



proofpoint®

CUSTOMER VOICES

# The Breaking Point

Security and IT leaders on why they left  
Cisco IronPort, and what happened next

## INTRODUCTION

# Cisco IronPort had one job: protect email. **It failed.**

We asked security and IT leaders four questions about their decision to leave Cisco: when they knew, what held them back, what finally caused them to make the switch, and what migration was like.<sup>1</sup> Here are the answers, in their own words.

**01 The Breaking Point**

When did you realize the risk of keeping Cisco was impossible to ignore?

**02 The Hesitation**

What initially held you back from switching?

**03 The Decision**

What made staying with Cisco the bigger risk?

**04 The Transition**

What made migration easier than expected?

1. To protect their privacy, customers are identified by their role, industry, and region only.

01

THE BREAKING POINT

# When did you realize the risk of keeping Cisco was impossible to ignore?

Most describe a slow decline in detection quality that became undeniable, rather than one dramatic failure.

“For years, Cisco’s own dashboard told the story: more and more email was being delivered without being detected as malicious. When we deployed, malicious email accounted for around 80% of our detections; by the end, it was less than 50%. Given their indifference and lack of a roadmap, it was time to explore new options.”

IT SECURITY PROFESSIONAL, LOCAL GOVERNMENT, UNITED STATES

“The most serious issue was the endless number of phishing emails that were delivered unnoticed through the gateway. That represented a massive additional risk for the company.”

SECURITY ENGINEER, APPAREL AND RETAIL, EUROPE

“We had a high number of spam, phishing, and BEC emails slipping through our filters. We tried everything the ESA was capable of, and it still wasn’t good enough.”

SECURITY ENGINEER, TECHNOLOGY, EUROPE

“We wanted to modernize our threat detection stack. Our existing setup had been static for years, and we needed to validate that a new platform wasn’t just as good on phishing and BEC—it had to be better.”

TECHNOLOGY, UNITED STATES

“IronPort wasn’t stopping threats. That’s what brought us to the table to evaluate Proofpoint in the first place.”

SECURITY TEAM, HEALTHCARE, UNITED STATES

“We’d see our gateways choke during traffic surges. We needed to know a new platform could handle that kind of load without falling over.”

TECHNOLOGY, UNITED STATES

## 02 THE HESITATION

# What initially held you back from switching?

The hesitation was rarely about doubting Proofpoint. It was about the operational weight of what they'd already built on Cisco.

“Over the years our scope crept—we were using the appliance as a mail relay, for data loss prevention, outgoing encryption, custom attachment rules, custom quarantine, even strategic rerouting of email based on content. The thought of change was mind-boggling, given our lack of documentation and standards.”

IT SECURITY PROFESSIONAL, LOCAL GOVERNMENT, UNITED STATES

“We tried tuning our Cisco ESA, then added Microsoft Defender as a second filter—but that broke SPF and DMARC, since mail routed through the ESA first. Two gateways in a row meant the rules we'd written for external email no longer applied internally.”

SECURITY ENGINEER, TECHNOLOGY, EUROPE

“We'd built years of process around how our old platform worked. Our first question for any new one was always: how do we configure this the same way?”

TECHNOLOGY, UNITED STATES

“We wanted separate lanes for business-critical email versus bulk email that could wait. That's how we'd always run it, so that was our starting assumption going in.”

TECHNOLOGY, UNITED STATES



## 03 THE DECISION

# What made staying with Cisco the bigger risk?

In most cases, the deciding factor was direct evidence, not persuasion.

## \$463K

Lower annual financial exposure to email-based breaches with Proofpoint<sup>2</sup>

“We ran a one-month POC, splitting our inbound mail flow to compare Proofpoint side by side against our existing setup. Most of the unwanted mail was caught by Proofpoint—the numbers were very clear.”

SECURITY ENGINEER, TECHNOLOGY, EUROPE

“We mirrored our mail stream so both platforms saw identical traffic, then ran them side by side and compared what each one caught using our own data pipeline. The results weren’t close.”

TECHNOLOGY, UNITED STATES

“We needed a deployment that was architecturally close to what we already had but modernized. There wasn’t another vendor who could meet those requirements the way we needed them met.”

TECHNOLOGY, UNITED STATES

## 61.7% vs. 24.8%

Proofpoint’s threat-resistance strength compared to Cisco’s<sup>3</sup>

“In our proof of concept, we caught 200,000 targeted attacks and millions of bulk emails that had been getting through. If you give me 200,000 chances to make a half-court shot, I’m going to make one.”

SECURITY TEAM, HEALTHCARE, UNITED STATES

“We warned Cisco a year in advance that we were evaluating competitors. They didn’t respond with a roadmap, a presentation, or even a conversation to try to keep us. Their interface hadn’t changed in eight years—the product looked abandoned.”

IT SECURITY PROFESSIONAL, LOCAL GOVERNMENT, UNITED STATES

2. Based on 2025–2026 proof-of-concept results with Proofpoint detection in live Cisco environments (normalized to 10,000 mailboxes).

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.

## 04 THE TRANSITION

# What made migration easier than expected?

Concerns about migration were consistently bigger than the experience itself.

## 48 hours

Time to deploy Proofpoint's comprehensive inbound protection behind an existing Cisco environment, with less than a day of configuration<sup>4</sup>

"The transition to Proofpoint was absolutely professional and seamless. Employees didn't notice the change at all—and the level of protection increased significantly."

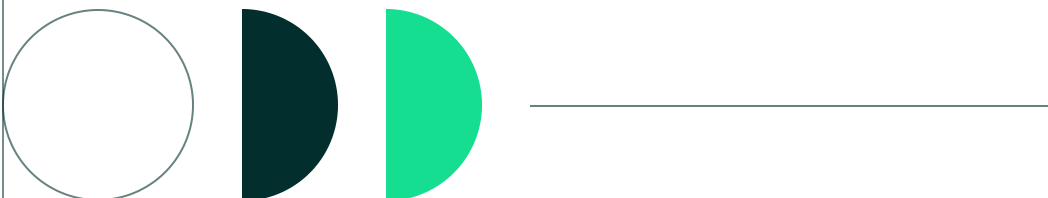
SECURITY ENGINEER, APPAREL AND RETAIL, EUROPE

"A lot of the custom rules we didn't need to migrate at all—Proofpoint's out-of-the-box filtering covered the same ground. The professional services team walked us through the first rule set, and after that we could complete it ourselves."

SECURITY ENGINEER, TECHNOLOGY, EUROPE

"In government, new deployments typically take months, not days. We had two to three weeks for this migration and finished the bulk of it in days. We've been hands-off, set-it-and-forget-it, for nearly a year now."

IT SECURITY PROFESSIONAL, LOCAL GOVERNMENT, UNITED STATES



4. Based on Proofpoint professional services deployment experience. Timelines vary by environment complexity, mail volume, and configuration requirements.

## NEXT STEPS

# Ready to see it for yourself?

## \$3.9M

Modeled annual security operations center (SOC) cost reduction for organizations using Proofpoint over Cisco<sup>5</sup>

Talk to a Proofpoint specialist about migrating from Cisco IronPort.

[Request a demo](#)



5. Based on a 10,000-mailbox benchmark: 30,260 additional threats allowed by Cisco per month, 10 minutes of SOC effort per incident, \$65 per resource hour. Actual results vary by email volume, click rates, and existing EDR/XDR controls.

**About Proofpoint, Inc.** 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](https://www.proofpoint.com).

**Connect with Proofpoint:** [LinkedIn](#)

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

8/26  
©Proofpoint, Inc. 2026