proofpoint®

Protecting People 2019

A Global Cybersecurity Analysis of Vulnerability, Attacks and Privilege

proofpoint.com

Not everyone in your organization is a VIP.

But anyone can be a VAP: Very Attacked Person™

And these VAPs aren't always the people you expect. That's because today's attacks target users in countless ways, across new digital channels, with objectives that aren't always obvious.

Just as people are unique, so is their value to cyber attackers and risk to employers. They have distinct digital habits and weak spots. They're targeted by attackers in diverse ways and with varying intensity. And they have unique professional contacts and privileged access to data, systems and resources.

These three factors—vulnerability, attacks, and privilege—determine their overall risk.

This report presents data gathered January–June 2019. We examine which employees, departments, and industries are the most vulnerable. We analyze which ones receive the most targeted threats. And we explore how their privilege might be abused.

Based on these findings, we recommend concrete steps you can take to build a defense that focuses on your people.

KEY FINDINGS

Here are some of the biggest trends of the first half of 2019.

Vulnerabilities

Education and food/beverage organizations were the industries most vulnerable to cloud-based attacks.

More than

7 of 10 unauthorized login attempts

to their cloud accounts were successful.*

Even heavily regulated industries were vulnerable to cloud account compromise.

In finance **20%** & in healthcare **40%**

of attack campaigns resulted in a successful compromise

Attacks

More than

20% of email addresses

at the highest risk† from malware and credential phishing attacks were generic aliases.

R&D/engineering and marketing/PR support

were among the departments facing the largest overall risk† from email-based malware and phishing attacks.

Facilities/internal support

was another high-risk group, though it faced a smaller volume of attacks.

Privilege

VAPs in lower-management roles are targeted in nearly

8% more email-based malware and phishing attacks

than the average VAP.

Overall, VAPs at every rung of the corporate ladder are at a roughly equal risk from email-based malware and phishing attacks.†

It's more evidence that your

VAPs aren't always your **VIPs**

*Cloud threat data in this report comes from a September 2019 blog post by the Proofpoint Cloud App Security Team. You can read the full report here: https://www.proofpoint.com/us/threat-insight/post/cloud-attacks-prove-effective-across-industries-first-half-2019.

†Based on our Attack Index. See "What is the Attack Index?" on page 8.

SECTION 1 VULNERABILITIES

Every industry is targeted in cyber attacks. But for a variety of reasons, they are not compromised in equal measure. The likelihood that an unauthorized login attempt is successful is one measure of their vulnerability.

Industries most vulnerable to cloud attacks

The education and food and beverage sectors were most vulnerable to cloud account attacks, with more than 7 in 10 attack campaigns resulting in a successful compromise (Figure 1).

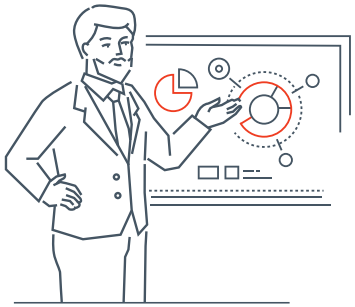
For cyber criminals, school districts, colleges and universities were easy prey. Possible reasons include large numbers of users (such as students) and decentralized security operations.

Cloud accounts that go largely unused, such as those provided to a school's alumni, represent ideal targets for brute-force password attacks. Many account owners don't use the account often enough to notice anything amiss. Once attackers gain control over the account, they can use it for spam, malware and phishing campaigns—especially against other users within the school's domain.

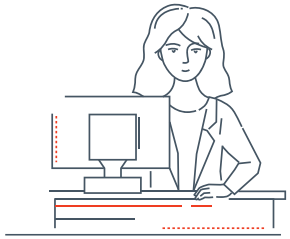
Get to know your VAPs

Common titles among targeted education users included:

