proofpoint.

PLANNING GUIDE

Moving from a legacy email gateway to Proofpoint

Legacy secure email gateways (SEGs) were built to stop spam and known malware. However, today's attackers use sophisticated threats and multi-vector techniques, such as business email compromise (BEC), account takeover (ATO), QR phishing and MFA bypass—threats that legacy email gateways weren't designed to handle. So, if you're using one, there's a higher risk your organization will experience a breach as well as soaring operational costs.

If you're looking to switch to Proofpoint for better security, this planning guide will help you map the migration path. It's designed for customers of Barracuda, Cisco (IronPort), Forcepoint (Websense), Symantec Email Security.cloud (MessageLabs), Trellix (FireEye/McAfee) and Trend Micro.

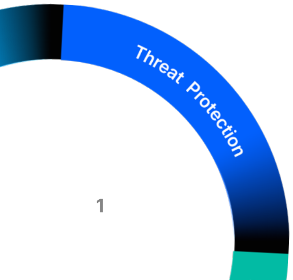
These step-by-step instructions will help you evaluate your legacy gateway's effectiveness, measure its costs and build a timeline for migration. Proofpoint offers flexible deployment options—SEG, API or a phased approach—so you can choose what fits your environment best. To simplify this process, your Proofpoint team can provide you with free tools—such as our Rapid Risk Assessment, Gap Report and Business Value Assessment—to quantify risk reduction and ROI.

Step 1: Quantify the effectiveness of your protection

Start with visibility. Measure how well your current defenses perform—and what's slipping through—to establish a clear baseline.

- Review false negative reports, which can be found in admin logs and SIEM/IR tickets. This can help you to understand the scale and range of missed detections.
- Document what percentage of user-reported mail were confirmed as a true positive, which will help you to quantify the amount time analysts spent on resolving false positives.
- Identify ATO incidents that were detected by other systems. Examples include mailbox rules abuse, impossible travel or geolocations, and MFA bypass.
- Review internal/lateral phishing attempts that were detected by other systems or reported by users.
- Run a Proofpoint Rapid Risk Assessment. This will give you data-driven insight into the threats that your existing gateway or Microsoft 365 setup may be missing.

This solution set is part of the Proofpoint human-centric security platform mitigating the four key areas of people-based risks.



Step 2: Calculate the cost of business as usual

Security isn't just about what you block—it's about how efficiently you operate. Evaluate the time, effort and analyst fatigue tied to manual triage, false positives and fragmented workflows to reveal the true cost of keeping your legacy gateway.

- Document how many clicks and minutes/hours it takes for your analysts to investigate a single phishing case. (It's not unusual for analysts to use more than 12 clicks and to spend several hours resolving each case.) Also, identify where delays typically occur.
- Track analyst hours spent on abuse mailbox triage. Calculate how much time analysts spend reviewing user-reported mail each week. Also, find out what percentage of those messages turn out to be real threats versus false alarms.
- Calculate the time your team spends preparing reports. Note how long it takes your team to compile and format security metrics into executive- or board-ready reports. Often, this requires manual data exports and spreadsheet work.
- Talk to security analysts and document their frustration points. What issues come up the most frequently? Examples include noise, false positives and console sprawl.

Step 3: Choose your migration path

Your environment and priorities will evolve, so your email security should, too. Proofpoint gives you flexibility that single-model vendors cannot provide. We are unique in that we offer three migration paths:

- **Option 1: Augment with API-based protection.** This option is low effort and high impact. Integrate Proofpoint Core Email Protection API with Microsoft 365 for immediate protection against threats, such as BEC, ATO and phishing. This also supports organizations transitioning off their legacy email gateway to a Microsoft + Proofpoint model, providing continuous protection during and after the migration
- **Option 2: Start with API, move to SEG.** This requires a moderate effort, but it has a higher impact. Begin with Proofpoint API for fast operational gains and risk reduction. Then, transition to Proofpoint SEG over time to get routing control, for changing compliance needs or to ensure advanced layered defenses.
- **Option 3: Full SEG replacement.** Retire your legacy email gateway entirely and migrate your MX records to Proofpoint SEG for maximum control and complete pre-delivery protection.

Step 4: Plan and pilot your migration

Validate results before full rollout. A controlled pilot lets you test Proofpoint alongside your existing gateway, confirm stronger detection and faster response, and build data-backed confidence with leadership.

- Define your success criteria up front. What are you hoping to achieve? Examples include improved threat detection, reduced false positives, faster remediation and ATO prevention.
- Observe potential detection improvements by running Proofpoint's email protection in silent mode.
- Look for these deliverables from your pilot:
    - Clear side-by-side results showing the threats Proofpoint caught and that your legacy email gateway missed
    - An easy-to-read summary of coverage gaps
    - A business value report that quantifies the time your team saved and your organization's reduced risk in dollars

Step 5: Build your timeline

Plan a phased transition that aligns with renewal cycles, staffing and risk tolerance. With Proofpoint's migration support, you can modernize protection without disruption.

- Create a 3-phase plan:
    1. Pilot
    2. Parallel run
    3. Cutover
- Review your license renewal schedule and budget cycles. If necessary, look for contract buyout opportunities.
- Run your old system in parallel as a safety net until leadership is confident in your new deployment.
- Use Proofpoint Premium Services for a white-glove migration experience. Our Advisory and Applied Services teams provide hands-on expertise to optimize configurations, accelerate deployment, and ensure continuous protection during your transition.

Wrap-up

When you choose Proofpoint, you don't have to navigate this journey alone. We provide migration playbooks, pilot templates and real-world customer success stories to guide your path. Whether you're starting with API, phasing into SEG or replacing your legacy email gateway entirely, we help you migrate with confidence and deliver measurable results.

Why Proofpoint?

About Proofpoint

People protection

3.4T	Emails scanned per year
>1.4T	SMS/MMS scanned per year
124M	BEC attacks stopped per month
>183M	Phishing simulations per year
0.8T	Attachments scanned per year
21T	URLs scanned per year
177M	Telephone-oriented attacks stopped per year

Market adoption

2.7M+	Customers
150+	Global ISP and mobile operators
>80%	F100 protected by Proofpoint
57%	F100 using Proofpoint DLP
>63%	F1000 protected by Proofpoint

proofpoint.

Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →