Cisco Advanced Phishing Protection

Enhances protection against sophisticated identity deception threats to stay one step ahead of email attacks

Provides defense for on premise email deployments as well as cloud email platforms like Office 365 and GSuite

Cyber attackers are continuously finding new ways to infiltrate your network; spoofing, ransomware, phishing, zero-day attacks and Business Email Compromise (BEC) are just some examples of new ways attackers are using identity deception to breach organizations successfully. BEC's ability to trick unsuspecting employees by those impersonating your CEO or other executives has cost companies $5.3 billion globally according to the FBI[1]. Organizations increasingly need more layers of protection to defend users from fraudulent senders.

Cisco® Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advance machine learning techniques, real time behavior analytics, relationship modeling and telemetry to protect against identity deception-based threats. This intelligence continuously adapts to drive a real-time understanding of senders, prevent breaches and provide enhanced protection.

The Power of Machine Learning

Cisco Advanced Phishing Protection leverages three areas of machine learning modeling.

- Determines which identities the recipient perceives is sending the message
- Analyzes the expected sending behavior for anomalies relative to that identity
- Measures relationships to determine expected sending behavior; highly engaged relationships (such as between coworkers) have tighter behavioral anomaly thresholds since they have higher overall risk if spoofed

How it Works

Cisco Advanced Phishing Protection deploys as a lightweight sensor via the cloud or on-premise.

- Sensor receives all messages considered clean by the Secure Email Gateway
- Determine if the message is malicious
- Pre-configured policies immediately block or redirect the message for further incident investigation

Prevent

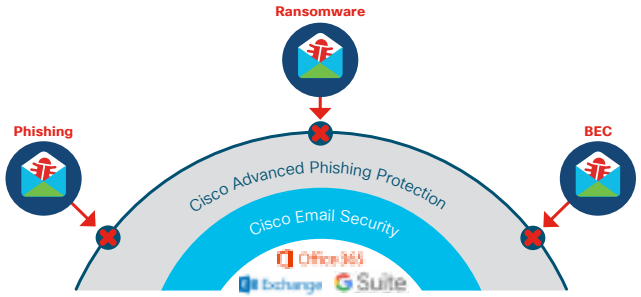
- BEC with no malicious payload or URL
- attacks that use compromised accounts and social engineering
- phishing
- ransomware
- zero-day attacks
- spoofing

Benefits

- Sensor-based solution can be rapidly deployed to ensure that your users are fully protected from damaging breaches
- Provides another layer of defense to more effectively secure your email environment
- Gain a real-time understanding of senders, learn and authenticate email identities and behavioral relationships to protect against BEC attacks
- Automatically remove malicious emails from users' inboxes and calls out identity-deception techniques to prevent wire fraud or other advanced attacks
- Get detailed visibility into email attack activity, including total messages secured and attacks prevented

Technology Highlights

- Uses predictive artificial intelligence to model trustworthy communications, based on 300+ million daily model updates
- Best-in-class BEC protection combines Rapid DMARC, advanced display name protection, and look-alike domain detection to stop attacks
- Partner Fraud Prevention models supply chain partners, auto-generating and continuously updating policies to prevent trusted partner fraud
- Account Takeover ID with enhanced machine learning models ATO threat behavior to block attacks originating from compromised email accounts
- Intelligent Content Inspection combines AI-based impersonation analysis, URL, and file analysis to detect malicious content that evades SEGs
- Email Forensics and enforcement provides customizable policies to enforce actions or report malicious activity to Security Operations teams via automated alerts or API integration



Included Onboarding Services

Kickoff and requirements gathering

On-Premise Sensors

- Provision On-Premise VMs for sensors (for On-Premise Sensor deployment model only)
- Install sensors into on-premise VMs

Hosted Sensors

- Install sensors into Supplier hosted environment

Configuration

- Configure policies and integrate with email gateway
- Verify policy configurations & mail flow
- Enable policy enforcement

Email Security Practitioner Services

Email Security Practitioner Services provides a strategic resource designed to accelerate solution adoptionand return on investment (ROI) for Cisco Domain Protection (CDP) customers.

For those without in-house expertise or resources, our experts understand your business, help you leverage CDP solutions to meet your business objectives, and offer the highest level of technical resource available.

Email Security Practitioner is a subscription-based 1-year service offering. Your Email Security Practitioner will work as your single point of contact with the project sponsor, project and business stakeholders, and key operational personnel within your organization to accelerate early phases of adoption and guide integration into daily operations.

The Service includes:

- **Days per Year:** up to 24 days (192 person-hours) of Supplier Personnel time
- **Onsite:** up to 25% on-site services
- **Travel:** included in price
- **Duration:** 12 months to use the services from date of purchase

1 Business Email Compromise, E-mail Account Compromise, The 5 Billion Dollar Scam, 2017