PROFESSOR



ALUMNI



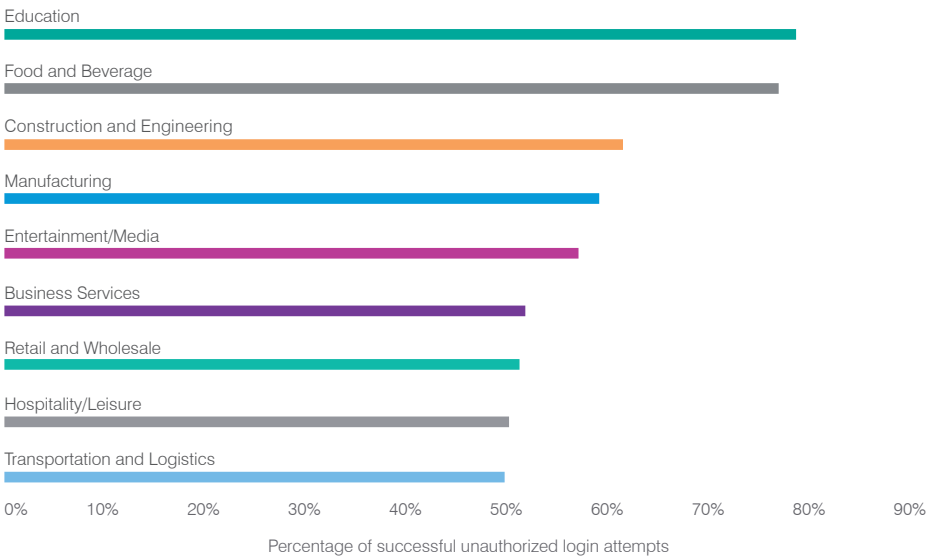
METHODOLOGY

We analyzed data from more than 1,000 cloud service tenants with over 20 million user accounts. (Tenants are single cloud service deployments in an organization. One organization may be tied to multiple tenants—it might deploy both G Suite and Microsoft Office 365, for instance.) We saw more than 15 million unauthorized login attempts, 400,000 of them successful.

Note: cloud threat data in this report comes from a September 2019 blog post by the Proofpoint Cloud App Security Team. You can read the full report here: https://www.proofpoint.com/us/threat-insight/post/cloud-attacks-prove-effective-across-industries-first-half-2019

Illicit Logins: Most Vulnerable Sectors (Figure 1)

Education and the food and beverage industry were the most vulnerable to cloud account attacks.



In the food and beverage industry, franchisees were highly targeted and vulnerable to cloud-based attacks. Franchisees—essentially, small businesses linked to a large corporate parent—are an easy entry point for threats.

Compromising an account within a franchise gives attackers access to corporate financial business processes and supply chains. That access makes food and beverage outlets ideal targets for:

- Wire fraud
- "Lateral movement" into other parts of the business
- "Internal phishing" against other users within the compromised environment

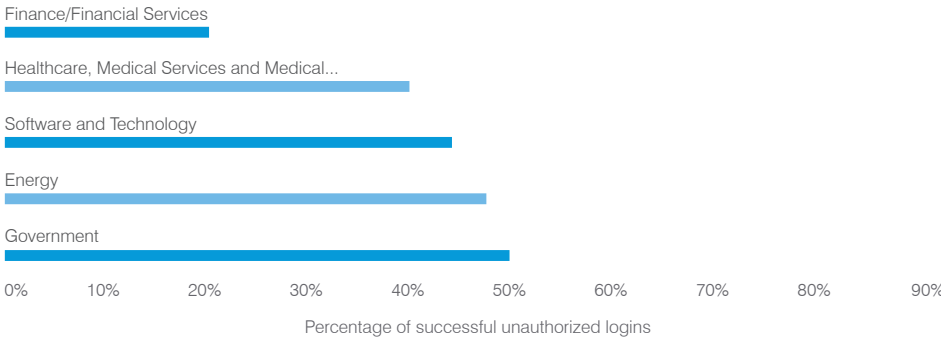
Best protected industries

Attackers had less success with heavily regulated sectors such as financial services and healthcare. This is likely due to these sectors' more stringent security controls. Even so, 2 in every 10 attack campaigns against financial services firms resulted in a successful compromise, and 4 in every 10 campaigns succeeded in healthcare (Figure 2).

Both are below the average of a successful compromise in every 5 to 10 attack campaigns overall. But given the sheer volume of attacks, even seemingly low success ratios reflect a large number of potentially compromised accounts. It's no wonder that more than half of all organizations overall had at least one account compromised in Q1 and more than 40% had an account compromised in Q2.

