EXECUTIVE BRIEF

proofpoint.

THE HIDDEN COSTS OF MICROSOFT OFFICE 365 SECURITY & COMPLIANCE

www.proofpoint.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

So your organization has decided to migrate to Microsoft Office 365. While you'll likely benefit from its cloud collaboration capabilities, you might want to ask more about what Office 365 means for security, compliance and e-discovery.

It sounds hard to turn down the promise of advanced threat protection, data protection and an online archive designed to meet privacy, compliance and data-retention requirements especially when it's all included with your Office 365 deployment. Why spend more money on third-party email security or archiving when it comes as part of your Microsoft license? Aren't all email security and compliance solutions pretty much the same?

The answers to those questions aren't that simple. While Microsoft security might be fine for some purposes, it could also lead to problems and cost more than you expect. Not all advanced threat, email security, or compliance archiving solutions are created equal.

Think about it like the differences between a camping tent and a house. Both can keep you dry during a sudden rain shower. But in a winter storm with gale-force winds, only one of them will make a good shelter.

In the same way, an advanced email security solution can provide better security and compliance defences in today's stormy cybersecurity environment.

WHY EMAIL SECURITY FOR OFFICE 365 MUST BE A TOP PRIORITY

It's no surprise that 91% of targeted attacks start with email.[1]

From phishing to malware, email makes it easy for attackers to exploit the human factor and to steal credentials, data and more.

PHISHING

In the 20-plus years since it was first identified as a threat, phishing has morphed into a highly sophisticated technique for stealing credentials, funds and valuable information. Today's phishing is multi-layered and evades many conventional defences. Attacks can be broad-based or highly targeted. Many use malware, but others don't. Cybercriminals even deliver phishing emails through legitimate marketing services to evade spam filters and other defences.

Whatever their tactics, phishing attacks are highly successful. According to Verizon's 2016 Data Breach Investigations Report, users last year opened 30% of phishing messages, up from 23% in the prior year.[2] And the SANS Institute reports that 95% of network attacks result from spear phishing.[3]

PROVEN SUCCESS AT LEADING ENTERPRISES

"Proofpoint has given us protection from standard bulk campaigns in Office 365 emails, giving us our time back to find more evil things.

—CISO, Global 500 Manufacturer

"Using Proofpoint to secure our Office 365 email has saved us time and money that would have otherwise been spent on rebuilding compromised systems."

—CSO, Fortune 500
Banking Company

"Customer service and support has been excellent. The product works very well and has kept us phish-free for a year now."

—Kenneth Brown, CIO,
Whitworth University

"Office 365 allowed too many legitimate phishing messages through. We had users fall victim, despite all the end user training to not click and enter credentials. With Proofpoint, efficacy has greatly improved to the point where I can't recall the last time it happened."

—Network Administrator,
Private University

MALWARE

Today's creative attackers use automated tools to mine information about their targets from social media profiles, which are often public. That means attackers know where you work. They know your role, interests, hobbies, marital status, employment history and more. Attackers use these details to craft convincing email messages enticing you to click on a malicious URL or attachment. Once you click, a malicious payload drops onto your system.

CYBERCRIMINALS KNOW THAT PEOPLE USE EMAIL MORE THAN ANY OTHER COMMUNICATION TOOL

BUSINESS EMAIL COMPROMISE

Beyond these tactics, another technique has emerged as a new and serious threat: business email compromise (BEC). BEC attacks are spoofed emails from someone posing as an authority figure. For example, an email that appears to come from the CEO might ask a staff accountant to wire funds. Instead, the money goes straight to the cybercriminal impostor. BEC doesn't stop at fraudulent transfers, either: attackers may also trick recipients into sending personally identifiable information, payroll details and more.

These threats can have a big impact on your bottom line. Today, the average total cost of a data breach stands at $4 million, 29% more than the average in 2013, according to a 2016 IBM report.[4]

How does all of this relate to your Office 365 migration? The heart of Office 365 is Microsoft Exchange Online email. The built-in security, compliance and archiving capabilities that come with this simply don't meet the needs of enterprise-class organizations.

Too little email protection can lead to costly breaches that taint your brand, damage your reputation and hurt your bottom line. That's why it's important to enhance your Office 365 email defences.

