IT Complete
THE Kaseya PLATFORM

# Preventing Email-based Cyberattacks

Email-based cyberattacks are some of the most prolific and devastating cyberthreats organizations face today. Hackers use various social engineering lures in disguised emails to deceive organizations' employees, often with catastrophic consequences. According to a study, **65% of IT security practitioners cited email as their most significant data loss risk.** Ensuring that your security buildout includes these key technologies helps mitigate your risk for all types of cyberattacks.

## Artificial Intelligence (AI) □

AI-enabled email security solutions analyze incoming messages to quickly detect and eliminate threats without human intervention. AI allows a security solution to make judgement calls, reducing administration time and junk alerts.

## Automation □

Automated email security solutions can stop email-based cyberattacks and quarantine threats before they reach employees without a tech's support. This reduces the chance of an employee misjudgement and the need to hire more security personnel.

## Security Awareness Training □

Training is a powerful tool against email-based cyberattacks that use social engineering techniques, reducing the chance that an employee will make a mistake. Organizations that engage their employees in regular security awareness training experience **70% fewer security incidents.**

## Phishing Simulations □

Threat actors repeat their successful methods of attack. By simulating phishing threats, you can determine which employees are most likely to fall for a cybercriminal's lure and keep everyone on the lookout for phishing to mitigate the threat.

## Identity and Access Management (IAM) □

An IAM solution prevents unauthorized access to your systems and data. Even if a cybercriminal succeeds at phishing a password from an employee, IAM will prevent them from being able to use it to harm your organization. IAM also allows techs to isolate an account quickly if a user account is compromised.

## Multifactor Authentication (MFA) □

TMFA makes it extremely difficult for cybercriminals to access your systems by requiring users to prove their identity, something a cybercriminal with a freshly phished password likely can't do. 99% of cyberattacks can be prevented with MFA.

## Endpoint Detection and Response (EDR) □

TEDR detects, investigates and advises on threat activity in your endpoints, such as end-user workstations or servers. EDR solutions combine anonymized data and behavioral analysis to protect your organization against existing as well as emerging threats, like a malware infection from an employee clicking a bad link.

## Managed Security Operations Center (SOC) □

A SOC employs a team of experts who monitor your endpoints, network and cloud systems 24/7 and provide managed detection and response. That enables you to make all the right moves if a disaster strikes like an employee downloading a ransomware-laden email attachment. A managed SOC offers you the opportunity to reap the benefits of a SOC without adding any additional hardware or security staff.

Learn more, schedule a demo today!