Illicit Logins: Least Vulnerable Sectors (Figure 2)

Financial Services and Healthcare were the least vulnerable to cloud account attacks.



SECTION 2 ATTACKS

Not all attacks are created equal. While every one is potentially harmful, some are more dangerous, targeted or sophisticated than others. Knowing who they target, and why, is a critical part of understanding this aspect of user risk.

Shared email aliases

Nearly 20% of email addresses that represented the highest overall risks from email* attacks were generic email accounts typically shared by or forwarded to two or more employees within an organization. Addresses such as sales@company.com and inquiries@company.com have value to attackers for three main reasons:

- They are sent to multiple victims.
- They are easy to obtain (often public-facing).
- They are harder to protect. Multifactor authentication, for instance, is difficult to configure when the email address is shared among several colleagues.

*Based on our Attack Index. See "What is the Attack Index? on page 8.

Attacking the Aliases

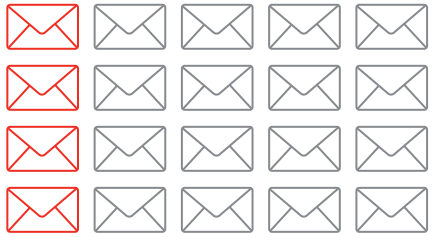
A single threat sent to an email alias can reach multiple targets.

Nearly

20%

of email addresses

that represented the highest overall risks from email* attacks were shared email aliases



*Based on our Attack Index. See "What is the Attack Index?" on page 8.

● Shared

METHODOLOGY

For insight into people-focused threats, we examined email-based malware and phishing attacks against Fortune Global 500 customers (we served more than 200 of them during the study period).

We collected the email addresses most at risk at each company, determined by our proprietary Attack Index. This number factors in the quantity, severity and sophistication of threats received. (See "What is the Attack Index?" on page 8.)

Then we matched the recipients' titles and functions using social-media profiles, internet databases, public records, news reports and other sources. We excluded email addresses of cybersecurity teams and vendors. We also noted generic email addresses likely forwarded to multiple people within a company.

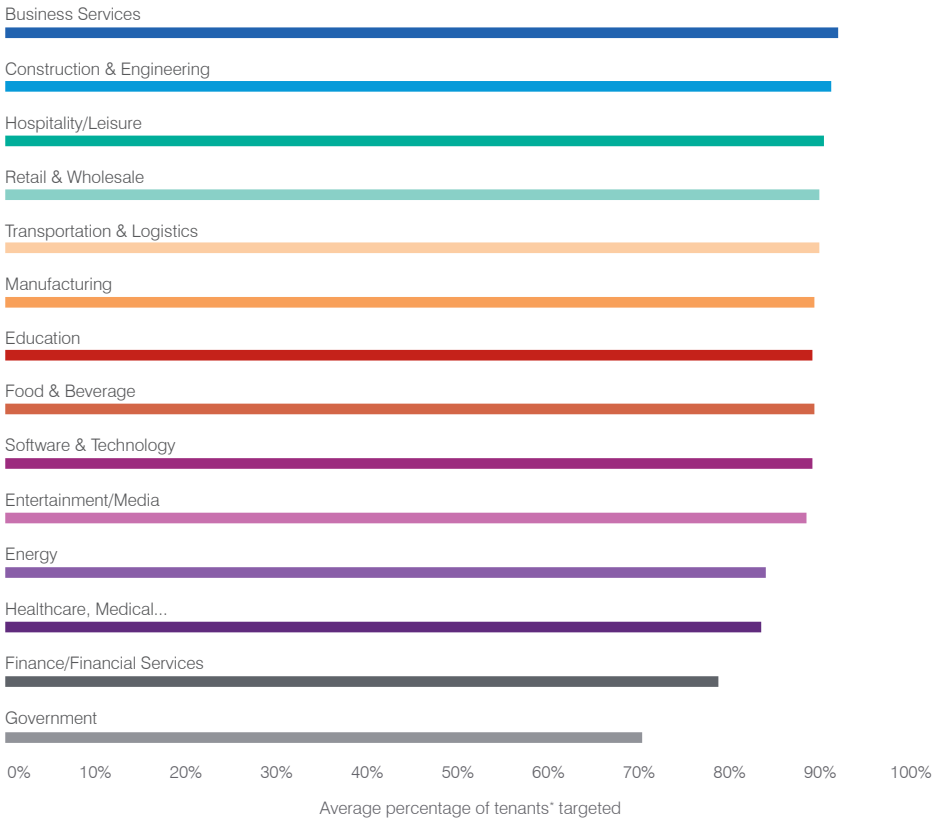
Industries targeted by cloud-based attacks

