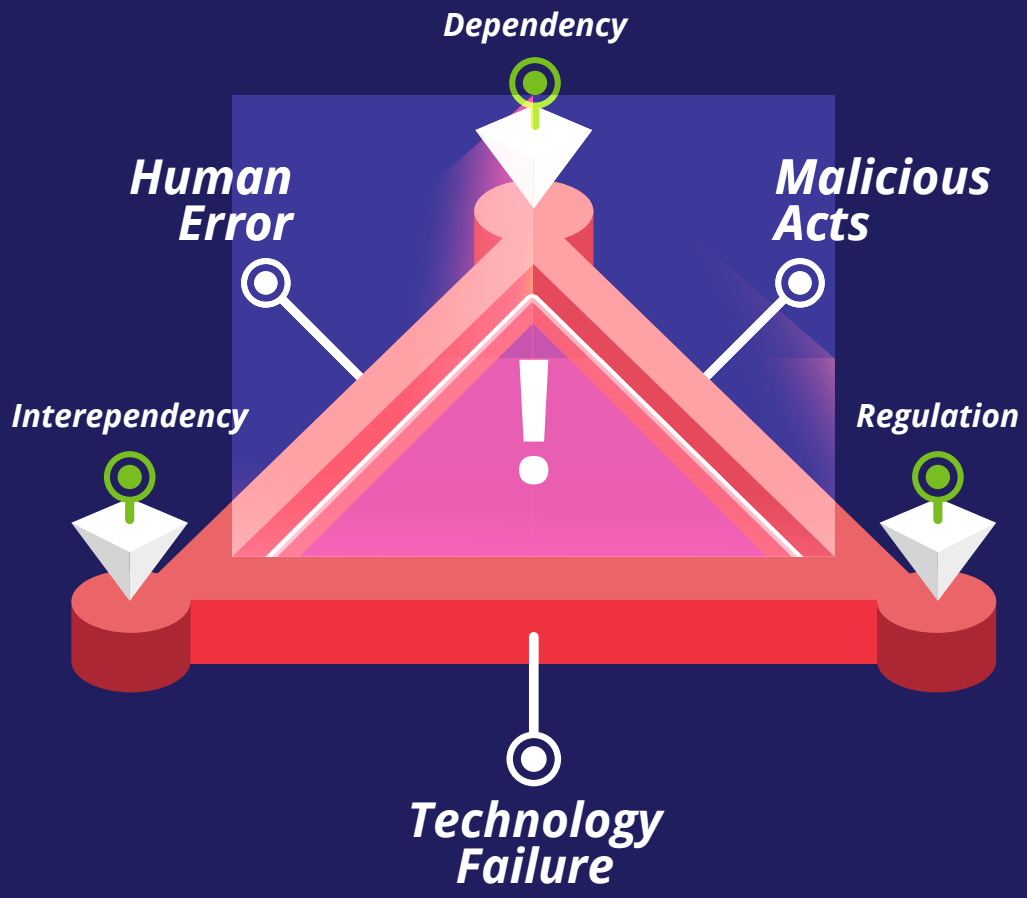
Email Security 3.0

A comprehensive email security strategy

The Role of Disruption

Business leaders are worried about and actively planning for disruption. Even with the most sophisticated protections in place, it's impossible to fully predict where disruption will originate. Technology is not infallible, people make mistakes, and bad actors will never stop looking for a way in.

The associated risks grow exponentially in the context of the digital world. An irreversible dependence on technology and deeply connected supply chains add up to the potential for a true disruption domino effect, while growing regulatory requirements layer on even more complexity.



Disrupting Disruption

Nearly all cyber-attacks leverage email. Why? Email is always on, it's trusted, it carries links and attachments, and it can easily be impersonated.

Protecting this channel used to mean protecting the perimeter, but the days when that was enough are long gone. Companies now need to move from a perimeter-based security approach to a pervasive one, with protection...

At Your Perimeter

- Sophisticated, targeted attacks
- Data leak prevention

Inside Your Network & Organization

- Internal email threats
- Human error

Beyond Your Perimeter

- Abuse of owned domains
- Brand imitation and lookalike domains

At Your Perimeter

Zone 1

Attackers send SPAM and viruses in emails and embed URLs in them to conduct phishing and spear phishing attacks. They also deliver forms of malware that organizations can't detect with signatures and classic antivirus technologies.

Although the traditional concept of a "perimeter" has evolved, the simple fact remains that securing email is the one of the most important steps organizations can take to reduce risk and keep disruption at bay.

Real-world scenario

Sam's company had recently migrated to Office 365, so he wasn't surprised to see an email asking him to update his user name and password. He took care of it right away. A couple of weeks later, he received an email saying his files had been encrypted and demanding a payment of $50,000 to unlock them. He had been phished and sent to a fake website, where attackers harvested his credentials. Because Sam worked in finance and had access to sensitive data, his company paid up.

Technology from Mimecast could have prevented this attack by scanning every click in real-time and rewriting all URLs in inbound email.

