proofpoint.

How secure is your email really?

A comparison of Cisco and Proofpoint core security

Email remains one of the biggest security threats in any organization

Use Proofpoint to enhance your email security to reduce risk and save money

Email remains the primary way businesses communicate and collaborate with employees, customers, and partners. Nearly 400 billion emailsare sent and received every day, and the average business user receives more than 120 emails daily. Unfortunately, this also creates a massive and constantly accessible attack surface and an ideal target for cybercriminals.

Email is still the primary gateway into organizations for cybercriminals, and the scale, sophistication, and financial impact of attacks are all increasing simultaneously. Attackers are leveraging automation, artificial intelligence, and social engineering to craft highly targeted messages designed to bypass technical controls and exploit human trust. These advances have provided threat actors one of the most dangerous and effective attack vectorsin cybersecurity.

Every organization that sends and receives email carries risk, and that risk can never be reduced to zero. However, many organizations take their email security posture for granted until it's too late. When something inevitably goes wrong, leadership will ask difficult questions:

Did we understand the risks in our email environment?

Did we implement appropriate controls to reduce them?

And did we clearly communicate those risks to the business so informed decisions could be made?

Effective email security is not just a technology problem — it is a business risk management challenge that requires visibility, accountability, and informed decision-making across the organization.

127
emails per day
is the average business users receive, creating an enormous threat surface for cybercriminals.[1]

1. The Radicati Group, *Email Statistics Report.*

How much risk is your email costing you?

Using Proofpoint to protect your environment can help you reduce risk and save money

Legacy solutions cannot keep up with the speed, diversity, and creativity of modern threat actors. Traditional secure email gateways rely heavily on signature-based detection, static rules, and reputation checks to identify spam, malware, and known malicious domains. While these technologies remain effective against commodity threats, they were not designed to detect the highly targeted and rapidly evolving attacks that organizations face today.

Modern threats such as AI-driven phishing, credential harvesting, and business email compromise (BEC) are far more convincing than the poorly written phishing attempts of the past. This means more threats getting through your existing firewall and significantly higher exposure to the business.

Businesses that continue to rely on basic email security face a form of double jeopardy: outdated tools fail to detect modern threats, and each missed attack can trigger costly downstream consequences. Security teams must then respond with manual investigations, incident response activities, regulatory reporting, and potential financial losses.

As threats grow more targeted and sophisticated, stopping 99% of attacks is no longer sufficient. The remaining 1% often represents the most carefully crafted and damaging incidents — those designed specifically to evade existing controls.

BUSINESS EMAIL COMPROMISE (BEC)

MALWARE

PHISHING ATTACKS

TELEPHONE ORIENTED ATTACK DELIVERY (TOAD)

A focused cybersecurity platform specializing in advanced email security, threat protection, compliance, archiving, and risk management is necessary to combat the advanced threats of today.

A modern email security program can reduce both operational and incident costs

Compare the reduced risk of Proofpoint Core Email Protection against Cisco

Proofpoint Core Email Protection provides the advanced threat detection required to combat the evolving tactics bad agents are using to compromise your environments. While Cisco provides some protection against cyberattacks, Proofpoint demonstrates superior protection against email-based attacks.

The following case study provides examples on how Proofpoint reduces exposure and therefore reduces security operating costs to support your environment.

Benchmark Assumptions: 1. 10,000 mailboxes. 2. Time frames are over 30 days. 3. SOC effort per incident: 10 minutes to several hours. 4. Average resource cost: $65/ hour. 5. $4.9M average cost per breach.

OPERATIONAL SAVINGS FROM REDUCED INCIDENTS

Threat	Additional Emails Allowed by Cisco[1]
BEC Attacks	3,610
Malware	8,900
Phishing	15,180
TOAD Attacks	2,570
Totals	**30,260**
Cost/Month	**$327,817**

$3.9M

Average annual reduction in SOC costs using Proofpoint[2]