Cloud apps give organizations flexibility at a scale scarcely imaginable just a few years ago. They also provide a vast new attack surface for cyber threats. Attackers are using the cloud for everything from spam to hard-to-detect internal phishing and fraud.

In the first half of 2019, business services, construction/engineering, and the retail/wholesale sectors were slightly more heavily targeted in such attacks than other industries. But no single industry was disproportionately targeted—or spared.

Compromised in the Cloud

Business services and construction/engineering were more heavily targeted by cloud account compromise attacks than other industries.



*A tenant is cloud account subscription that may include all accounts within an organization or an individual business unit.

SECTION 3 PRIVILEGE

User privilege is another critical component of user risk.

Attackers target people at all career levels. But the potential impact of a successful attack can vary according to what data, systems and resources the user has access to.

What is the Attack Index?

The Proofpoint Attack Index quantifies users' risk based on the type and severity of threats that target them. The index assigns each threat a score of 0–1,000 based on the type of attacker, targeting and threat.

Here's how each of those attributes factors into the overall Attack Index score.

Attacker type
This attribute speaks to the attacker's level of sophistication and, in turn, risk to the organization. For example, a state-sponsored attacker gets a much higher score than a small-time cyber criminal.

Targeting type

This is a way of describing how narrowly the attack is targeted. Did the threat hit only one user or the entire planet? Was it focused on a user, company, vertical or geography? Or was it a "spray-and-pray" campaign seen by half the globe? The more targeted the threat, the higher score it gets.

Threat type

This component reflects the type of malware involved in the attack. In most cases, the malware used in an attack can reveal how severe the threat is or how much effort the attacker put into it. A remote access Trojan (RAT) or stealer, for example, gets a higher score than a generic consumer credential phishing attempt.

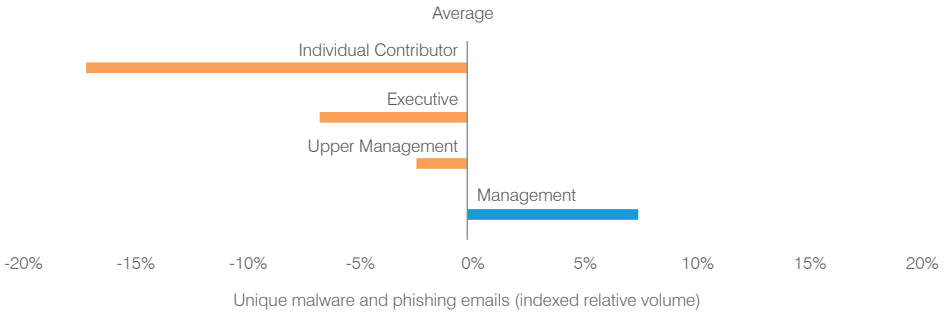
VAPs aren't always VIPs

Overall, VAPs at every rung of the corporate ladder are at a roughly equal risk of email-based malware and phishing attacks. Across the board, Attack Index scores fell within one or two percentage points of the overall VAP average.

But VAPs in lower-management roles saw nearly 8% more phishing and malware attacks than the average VAP. The split suggests that attacks targeting these VAPs were higher volume but lower risk than those targeting both higher- and lower-level VAPs.

Malware and Phishing Attacks

VAPs in lower-level management roles saw the highest volume of malware and phishing attacks on average.