Zone 1 - Challenges
Phishing and Spear Phishing
Impersonation
Malicious URLs and Attachments
Accidental or Malicious Data Leaks
Business Email Compromise

Inside Your Network & Organization

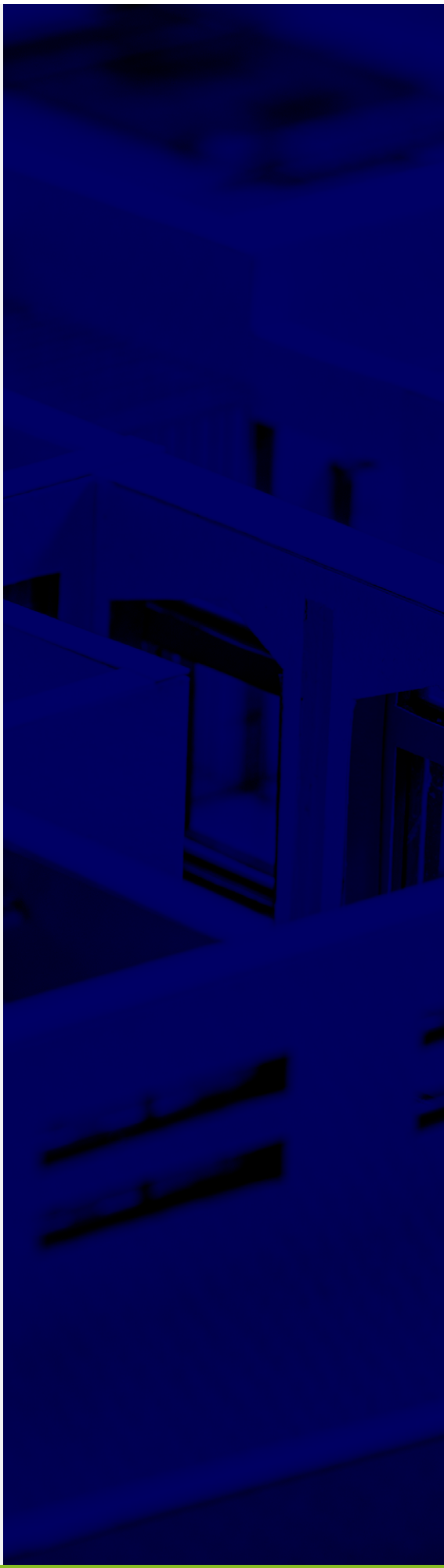
Zone 2

Even with a robust email security perimeter in place, attackers can bypass defenses and operate inside an email network, using compromised accounts or social engineering to send bad things inside and out. Employees are also susceptible to opening attachments, clicking on links, and falling for scams. Unsurprisingly, human error is a factor in the overwhelming majority of successful attacks.

Real-world scenario

A friend of Maria's sent his resume to her personal email address. Wanting to help out, Maria downloaded it via Dropbox, saved it to her work computer, and forwarded it to HR. When her colleague opened the file, it deployed malicious code, which infiltrated the organization's network. Before IT could resolve the problem, emails and files from several members of the executive team had been deleted. With no archiving system in place, the information couldn't be recovered.

Zone 2 - Challenges
Attacks Spread from User to User
Attacks Spread from Employees to Customers and Partners
Employee Mistakes/ Lack of Awareness
Permanent Data Loss



Beyond Your Perimeter

Zone 3

Without confronting an organization's email security perimeter, it's quite easy for attackers to impersonate a brand on the internet. Even unsophisticated attackers can register a similar brand domain or host a website designed to trick customers, partners, and employees, destroying the value and trust that brand owners may have taken years or decades to build.

Real-world scenario

A university in Australia was attacked by a malicious third-party who cloned their website, sent phishing emails to students, and began harvesting their credentials. The attack was first detected not by the University but by cybersecurity partner Mimecast, which can continuously scan the web looking for just these types of scenarios. After notifying the university, Mimecast took the fake website down in less than an hour. And three days later when yet another fake website appeared, Mimecast saw it and shut it down before any more students could fall victim to the scam.

Zone 3 - Challenges
Illegitimate Emails Sent from Your Domains
Brand Imitation
Fake Websites
Lookalike Domains
Highly Sophisticated, Integrated Phishing Attacks

Across the Security Estate

Complex security challenges often lead to complex security ecosystems – a reality reflected by the fact that organizations are using numerous disparate technologies to address their security needs. The ability to make everything work together has never been more important.

Email attack surfaces are a rich source of telemetry and threat intelligence. The ability to capture and incorporate that information into the larger security ecosystem makes IT teams and their overall security systems smarter.

Real-world scenario

A large restaurant chain was regularly targeted with phishing emails that required investigation and action by its IT team, a process that took from one to three hours for each email. Amount of time spent addressing this one problem alone? Roughly 6500 man-hours a year. There had to be a better way, and integration of its email security solution (Mimecast) with its SOAR provider (Demisto) turned out to be the answer. By integrating Mimecast's message search, URL decode, and block sender capabilities into Demisto, the company was able to reduce the time required to investigate and remediate phishing emails from 6500 hours a year to just 270.

Key Challenges
Complex Security Ecosystems
Disparate Platforms and Technologies
Limited Visibility Across Systems
Optimization of Existing Investments
Lean IT Teams

Why Mimecast, Why Now?

Mimecast is addressing the email security challenges of today at industry scale with Email Security 3.0. Our technology is built with an intentional and scalable design that helps customers achieve greater security while also reducing cost and complexity, bringing together numerous essential but disparate technologies into a single, easy-to-use platform.

Stronger Together

At the end of the day – when the talk of technology, threats, and risk has run its course – one simple truth stands out: we are all in this together. Every organization, big or small, plays a role in the digitally interconnected national and global ecosystems in which we live and work today. As such, we have a collective responsibility to work together to disrupt disruption and prevent bad things from happening to good organizations. Doing so contributes to the greater goal of building a global community of governments, businesses, organizations, and people that can stand strong in the face of whatever lies ahead.

Missing Partner Image