ATTACKS TARGET PEOPLE

More attacks come in via email than through any other vector. That's because cybercriminals know people use email more than any other communication tool.

The bad guys typically target individuals in HR, IT, or finance with access to funds or high-value data. They use social engineering tactics to lure users into opening infected attachments, visiting malicious sites, or giving up assets (such as credentials or financial data). Once they gain entry to a user's system with malware or stolen credentials, cybercriminals can penetrate corporate networks and exfiltrate treasure troves of sensitive information and valuable assets. So it's no wonder that security has evolved into a boardroom challenge. Deploying a secure email gateway is clearly a business-critical decision.

YOU CAN'T RESPOND TO WHAT YOU CAN'T SEE

To discover and respond to indicators of compromise (IoCs) effectively, you need the right insights. Unless you have an email gateway that provides you with deep, detailed reporting, you'll be left searching for the proverbial needle in the haystack.

Blocking threats using an email gateway has two critical advantages. First, you gain understanding about the whole attack, not just the final stages of it, after it has reached your network. Second, by catching threats at the gateway, you can stop them before they compromise your environment.

SILOED SECURITY IS NOT SUSTAINABLE

In the ever-evolving threat landscape, hackers coordinate attacks across multiple vectors. A well-orchestrated defence is vital to a good security posture. Protecting Office 365 is a top priority. But an effective solution must also integrate with the rest of your security ecosystem. From your firewall to your security management platform, smart and automated coordination can help you effectively prioritize and contain the impact of threats.

ACCURACY AND FLEXIBILITY ARE VITAL TO DATA LOSS PREVENTION DECREASES YOUR CHANCE OF SUCCESS

One of Office 365's core features is basic data loss prevention (DLP). But accuracy and flexibility are vital to DLP success. Inaccurate solutions can lead to confusing false positives, or worse, lost data. Additionally, each organization has individual DLP needs. Only custom classifiers and flexible policies can create a tailored DLP system that will work for your business. If you have data both on-premises and in Office 365, juggling multiple sets of policies, incident queues and enforcement tools may not an effective way towards a successful information protection practice.

ARCHIVING AND COMPLIANCE MUST BE DEFENSIBLE AND E-DISCOVERY-READY

While it's important to keep out malicious content, your organization also needs to retain and archive business-relevant content in a way that's legally defensible and according to the regulations that apply to your organization. It's critical to be able meet e-discovery obligations quickly, cost-effectively and defensibly.

Adhering to compliance and e-discovery rules requires more than just storing unprotected data within the Office 365 ecosystem. It involves email, social media, enterprise collaboration (such as Yammer and Slack) and even data stored on users' laptops. What's more, low-cost archiving isn't always the best solution: it can end up costing more in the long run through penalties and higher litigation readiness costs.

CALCULATING THE HIDDEN COSTS OF BUNDLED SECURITY

Bundled solutions can come with significant hidden costs as well as short- and long-term consequences. If your Office 365 deployment doesn't meet your security needs, the results could cost you time, information, money and even your reputation. Plus, "trying out" a bundled solution, only to find you need a dedicated security layer, can be a major drain on internal resources. How do you calculate the costs you might be missing?

FOR SECURITY TEAMS

Security has always been a tough job. Today's advanced threats make it even tougher. As compliance regulations push security up to the board level, the issue isn't just efficacy. You also need to ensure visibility to understand the threats targeting your business. Without such insights, it's hard to address security issues at an organizational level. The result can be a significant loss of time.

According to the Ponemon Institute, the biggest financial consequence for organizations experiencing a data breach is lost business.[5] The cost of this can vary widely based on the types of assets lost, as well as on how many.

NOT HAVING THE VISIBILITY AND INSIGHTS THAT YOU NEED TO ADDRESS SECURITY ISSUES AT AN ORGANIZATIONAL LEVEL CAN RESULT IN SIGNIFICANT LOST TIME.

