

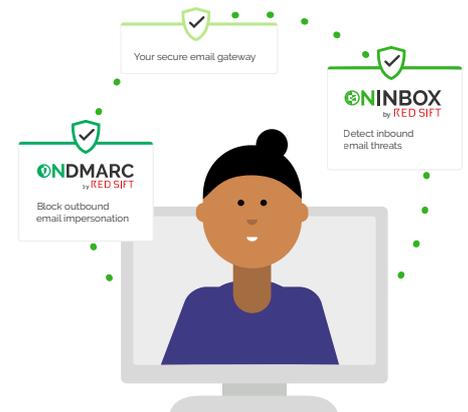


360° Email Protection by Red Sift

What's the problem?

86% of enterprises worldwide now use cloud-based tools.¹ At the same time, Business Email Compromise (BEC) accounts for over 50% of all cybercrime losses² of which the majority are email-based phishing and social engineering attacks. This is because of the gaps in your email security.

Organizations must adapt a layered approach with solutions like 360° Email Protection that integrate with cloud-based email infrastructure and work with secure email gateways to provide a full circle of business email protection around your organization, your employees, and beyond your network perimeter to your customers.



Highlights

- **No need to replace your email gateway**
360° email protection is complementary to SEGs by addressing email threats that slip through the cracks or never cross your network boundary.
- **A security analyst inside every inbox**
OnINBOX assists email users, that's anyone using email across your organization, with visual risk indicators upfront and center inside every email when it's opened.
- **Take back control of your domain**
OnDMARC is outbound email security that protects your reputation by protecting your domain. Block unauthorized sources from using your email domain.

The gaps in your email security

Traditional rule-based email security relies on people always playing catch up in a modern threat landscape where threats are constantly evolving and new rules need to be set. Without an automated and adaptive service like 360° email protection, your organization has gaps that create an opportunity for cybercriminals:

- 1) Secure email gateways can't keep up** With the speed of evolving threats today and social engineering techniques commonly found in BEC attacks, email threats lack obvious threat signals such as malicious URLs and blacklisted IPs which means they slip through your email gateway undetected.
- 2) You can't teach users to spot every attack** Phishing training is a good start towards people-centric email security but there is no indicator of trust inside the email post-delivery which means organizational security relies on the guesswork and vigilance of every single employee when they open an email.
- 3) No control beyond your network boundary** Without DMARC configured, cybercriminals can spoof your domain which looks like the email is sent from your email address. This type of attack has the highest chance of success and the consequences have both financial and reputational risks to your organization and your customers.

It takes a number of layered solutions to fill the gaps in traditional rule-based email security.

Why is Red Sift 360° email protection the solution?

The 360° email protection suite is complementary to your Secure Email Gateway and automatically safeguards your organization against domain fraud targeting your customers, partners and suppliers whilst defending against advanced inbound threats like business email compromise (BEC), spear phishing, and other targeted impersonation attacks.

The necessary modern security layers of 360° email protection are:



A preventative foundation

Traditional email gateways sit between the internet and your inbox scanning attachments and filtering email threats when they cross your network boundary.



With proactive defense

OnDMARC lets you actively block phishing attempts and secure your domain against email impersonation. This is via the speedy and correct implementation of DMARC.



Empowering people's decisions

OnINBOX's intelligent inbound email threat detection uses automated visual risk indicators inside every email for personalized endpoint protection and company-wide insight.

Get in touch today to find out about how you can use the full circle of Red Sift's 360° email protection to close the net on the phishing problem.



¹ Verdict (2020), Cloud adoption trends: Infrastructure, apps and security

² FBI (2019), Internet Crime Report

RED SIFT

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. By harnessing the power of AI we can securely collate, compute & visualize data from thousands of individual signals to help organizations to optimize their cybersecurity.

Products on the platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence.

 www.redsift.com

 contact@redsift.com

 [@redsift](https://twitter.com/redsift)