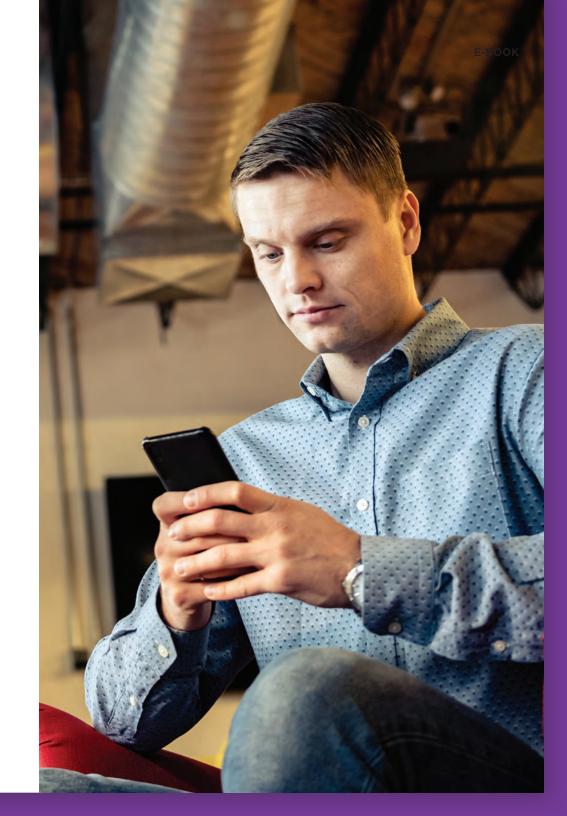proofpoint.

Rethinking Mimecast

10 Reasons Organizations Choose Proofpoint
to Secure Email and the Cloud

proofpoint.com

Introduction:
Why Email Security Matters

Today's email threats are wide-ranging and ever-evolving. At the same time, organizations are moving to the cloud and must support an increasingly remote and distributed workforce.

Are your email defenses keeping up with these changes? Email security that focuses on a single threat vector or only some types of threats may not be enough to keep your organization protected.

Today's attacks target people, not technology. As your "people perimeter" expands, attackers are finding new ways to exploit them to get access to critical data, systems and resources.

Your next attack is more likely to arrive through Microsoft 365 (formerly Office 365)—in some cases from your users' own accounts—than a botnet. That's why you need a people-centric approach, one that understands and adapts to each user's unique risk profile.

Here are 10 reasons organizations around the world are turning to Proofpoint for a comprehensive people-centric approach to security.

Introduction | **1** 2021 Threat Landscape | **2** Business Email Protection | **3** Account Takeover Protection | **4** Cloud Visibility and Control | **5** Security Operations Through Workflows | **6** Actionable Intelligence | **7** Threat Visibility | **8** Security Platform | **9** Technology Integrations | **10** World-class Support

2021 Threat Landscape

Attackers seeking to compromise your users have many ways to reach them and countless techniques to exploit their all-too-human vulnerabilities. An effective email defense must stop all of them, including:

- Credential phishing
- Filesharing abuse
- Business email compromise (BEC)
- Email account compromise (EAC)
- Sophisticated attacks on Microsoft 365 and Google Workspace (formerly G Suite) accounts

Often, these attacks use multiple channels and tactics in tandem. An attack might start with an email and end with a user accepting the permissions to a risky third-party app. Or it might involve hijacking a legitimate cloud account and using it to share malicious files through email links.

No matter what form they take, organizations must protect against these hybrid cross-vector attacks.

Our Proofpoint Nexus Threat Graph collects, analyzes and correlates more than a trillion data points across email, cloud, network and social media. It uses a combination of our NexusAI machine learning, advanced detection techniques and human expertise to protect our customers from the ever-changing threat landscape. This intelligence powers our products and protects against the entire spectrum of hybrid cross-vector attacks.

Other email security tools view the threat landscape in a siloed approach—focusing on the email vector alone. Today's threats call for a broader, more holistic approach.