Ask yourself these questions:

- How much productivity is lost cleaning up damage from compromises that could have been prevented?
- How much time does your team spend investigating, prioritizing and confirming threats? (For many organizations, this can range from 2 to 16 hours for each targeted user.)
- How much time do you spend cleaning up emails with malicious attachments or URLs from your users' mailboxes?
- How do you quantify the risk you face as a result of your users' prolonged exposure to such emails?
- How much time is lost from disjointed security enforcement aimed at containing threats and protecting your organization's reputation? (Hours to days per alert are common.)
- How much extra time does it take to understand threats targeting your environment when you have limited visibility?
- What is the security impact of users switching to personal mail during Office 365 email outages? (Office 365 downtime is one of the top concerns cited by organizations and leading analysts.[6])

FOR IT DEPARTMENTS

If you're an IT administrator, consider the costs of outages and support.

> **"Proofpoint has given us protection from standard bulk campaigns in Office 365 emails, giving us our time back to find more evil things.**
>
> —CISO, Global 500 Manufacturer

UPTIME/SERVICE AVAILABILITY

Forrester Research cites availability as one of the top challenges organizations face with Office 365 email.[7] According the most recent industry calculations, the overall cost of an outage is about $5,600 per minute, or more than $300,000 per hour.[8] As you look to boost your Office 365 security and minimize these costs, ask yourself these questions:

- How heavily does your business rely on email? What is the impact if emails from customers or prospects are lost due to email outage?
- When Office 365 email flow interrupted, how quickly are you made aware?
- Do you have timely data and sufficient visibility to set expectations on when service will be restored?
- What security and compliance risks are introduced when well-intentioned users resort to personal email to "get work done?"

MESSAGE TRACE, NON-DELIVER REPORT (NDR)

"What happened to my email message?" is a common question fielded by email IT and security professionals every day. Take a deep look at your process for dealing with these issues:

- How much time can you afford to spend supporting these issues?
- How often are message logs indexed? How long are logs retained?
- Are search query results returned in minutes or hours?
- Does the search experience differ in older versus newer logs?
- Do you have the required search criteria available to find logs quickly? Are the details returned from the search sufficient?
- What is the process for calling support for more detailed information?
- What is the impact of the false positives on the volume of message traces and time required?

TIME SPENT ON EMAIL AND MACHINE CLEANUP

IT can spend hours and even days reimaging infected machines when email-related security events occur and systems are compromised. Further, IT should remove these emails to prevent re-infection, which occurs when a user unknowingly re-accesses the content, or even forwards it to another user. This process impacts both IT and user productivity, typically a day per incident. Ask yourself:

- How many machines are undergoing unnecessary or avoidable reimaging?
- Does IT have the tools to confirm infections and to prioritize machines that were exposed but not compromised?
- How much time does IT spend on message cleanup?

FOR COMPLIANCE STAFF

Compliance is serious business. The consequences of failing to comply can be costly and hurt your business.

ARCHIVING

At the data center level, Office 365 complies with major regulations. These mandates include European Union data protection laws, the Health Insurance Portability and Accountability Act (HIPAA), ISO 27001 and others. But Office 365 has some serious flaws when it comes to archiving and supervising email data and making it readily accessible when there's a legal dispute or at audit time. Not having legally defensible records retention and workflows can drain time and resources and even result in accusational costs.

The UK Financial Services Act requires its members to retain records for six years. Whereas as Supervisory Review module is needed to manage the selection and review of communications in accordance with Financial Services mandates established by Financial Industry Regulatory Authority (FINRA), Securities and Exchange Commission (SEC) and Investment Industry Regulatory Organization in Canada (IIROC),

Fines for non-compliance with FINRA (USA), SEC (USA) and the IIROC (Canada), which aim to protect investors by making sure the US and Canadian security industry operates fairly and honestly, can run well into the millions.[9] Added costs include the cost of deploying additional security measures, audits and potential reputational damage.

As you evaluate the capabilities of Office 365, ask these important questions:

- If your organization is involved in a legal dispute, will Office 365 enable you to provide records of all communications and transactions conducted by specific individuals including social media and enterprise collaboration platforms? What happens if you have multiple cases in progress?
- How well are you able to put content on Legal Hold when a legal dispute happens?
- How much time does it take for IT to perform e-discovery and data export? How quickly do searches execute? Does Microsoft offer a service level agreement (SLA) that defines the parameters of this key capability? Where does the processing of the search occur?
- Once you determine the data set that you want to export, can you upload the files to a specified FTP site in an automated way? Or do you need schedule time to finish this part of the workflow manually? What are the consequences of delay in getting the required data to review teams?
- Are you able to capture and preserve all of the compliance content your organization generates? What about data from social media platforms?
- How well are you able to supervise and monitor content? Several regulations require the monitoring and sampling of content. Does it use the latest technology or does it simply rely on basic keywords matching?