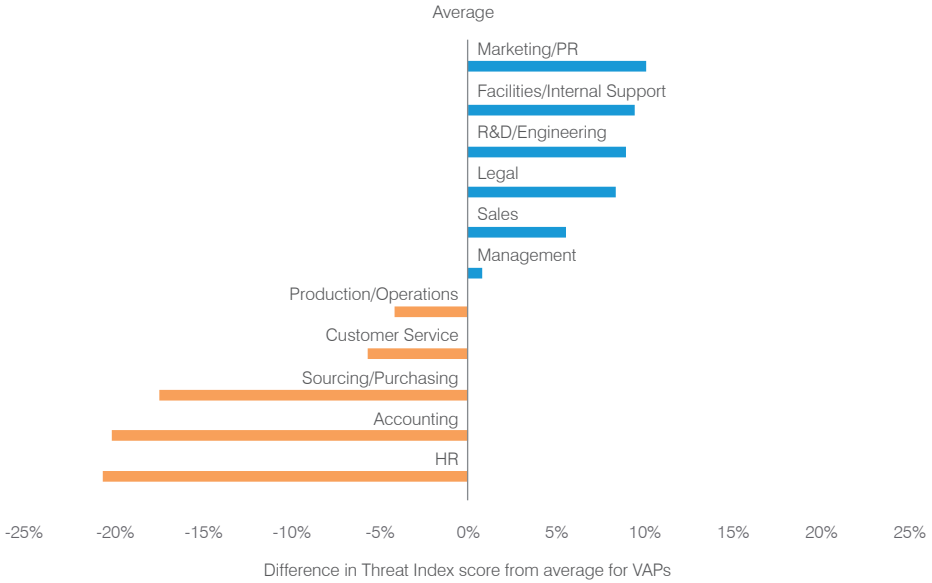
Some departments are more targeted than others

By department, workers in marketing/public relations functions represented the highest overall risk from malware and phishing, followed closely by facilities/internal support (which includes IT workers) and R&D/engineering. The Attack Index score for all three groups was about 9% higher than that for the average VAP.

Email addresses in the marketing/PR category may be bigger targets simply because they are more readily accessible. Public relations professionals often include their full name, email address and other contact information in press releases and newsroom sections of company websites. And marketing professionals often promote themselves on social media and other digital channels. In our research, email addresses both sectors were much easier to match to the person they belong to than those in most other categories.In either case, compromising these accounts can be stepping stone to gaining broader access to the targeted organization.

Very Attacked Targeted Departments, by Overall Risk

VAPs in marketing and PR represented the highest overall risk from email-based malware and phishing attacks. They were followed closely by facilities and R&D/engineering functions.

