Email Security

Improve email security by detecting any email-borne threat before it reaches your internal company domain. Block email threats – including spam, phishing, business email compromise (BEC), malware, advanced persistent threats (APTs), and zero-days – before they reach end-users' Microsoft 365, Google Workspace, or any on-premise email server mailboxes. Leverage a next-gen cloud-based email security solution with the highest detection rates and lowest false positives, combining speed, scale, and agility, powered by Perception Point.

What does IronTree's Email Security solution offer?

Stops phishing and spoofing attempts Minimise email risks with powerful threat intelligence, signature-based detection, URL reputation checks, unique image recognition algorithms, and machine learning with DMARC, DKIM, and SPF record checks.

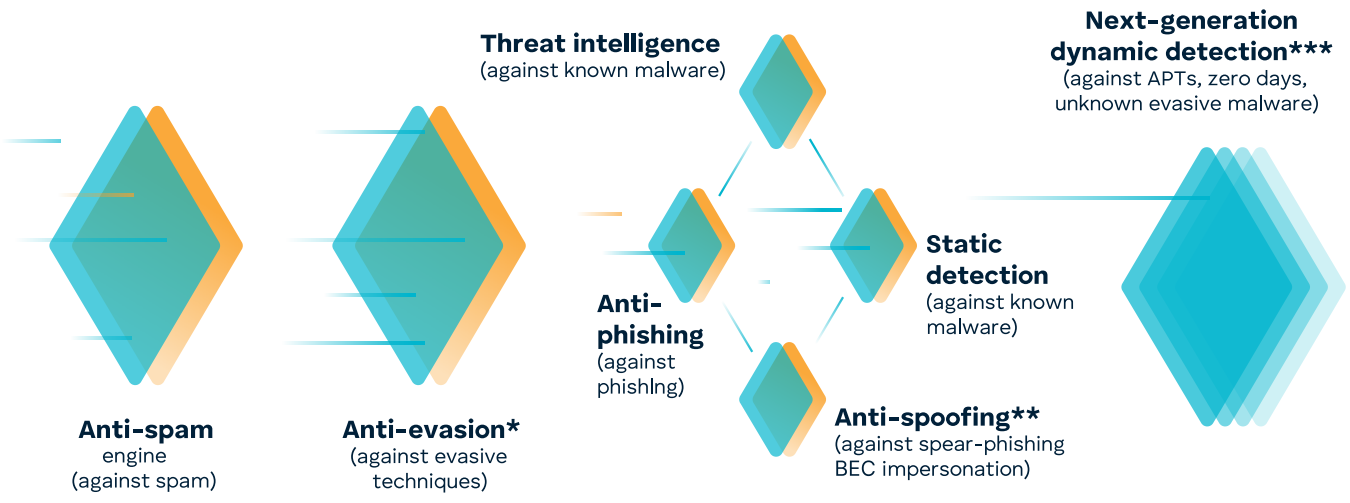
Catch advanced evasion techniques Detect hidden malicious content by recursively unpacking attached or embedded files and URLs, separately analysing each with dynamic and static detection engines – performing deep scanning of 100% of the content.

Prevent APT and zero-day attacks Prevent advanced threats that evade conventional defences with Perception Point's unique CPU-level technology, which blocks exploits before the malware is released and delivers a clear verdict in seconds.

Protect your riskiest communication channel with unmatched protection technologies

- **Spam filter:** Block malicious communications with anti-spam and reputation-based filters, leveraging the combined data of several market leading technologies.
- **Anti-evasion:** Detect malicious hidden content by recursively unpacking the content into smaller units (files and URLs) which are then dynamically checked by multiple engines in under 30 seconds – much faster than the 20+ minutes of legacy sandboxing solutions.
- **Threat intelligence:** Stay ahead of emerging threats with the combined threat intelligence of six market-leading sources and Perception Point's unique engine that scans URLs and files in the wild.
- **Static signature-based analysis:** Identify known threats with best of breed signature-based antivirus engines enhanced with a unique tool by Perception Point to identify highly complex signatures.
- **Anti-phishing engines:** Detect malicious URLs based on four leading URL reputation engines in combination with Perception Point's advanced image recognition technology to validate the legitimacy of URLs.
- **Anti-spoofing:** Prevent payload-less attacks such as spoofing, look-alike domains, and display name deception with unmatched precision through machine-learning algorithms with IP reputation, SPF, DKIM, and DMARC record checks.
- **Next-generation dynamic detection:** Stop advanced attacks such as APTs and zero-days with Perception Point's unique, CPU-level analysis that detects and blocks them at the exploit stage by identifying deviations from normal execution flow during runtime.
- **Incident response service:** Gain direct access to cyber analysts who act as an extension of your service delivery team. Monitor all customer traffic and analyse malicious intent with ongoing reporting and support, including handling false positives, remediating, and releasing when required.
- **Integrated solution:** Email Security is part of IronTree's Protect solution, which unifies cybersecurity, data protection and endpoint protection management in one integrated solution.

Seven layers of protection against modern email-borne threats



*Anti-evasion: Recursively unpacks embedded files and URLs into their individual components to identify hidden malicious content.

**Anti-spoofing: Catch any impersonation attempt or (BEC) with a machine learning-based technology that inspects all relevant data and meta-data (IP reputation, SPF, DKIM, and DMARC record checks, text, and meta-data analysis; scoring of senders; other algorithms) to detect spoofing attempts well before they reach the end-user.

***Next-generation dynamic detection: Unique CPU-level technology that acts earlier in the attack chain (at the exploit stage, prior to malware release) by analysing the execution flow during runtime, reading the assembly code to catch and stop advanced threats such as Advanced Persistent Threats (APTs) and zero-days.

Ready to protect your inbox?

Tell us what you're running and **we'll show you where the gaps are** – no jargon, no obligation.

TALK TO US →

CT: 1 Westlake Dr, Westlake, Cape Town, 7945 • **JHB:** Infinity Business Park, Cnr William Nicol Dr & Pieter Wenning Rd, Fourways

087 943 2278 sales@irontree.co.za www.irontree.co.za