INFORMATION PROTECTION

Breach statistics in all sectors are worth paying attention to. Enterprises are always at risk of data loss. Malicious insiders can leak it, external bad actors steal it and even well-intentioned employees may unknowingly expose vital company assets. The US government suffered 61,000 cybersecurity breaches in 2014 alone.[10] 91% of healthcare organizations have experienced at least one breach over the past two years according to the Identity Theft Resource Center.[11]

Take business email compromise (BEC), which has escalated beyond financial fraud. The spoofers have duped legal departments into sending out sensitive information. They have tricked human resources staff into sending end-of-year tax forms.[12]

Concern about the liability stemming from data breaches has made security a boardroom issue. With this in mind, you need to look at Office 365 security with a critical eye. Review its ability to find sensitive data (including multiple file types), resolve issues across all channels and enforce and report policy issues.

Applying policies to outbound mail, with the workflow to manage incidences serve as an important layer of security, not just compliance.

Here are some specific questions to ask:

- Can you detect sensitive data across the breadth of file types that may contain sensitive information?
- Can you quickly pinpoint what content triggered a policy alert?
- Do you have an incident response workflow in place to remediate the situation?
- Does your automated response enable remediation across multiple channels, including email, file share and Microsoft SharePoint sites? Do you need a separate DLP solution to reduce the attack surface across each of these channels? How are you keeping these policies synced and reporting consistent?
- When sensitive data is detected, how is encryption handled? What type of granularity do you have to revoke messages to the wrong recipient? What percentage of encrypted emails do you anticipate to be viewed from mobile devices? What is the recipient experience?

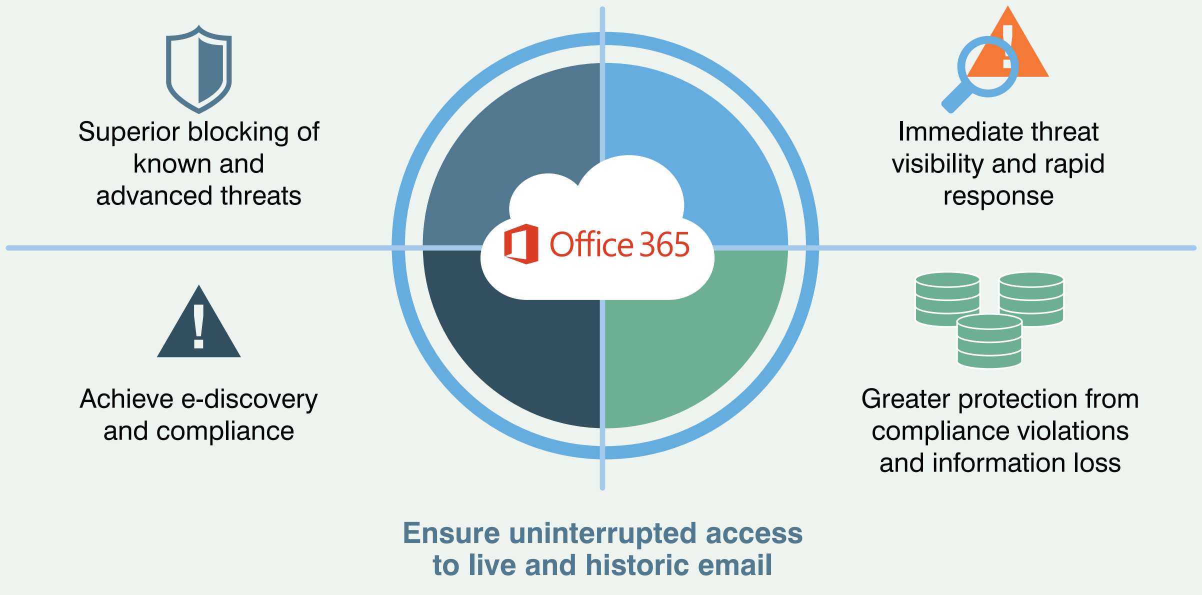
THE PROOFPOINT DIFFERENCE

Today's complex and ever-changing threat and compliance landscape requires a new approach to threat protection. When it comes to email, you need much more than just reputation checks against URLs and archaic message trace capabilities. While important, these techniques alone don't enable threat visibility, provide campaign intelligence, or help you verify and contain compromises.