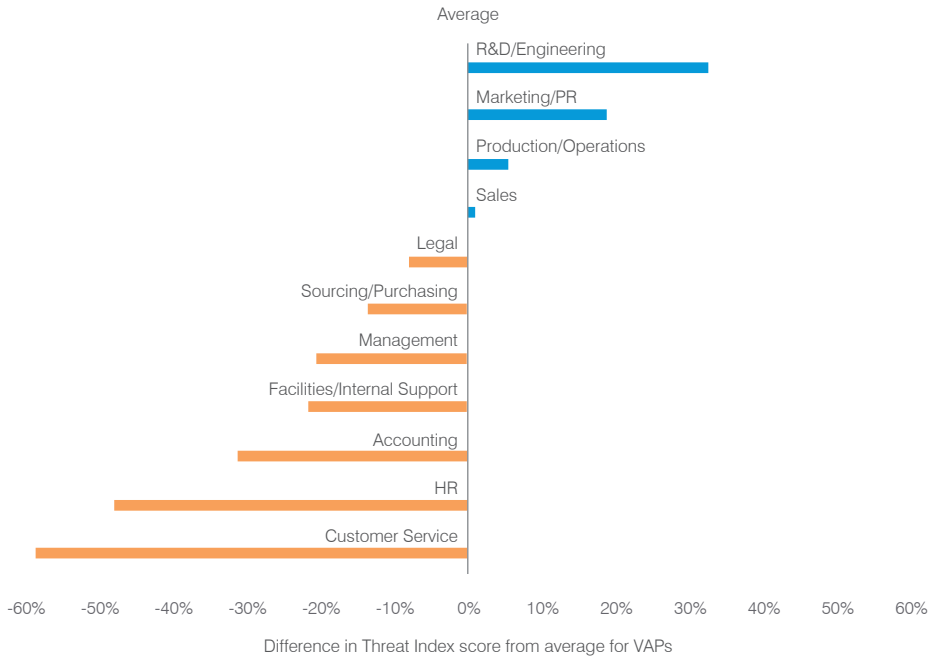


Comparing attack volumes tells a slightly different story. Marketing/PR and R&D/engineering faced a volume of malware and phishing attacks that mostly coincided with their overall Attack Index score. But facilities/internal support workers, No. 2 in terms of overall risk from malware and phishing attacks, saw 23% fewer attacks than the average VAP (Figure 3).

The discrepancy suggests that attacks on this group included more sophisticated or narrowly targeted threats than other groups.

Very Attacked Departments, by Attack Volume

Facilities/internal support workers were among those at the highest overall risk based on attack index scoring* but saw 23% fewer malware and phishing attacks than the average VAP.

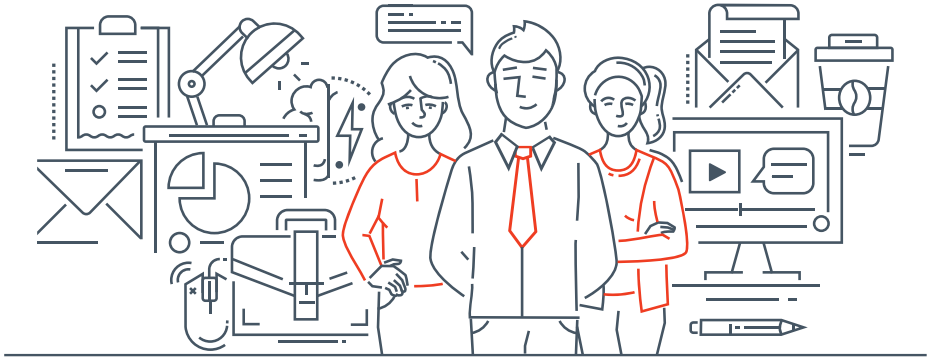


*Based on our Attack Index. See "What is the Attack Index?" on page 8.

Cloud attacks by job role

Across all sectors, sales representatives and managers were among the most highly targeted users. The nature of their roles makes them easier to reach; they often must respond to unsolicited emails, exposing them to more phishing attacks.

Salespeople are also in frequent contact with people in finance departments and external organizations. So an attacker who compromises a sales rep's account can use it to target the victim's supply-chain partners and colleagues who have access to critical data and resources.



CONCLUSION AND RECOMMENDATIONS

Today's threats require a people-centric approach. We recommend the following as a starting point:

Adopt a people-centered security posture.

Attackers do not view the world in terms of a network diagram. Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.

Train users to spot and report malicious email.

Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into current trends and the latest threat intelligence.

At the same time, assume that users will eventually click some threats.

Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. And stop outside threats that use your domain to target customers.

Build a robust email fraud defense.

Email fraud can be hard to detect with conventional security tools. Invest in a solution that can manage email based on custom quarantine and blocking policies. Your solution should analyze both external and internal email—attackers may use compromised accounts to trick users within the same organization.

Isolate risky websites and URLs.

Keep risky web content out of your environment. Web isolation technology can render web pages from suspicious and unverified URLs in a protected container within users' normal web browser. Web isolation can be a critical safeguard for shared email accounts, which are difficult to secure with multifactor authentication. The same technology can isolate users' personal web browsing and web-based email services, giving them freedom and privacy without compromising the enterprise.

Protect your brand reputation and customers in channels you don't own.

Fight attacks that target your customers over social media, email, and the web—especially fake accounts that piggyback on your brand. And look for a complete social media security solution that scans all social networks and reports fraudulent activity.

Partner with a threat intelligence vendor.

Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics, and targets—and then learns from them.

LEARN MORE

Learn how Proofpoint can help you protect your people against today's biggest cyber threats at **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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 cyber attacks. 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. More information is available at www.proofpoint.com.

proofpoint.

0719-015