

Solution Brief

Advanced Threat Protection

Find and Stop Complex Attacks



Advanced threat protection (ATP) is a cybersecurity toolset for counteracting complicated malware, phishing, and hacking attacks. ATP is critical to maintaining security, brand reputation, customer trust and profit margins and is part of security protocols for early threat detection and prevention.

Social Engineering Schemes

Social engineering is a sophisticated attack vector in which hackers learn inside information about specific companies or its employees to manipulate them to gain access to their data systems or finances.

Oftentimes, individuals think they're helping a reliable source, but in actuality attackers are tricking them into giving up privileged information, like access credentials. Social engineering contributed to a [400% increase in complaints to the FBI](#) about cyber crimes in the latter part of 2020.

Malware and Ransomware

Malware is malicious software that enables hackers to gain access to individual computers or IT system components. Doing so enables them to monitor activity, view and manipulate data assets, encrypt files, or engage in any other nefarious behavior to compromise IT systems.

Ransomware attacks are a payload of malware intrusions in which files are encrypted and held ransom until organizations pay attackers to receive the keys to decrypt them. The average ransom demanded in 2020 was \$178,000.

The Challenge

Two-thirds of the world's small and mid-sized businesses say they are actively dealing with a cyber attack. The average security breach in the U.S. costs approximately \$4 million. With new types of attacks and with well-funded cyber criminals seemingly emerging daily, the job of identifying and defending against security intrusions is non-stop. If your organization is solely focused on defending against known infiltration attempts, you may wonder how you are expected to cope with the endless array of new zero day attacks.

Email Security Challenges

It is vital to understand the most prevalent forms of cyber attacks so that your organization can successfully avoid or mitigate them. The most common threats typically involve:

-  Social Engineering Schemes
-  Malware and Ransomware
-  Phishing




Phishing


Phishing involves sending fake or impersonated emails in an attempt to procure compromise sensitive information like login credentials to access a company's network or HR data. The requests in phishing emails often sound reasonable or urgent, which explains why many people fall for the same.


For example, [Covid-19 related](#) phishing attacks [increased 600 percent](#) in the first quarter of 2020, partly because attackers were able to exploit people's uncertainty and anxiety about the pandemic to add a sense of urgency to their scams. Social engineering attacks often enhances the efficacy of phishing attacks, for example around current or recurring events.

Features and Benefits


When properly implemented, advanced threat protection remediates or prevents phishing attacks, ransomware and malware attacks, and more. ATP cybersecurity creates dependable protection against known and zero day attacks by using a multifaceted approach to detection, protection, and response.


 **Democratized threat hunting** provides instant responses and updates from a community of security professionals across the world about the latest threat vectors, attacks, and responses.

 **Mailbox-Level BEC Protection** parses a company's entire email mailbox, analyzing all communications to create a baseline of what messages are deemed normal. This baseline is then used to determine whether or not future communication represents a [BEC threat](#).

 **Advanced URL and Malware Detection** uses computer vision and neural networks for identity profiling and scoring emails senders in real-time.

 **Auto Triage Incidents** uses machine learning and automation to assist in triaging threats.

 **Forensic Examinations** automatically orchestrate a comprehensive phishing forensic examination of any suspicious email using our proprietary deep content analysis in conjunction with multi-AV, visual similarity, and sandbox scans.

 **Rapid Remediation** automatically detects and remediates suspicious e-mails (and cluster of similar emails) in seconds, blocking them for good.



About IRONSCALES

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks are launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com   

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