Superior threat protection, immediate threat visibility and rapid response are absolute necessities. Proofpoint's email security technology far surpasses native Office 365 capabilities and provides you with the robust protection you need across multiple dimensions. Our award-winning customer support reflects our commitment to your success. With Proofpoint, you get:

- Superior blocking of both known and advanced threats
- Immediate threat visibility to help you respond faster
- Strong data protection to safeguard valuable information and foster compliance
- Capabilities that enable compliance and e-discovery
- Uninterrupted access to active and historic email for forensic purposes

HOW PROOFPOINT HELPS



Superior blocking of known and advanced threats

Immediate threat visibility and rapid response

Achieve e-discovery and compliance

Greater protection from compliance violations and information loss

Ensure uninterrupted access to live and historic email

ADVANCED TECHNOLOGIES BOOST YOUR OFFICE 365 DEFENCE

Here's how Proofpoint adds greater power and benefits to Office 365's built-in defences.

INDUSTRY LEADING EFFICACY FOR ADVANCED THREATS

Security is our business. With the sophistication of today's attacks, you need a dedicated security layer. Proofpoint uses a combination of static and dynamic techniques to catch even the most advanced threats. The sandbox constantly adapts to detect new attack tools, tactics and targets. It applies to URLs and attachments in email to protect you from banking Trojans, credential phishing and other attacks targeting your organization.

Our unique predictive analysis preemptively identifies and sandboxes suspicious URLs based on email traffic patterns. This means analysis minimizes the risk of a patient-zero case from a previously unknown malicious URL.

IMPOSTOR EMAIL CONTROLS

Significantly reduce exposure presented by advanced spoofing and BEC attacks with a comprehensive solution that includes policies, authentication, classification and advanced DLP to provide visibility and enforcement. This includes proprietary machine learning, communication trend baselining, malformed message attribute analysis and pre-built policies for holistic detection and visibility.

LOW-PRIORITY INBOX

We provide graymail classification with a high degree of accuracy and responsive learning of individual preferences. This ensures that low-priority messages are handled appropriately without blocking business-critical emails. Granular visibility via user digests gives employees quick visibility into emails that have been filtered and categorized into low priority inboxes. And as their needs change, they can update their preferences directly through the digest.

DETAILED FORENSICS AND THREAT INTELLIGENCE FOR CAMPAIGN INSIGHTS

Get immediate insight into bad actors, the tools and techniques they are using and the people they are targeting. You gain an understanding of the bigger picture around the attack campaigns targeting your organization.

AUTO-PULL SAVES CLEANUP COSTS

You can move emails to a user-inaccessible quarantine, either automatically or on-deman. This feature works for both Office 365 Exchange Online and Exchange mailboxes.

INTEGRATION WITH YOUR SECURITY ECOSYSTEM

We work closely with a large ecosystem of security vendors to quickly contain threats that have an impact beyond your Office 365 deployment, including:

- Integration with Palo Alto Networks wildfire for additional threat intelligence
- Security information and event management (SIEM) tools, such as Splunk, for threat intelligence and detection. Real-time streaming can help you correlate email with network events to detect and respond to threats faster.
- Yield immediate protection. Apply email threat intelligence seen in your environment at the at the network level, leveraging your existing enforcement tools to close the gap between threat detection and protection. Stop:
  - Infections from spreading from one system to another
  - Control signals from reaching malware
  - Sensitive data from reaching external sites

Proofpoint automates containment, using your existing enforcement tools to close the gap between threat detection and protection.

