Trellix

Trellix Email and Collaboration Security

Trellix is pleased to collaborate with customer on upgrading their existing Microsoft Email Security and advancing their security maturity journey towards Trellix Email and Collaboration Security

The current and future state below explains customer's situation and reason to action

Current State

Advanced Email Threats Being Missed:
Executives being spear-phished multiple times in the last month alone as too many phishing campaigns are still getting through Microsoft Security. Too much sensitive data continues to leave the organization through email.

Third-Party Exposure: Digital transformation initiatives accelerated collaboration workflows with customers and partners, but also opened the door to new attack vectors, increasing risk exposure that's hard to determine.

Increased Velocity, Volume of File Sharing: Makes it difficult keeping up with consistent monitoring or cross-application file sharing, making manual submission infeasible and human error imminent.

Rising TCO: Due to increased security operation efforts to monitor, investigate, and remediate incidents across inbound email; chat and file sharing workflows on SaaS apps with external customers and partners. Increased operational efforts in integrating existing security tools with more file-sharing and collaboration tools requires extensive configuration, further increasing TCO.
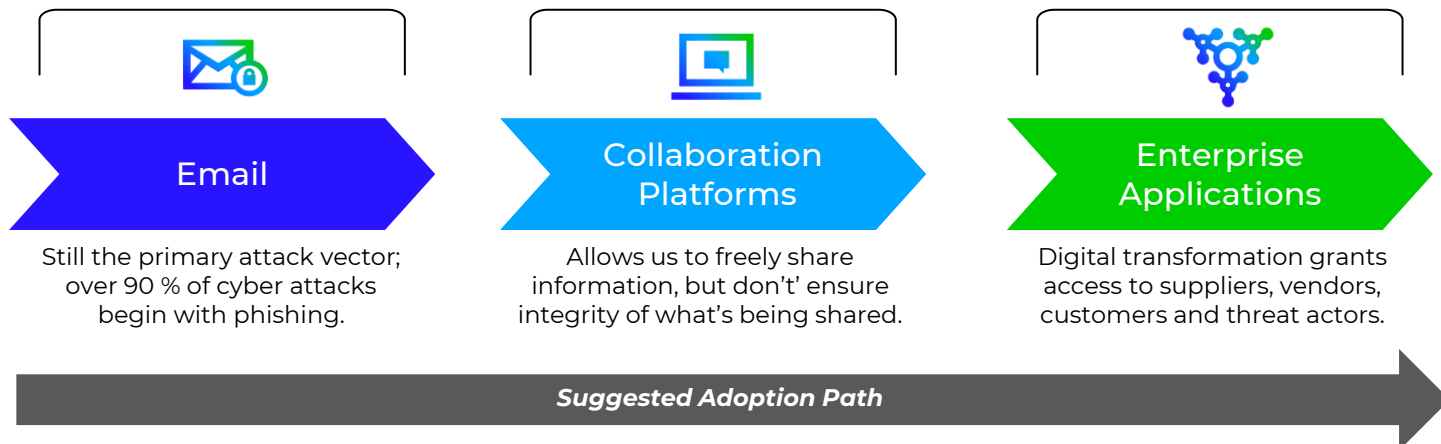
Future State

Defend Email Security With Confidence: Seamlessly protect Microsoft Exchange Online with proven, multi-layered threat protection to stop advanced threats before delivery. Block sensitive data from leaving the organization through email.

Collaborate Confidently: Pursue digital transformation securely with ongoing insight into partners' true security posture to reduce external party compromise risk while scanning content such as email, chat communications, and files from them for security threats.

Continuous, Real-Time Detection: Minimize malicious attacks and human error with unobtrusive file and URL inspection over various collaboration channels at scale, isolating malicious content upon entry..

Reduce Cost and Complexity: Use a single solution to secure the extended enterprise workflows. This accelerates TTV and reduces TCO with seamless out-of-box integrations covering Microsoft O365, Slack, Amazon S3, and more – with minimized end-user friction.

Trellix brings unparalleled, industry leading Email and Collaboration Security experience with a proven record of excellence to support customer's security maturity journey to the Email and Collaboration Security.

Email
Still the primary attack vector; over 90 % of cyber attacks begin with phishing.

Collaboration Platforms
Allows us to freely share information, but don't' ensure integrity of what's being shared.

Enterprise Applications
Digital transformation grants access to suppliers, vendors, customers and threat actors.

Suggested Adoption Path

Trellix IVX in Action

Furniture Retailer
Uses Trellix IVX to analyze files shared in their IT department's Slack collaborations

Large Multinational Bank
Uses Trellix IVX to analyze files in Box.com repositories

Top 5 US Fast-Food Company
Uses Trellix IVX to get a screenshot of suspicious URLs

Cloud Native Bank
Uses Trellix IVX to automatically scan loan application files before letting them through to their Salesforce platform

US Federal Agency
Uses Trellix IVX to detect malware in their file upload portal

Insurance Conglomerate
Uses Trellix IVX to analyze suspicious files from Endpoints

Why customer should move to the Trellix Email and collaboration Security offering now?

Email continues to be the #1 attack vector for launching attacks as over 90% of cyber attacks begin with spear-phishing

The average Microsoft E5 customer still sees up to 70 email campaigns get through every week. An attacker only needs 1

82% of companies experienced a breach as a result of digital transformation

55% of companies experienced at least one breach through a 3rd party

Only 32% of organizations have a comprehensive inventory of all 3rd parties with whom it shares sensitive information with