Some threats don't use a malicious attachment or URL. Instead, they rely on social engineering to trick people into wiring money, sending sensitive information, changing bank account details and more.

Business email compromise (BEC) is a $26 billion problem[1] that comes in many forms, so no one approach can stop it. A security tool may stop one or two tactics but still leave you exposed to a multitude of others.

That's why you need a solution that addresses every angle of these deceptive and hard-to-detect threats.

Our integrated, holistic solution addresses all attacker tactics. We use more than 20 detection techniques to identify email fraud attacks through our NexusAI machine learning platform. NexusAI dynamically analyzes header and message content to identify and block these attacks.

Other BEC tools use static analysis techniques that must be manually configured and tuned. If this weren't enough of a management headache, this approach is also prone to false positives and, worse, false negatives. It all adds up to more work for your security team and more work for your people.

[1] FBI. "Business Email Compromise: The $26 Billion Scam." September 2019.

Complete protection against
business email compromise

EAC

BEC

Protection against
cloud and email account takeover

3

In the wrong hands, your users' cloud accounts can be weapons.

Cyber attackers who take over your user's Microsoft 365 and Google Workspace accounts have free reign over any sensitive data they have access to. And anyone who controls their email account can exploit people who trust it—inside and outside of your environment. (These attacks are known as email account compromise, or EAC.)

We help protect your cloud accounts with real-time alerts of suspicious activity, automated remediation and risk-based access controls.

When incidents occur, you can investigate past activity and alerts with our intuitive dashboard. Our robust policies alert you to issues in real time, remediate compromised accounts, quarantine malicious files and apply risk-based authentication when needed.

Other tools monitor only emails sent from the accounts, an approach that offers only limited visibility into EAC. It may find possible symptoms of the problem, but not the root cause.

Visibility and control
over cloud apps and OAuth access

4

The "people perimeter" has replaced the old network perimeter. Your people share sensitive data without oversight, use unsanctioned cloud apps and countless personal devices.

That's why we take a people-centric approach to protect against cloud threats, discovering shadow IT and governing cloud and third-party OAuth apps.

With rich cross-channel threat intelligence and user-specific contextual data, we go far beyond native Microsoft 365 security to safeguard users, sensitive data and cloud apps from external threats.

We identify your **Very Attacked People**™ and apply risk-based controls to keep their accounts safe. We also discover what cloud app and services your people are using and flag any risky third-party apps.

More efficient security operations through
automation and streamlined workflows

5

For already-stretched IT and security teams, every minute counts. They need a reliable solution that doesn't require painstaking setup and constant tuning.

Here are just a few of the ways we help make your IT and security teams more effective and efficient.

- **Preconfigured security and compliance policies** provide out-of-the-box value—no need to maintain policies through manual Boolean logic.
- Our **smart search feature** can locate all messages sent and received, freeing up your IT and security teams to focus on things that only people can do.

Proofpoint Closed-Loop Email Analysis and Response (CLEAR) automates the process of analyzing, verifying and removing suspicious emails reported by users. While an informed employee can be your last line of defense against a cyber attack, user-reported emails are not always malicious. Enriched with our world-class threat intelligence and security awareness training, CLEAR stops active attacks in their tracks with just a click. It helps your team follow up on reports without adding hours of triage and remediation time. Potentially risky emails are resolved in minutes, not days.

Our threat intelligence spans email, cloud, network, mobile and social media, giving you a complete picture of the threats that target your people.