ENFORCEMENT DEVICES

- Cisco ASA
- Palo Alto Networks
- Check Point
- Cisco IOS
- Juniper SRX (JUNOS)
- Fortinet FortiGate
- Blue Coat
- Microsoft Exchange/ Office 365
- OpenDNS
- CyberArk
- Imperva

ENDPOINT FORENSIC COLLECTION AND COMPROMISE VERIFICATION

Not all attacks result in compromise. That's why you need insight into where to prioritize efforts. Automatic indicator of compromise (IoC) forensic collection from the endpoint lets you compare a forensic snapshot of the endpoint to a sandbox forensics version to help verify infections and gain threat insights. You can also check for evidence of past infection on the target machine and scan on demand to check for IoCs on other machines. Automating data collection improves your quality of response.

> **"Using Proofpoint to secure our Office 365 email has saved us time and money that would have otherwise been spent on rebuilding compromised systems."**
>
> —CSO, Fortune 500
> Banking Company

EMAIL DATA LOSS PREVENTION

DLP projects are prone to failure. Focusing on the channels you care about most with a unified set of policies and incident response queues dramatically increases the likelihood of success. We protect multiple content types, not just Office 365 files. Beyond 'set-and-forget' DLP, we also offer deep insights into compliance violations. Policies can be fine-tuned to meet your organization's needs and priorities. A robust incident response workflow for administrators and users makes it easier to take swift action when incidents arise.

EMAIL CONTINUITY

Keeps users connected and productive in the event of an Office 365 email outage. This always-on insurance policy for critical business communications enables users to continue sending and receiving email without requiring any action from IT. End users get full access, including calendar and contacts, either natively within Outlook or via web portal. The most recent 30 days of email can be made available in the end user inboxes. All emails are restored, with headers intact, to the email server. That means archiving and forensics for legal purposes are never a problem.

COMPLIANCE ARCHIVING

Most organizations are required to ensure legally defensible retention of content in Office 365, including Exchange Online, OneDrive for Business and Skype for Business. The archive features provided by Microsoft are much more about storage management than e-discovery and compliance.

We go far beyond Microsoft Office 365 archiving. We guarantee immutable archive storage and exhaustive indexing of more than 500 attachment types, including non-proprietary Microsoft file formats as well as capture and preserve content from a wide variety of content sources including Slack, Bloomberg and social media platforms. The robust e-discovery workflow and guaranteed search performance makes forensics faster and easier. Our proprietary Double-Blind Key Encryption architecture ensures that you retain complete control over the encryption key for data kept in our cloud-based storage.

CUSTOMER SUPPORT

In addition to our dedicated focus on security, we offer best-in-industry customer support with a 95% satisfaction rating. Our comprehensive support options make it easy to manage and scale security, continuity and compliance.

REINFORCE YOUR OFFICE 365 SECURITY WITH PROOFPOINT

Doing all you can to ensure the security of Office 365 makes a lot of sense. As the volume and sophistication of advanced threats continues to evolve more rapidly than ever before, you must protect your people, data and brand from advanced attacks and compliance risks.

Our security solutions provide you with industry-leading security, compliance and email continuity capabilities for your cloud-based Office 365 deployment that far exceed Microsoft's native protection. With Proofpoint, you can take advantage of the freedom, flexibility and cost savings of Office 365—without sacrificing your ability to keep users connected and protected.

For more information, visit: www.proofpoint.com/office365

[1] Kim Zetter (Wired). "*Hacker Lexicon: What Are Phishing and Spear Phishing?*" April 2015.
[2] Verizon. "2016 Data Breach Investigations Report." April 2016.
[3] Neal Weinberg (Network World). "*How to blunt spear phishing attacks.*" March 2013.
[4] IBM "*IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident*"
[5] Ponemon Institute and IBM. "2016 Ponemon Cost of Data Breach Study: Global Analysis" June 2016.
[6] Proofpoint. "*Is Microsoft Office 365 Secure*?" 2016.
[7] Proofpoint. "*Six Key Capabilities for Securing Office 365 Email.*" May 2016.
[8] Andrew Lerner (Gartner). "*The Cost of Downtime.*" July 2014.
[9] Financial Industry Regulatory Authority (FINRA). "*FINRA Fines Scottrade $2.6 Million for Significant Failures in Required Electronic Records and Email Retention.*" November 2015.
[10] Ian Bremmer (Time). "*These 5 Facts Explain the Threat of Cyber Warfare.*" June 2015.
[11] Identity Theft Resource Center.
[12] FBI. "*FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals.*" March 2016.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.