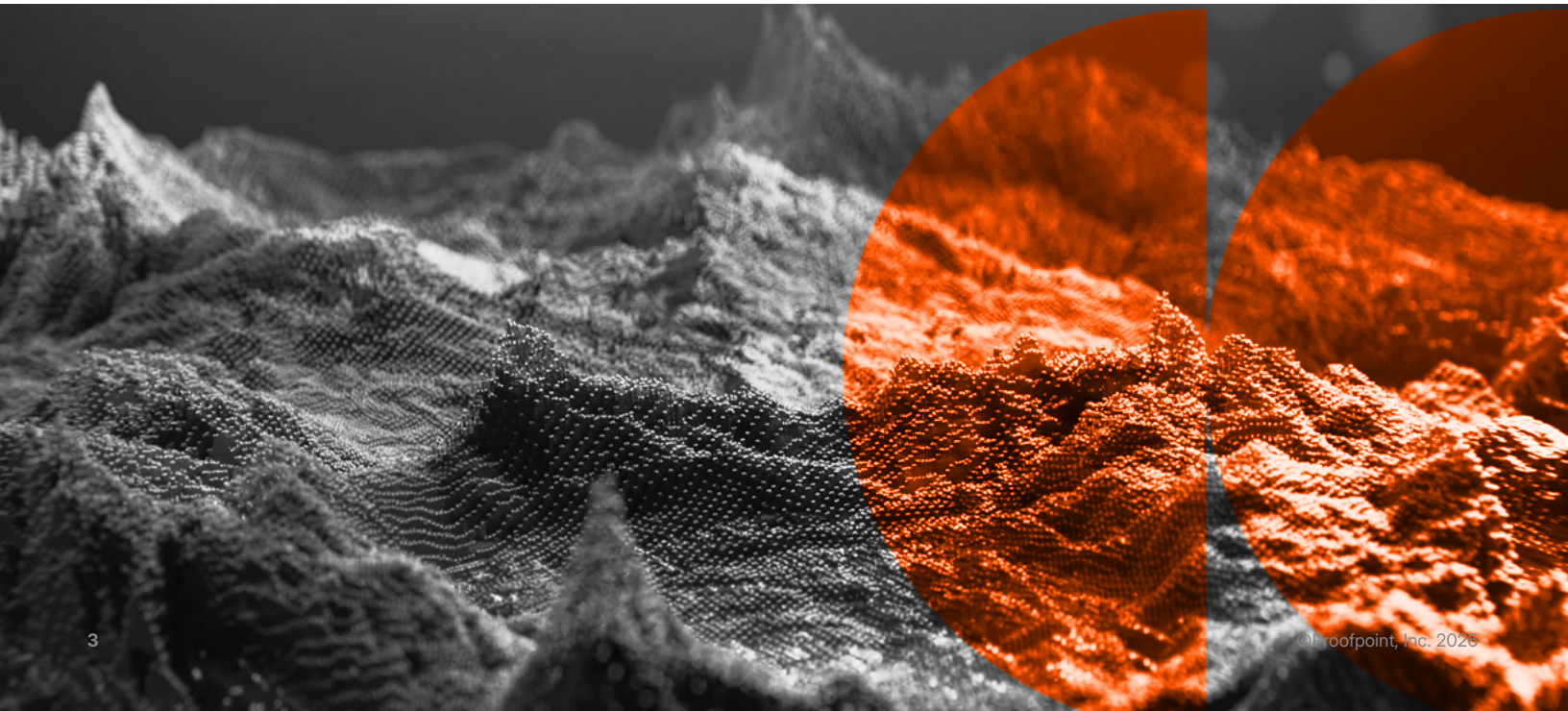
REDUCED FINANCIAL EXPOSURE FROM MAJOR INCIDENTS

	Proofpoint	Cisco
Strength of Resistance[3]	61.7%	24.8%
Incident Probability	25.7%	25.7%
Annual Exposure	$482K	$945K

$463K

Reduction in financial exposure from data breaches with Proofpoint

1. Based on 2025/2026 proof-of-concept results with Proofpoint detection in live Cisco environments (normalized to 10,000 users)
2. Observed reduction of annual security operations costs range from $87.1K - $848.6K, depending on email volume, click rates, implemented EDR/XDR controls, etc. This excludes the additional average annual reduction in risk exposure from a data breach via email of $291.7K
3. Resistance strength is based on a standardized evaluation methodology developed by a cross-functional group of Proofpoint experts across Competitive Intelligence, Engineering, Security Operations, and Product. It reflects observed differences in control efficacy—how effectively each platform detects, prevents, and remediates threats—which directly drives the relative resistance strength percentages.



Layer first, replace later

When Cisco IronPort alone is not doing the job: a case for augmenting your email security environment

Problem

A leading financial institution had built its email security stack on Cisco IronPort, a legacy secure email gateway that required constant tuning and manual policy management just to maintain a baseline. Despite the security team's efforts, users continued receiving phishing, spoofing, and BEC messages. The bank's Cisco IronPort environment relied on static, signature-based detection, which is an approach that is increasingly ineffective against today's socially engineered and AI-assisted attacks. The security team spent valuable time managing complex configurations with limited visibility, while threats continued reaching inboxes. The organization needed protection that could keep pace with advanced threats, work out of the box without weeks of tuning, and integrate seamlessly with Microsoft 365.

Complications

The strain on operations was a growing concern. Without adequate detection, every threat that slipped through Cisco IronPort triggered manual investigation cycles—analysts reviewing suspicious messages and trying to determine how they reached inboxes in the first place. At the same time, the organization needed security controls that would not disrupt email flow or create false positives across its environment. The result was a growing gap between the protection the business required and the operational effort that was required to maintain it.

Resolution

Rather than enduring a lengthy migration, the bank deployed Proofpoint Core Email Protection via API behind its existing Cisco environment—delivering comprehensive inbound protection in just 48 hours with less than a day of configuration. The bank also gained Adaptive Email DLP capabilities to prevent accidental data exposure and exfiltration, consolidating both inbound and outbound protection under a single platform and establishing a clear path to fully replacing Cisco.

How much can you save?

Partner with Proofpoint to build your custom Business Value Assessment that blends workforce efficiency metrics with data from your own environment to estimate your reduced risk and financial savings.

www.proofpoint.com

About Proofpoint

Proofpoint Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks.

Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.