By having visibility into all these threats, we provide unique people-centric insights into threats at the organization and user level.
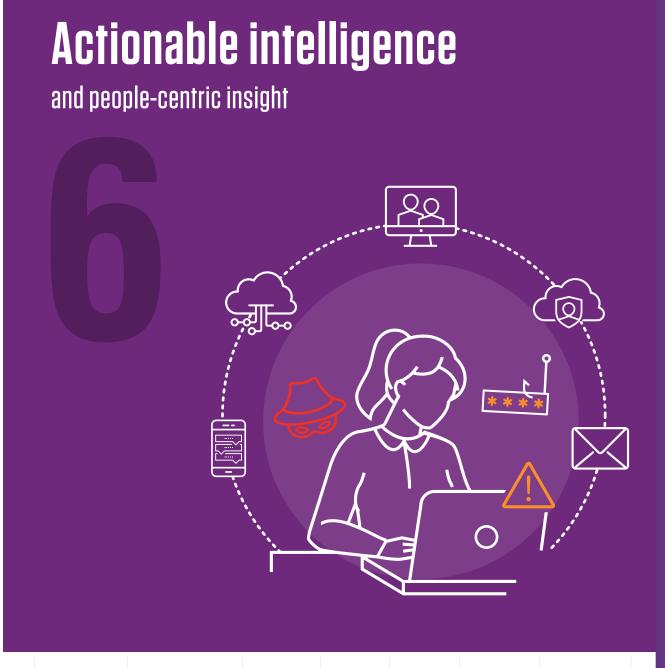
Knowing who your most attacked people, or **VAPs**, are helps you protect them and carefully manage access to guard against the effects of account compromise.

The Proofpoint Attack Index helps identify these VAPs. The index is a weighted composite score of all threats sent to each user in your organization. It scores every threat on a scale of 0-1000 based on four factors:

- The attacker behind it
- The attack's reach and focus
- The type of attack
- Overall attack volume

By better understanding your VAPs, you can then prioritize them and resolve threats more quickly.

We provide detailed information on threats and campaigns in real time. You gain visibility into both widespread and targeted attacks. It gives you details around the threat itself from affected users, attack screenshots and in-depth forensics such as suspicious logins and risky third-party apps.

Actionable intelligence
and people-centric insight

6

A trusted security partner

with wide visibility into today's threats

7

Our solution is the most widely deployed email security platform across the Fortune 100, Fortune 1000, and Fortune Global 2000. No other standalone cybersecurity vendor has an install base as large as ours.

With that breadth of coverage, we have a much broader view of the threat landscape across email, the cloud, networks and domains and social media. You benefit from our insight into today's biggest threats across every industry, in every segment, within every geography in the world.

As the market leader, we analyze more than 2 billion emails, 26 billion URLs and 120 million attachments every day.

We have more than 6,000 intrusion detection sensors deployed in more than 70 countries. Together, they provide real-time network and email telemetry to better understand how attacks are targeting the organizations we serve. Our global presence helps us understand how attackers target regions differently. This unique insight makes us better security partners and helps you more effectively protect your people.

As today's number one threat vector, email should be a critical part of your security strategy. But risk comes in many forms, so a mature cybersecurity strategy calls for mitigating other threats, such as:
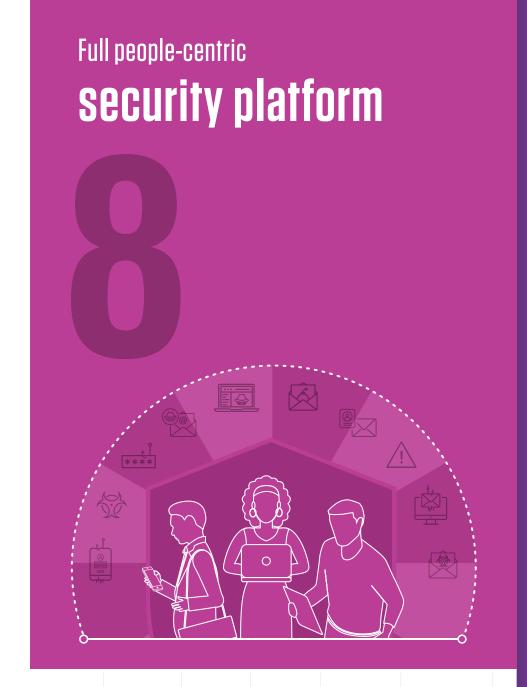
- Cloud accounts
- Insider risk
- Web-based attacks
- Software-as-a-service compromise

- Brand and executive impersonation on the web and in social media
- Dark web and physical security threats

With Proofpoint, you can enhance your threat response capabilities, extend protection to more digital channels, get custom insight and secure your business ecosystem.

