

More than **94% of attacks** and malware are delivered through email, making end-users one of the biggest risks to your organisation. Protecting your end-users from email borne attacks provides the **biggest reduction of risk of any other solution**. Many organisations are still relying on the basic spam protection tools - which are simply not enough.

The solution works with **Microsoft 365, Google Workspace, and any other email service** (on-premise email server or cloud-hosted email server). It has **direct integration with Microsoft 365 and Google Workspace**, ensuring a fast and friendly deployment process.

## Advanced Email Security protects your organisation from:

- 🔒 Phishing attacks
- 🔒 Spam emails
- 🔒 Spoofing attacks
- 🔒 Malware
- 🔒 Business Email Compromise (BEC)



## Why you need it

- You can easily integrate the solution with your existing email platforms
- Protects your organisation from fraud, reputational damage, and ransomware
- Includes a dedicated Incident Response (IR) service
- Includes 24/7 support directly from the console

## How it works

- Scans every email before reaching your mailbox
- Scans URLs and attachments
- Scans emails for malware
- Built-in Threat Intelligence
- Next-generation detection of new threats

## The Protection Process

The Protection Process ensures exceptional protection against email threats. All emails are scanned through the following process:

### **Anti-Spam Protection:**

Determines if an email is spam, based on a number of characteristics. Spam emails are sent to the user but marked as spam and put in the user's junk/spam folder.

### **Anti-Evasion:**

Unpacks email components such as attachments and embedded URLs. These components are scanned by the rest of the security layers separately.

### **Threat Intelligence:**

Gathers threat intelligence from multiple commercial sources, as well as custom tools that gather data from the users and internal research.

### **Anti-Phishing Protection:**

Protects users from phishing attempts by scanning the following:

- Sender and recipient reputation
- Content of email such as URLs, images, logos
- Checks multiple filters

### **Anti-Spoofing Protection:**

Protects users from being impersonated. Prevents 'bad actors' from tricking internal users who might share sensitive information or send money to the 'bad actor'. It does this by scanning the following:

- Sender reputation
- Checks text and metadata of the email using Artificial Intelligence (AI)


### **Traditional Antivirus (AV) Scanning:**


Email attachments are scanned by multiple AV engines for malware and ransomware. This detects and blocks known malware from reaching the end-users mailbox.

### **Next-Generation Detection:**

Unique proprietary technology to detect 'new' zero-day threats. Designed for fast detection and analysis.

## Additional Microsoft 365 protection features

 **Account Takeover Protection (ATO):** Detects if a user's account is compromised. It does this by monitoring logins, email rules, and number of emails sent from the account.

 **Outbound Email Scanning:** Protects your organisation from reputational damage caused by compromised email accounts.

**Add-ons for OneDrive, Teams, and SharePoint protection against malware and malicious URLs.**

For more information, contact [sales@irontree.co.za](mailto:sales@irontree.co.za) or [www.irontree.co.za](http://www.irontree.co.za)