The cost of hiring and training personnel to manage email security is also high.

HOW DOES EMAIL SECURITY-AS-A-SERVICE WORK?



EMAIL SECURITY-AS-A-SERVICE — BENEFITS

- A multi-layered and AI-powered email security framework to prohibit the unwanted email from reaching users' inbox.
- It covers complete email threat vectors; spoofing, anomalies, phishing, shadow IT, malware UBA & DLP.
- Recommendation to improve the security posture based on the analysis of corporate email traffic.
- It ensures adherence to local data privacy laws and provides the custom report for auditing.
- Weekly/monthly/quarterly SOC governance calls.
- 30-min GOLD SLA & Dedicated 1800-SOC number.

OUR SOLUTION PARTNERS



GreatHorn



TESSIAN



Symantec.
A Division of Broadcom



Microsoft



CONTACT US

CONTACT US NOW!