Here are some of the key solutions that make up our people-centric security portfolio:

- **Proofpoint Insider Threat Management** to protect against malicious, negligent and compromised users
- **Proofpoint Security Awareness Training** to educate users and make them more resilient
- **Proofpoint ThreatSim** phishing simulation to reveal potential user vulnerabilities
- **Proofpoint Web Isolation** to keep harmful web content out of your environment
- **Proofpoint Domain Discover** to monitor and takedown lookalike web domains that might be used to attack your people
- **Proofpoint Social Discover** to identify fraudulent social media accounts posing as your executives and brand
- **Proofpoint Social Patrol** to remove risky content from your organization's social media accounts
- **Proofpoint Digital Risk Protection** to find and remediate doxing of executives and other high-profile employees
- **Proofpoint Threat Response Auto-Pull** to automate security event correlation and response
- **Proofpoint Cloud Access Security Broker** to protect cloud-based accounts and activity

Full people-centric
security platform

8

Technology integrations

that streamline operations

9

Our complete, integrated security platform combines powerful, effective cloud and email protection to solve today's most pressing challenges.
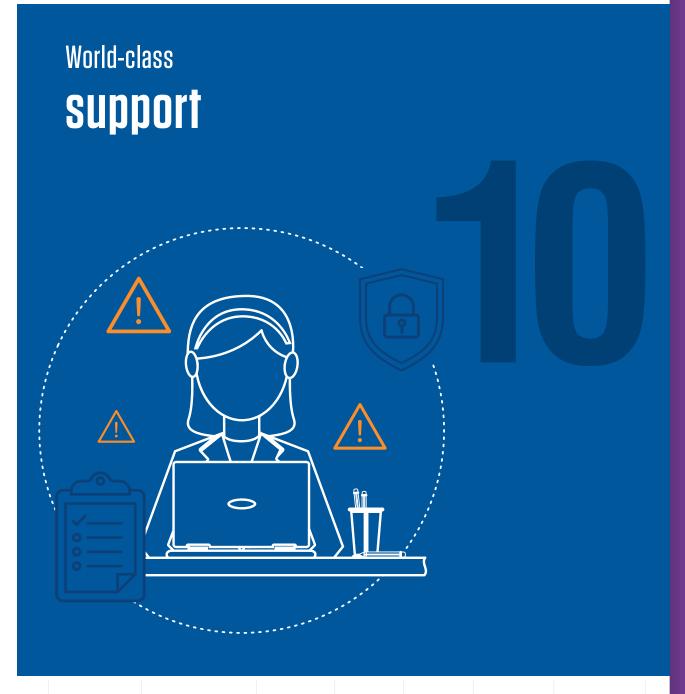
We also integrate with best-in-class security vendors such as Palo Alto Networks, Okta, CrowdStrike, SailPoint and CyberArk to streamline your workflow and help your security team work better and faster.

Together, it all adds up to unified, people-centric security that protects your cloud deployment. Our proven approach to security reduces your risk, frees up resources, cuts costs and makes your security operations more effective and efficient.

World-class
support

10

Every purchase includes full installation and customization of the solution along with access to the latest industry trends and best practices.

We offer 24/7/365 support after deployment—no complicated service add-ons. Our company earns a sustained customer satisfaction rate of more than 95% and a yearly renewal rate of more than 90%.

It's no wonder that we have the most widely deployed solution of the Fortune 100. We serve more than 140,000 customers, including:

- The top global banks
- The top global retailers
- The top pharmaceutical companies
- The top research universities

LEARN MORE

For more information, visit **proofpoint.com**.

proofpoint.