proofpoint®

CLOUD COVER

MANAGING NEW SECURITY RISKS IN OFFICE 365 AND BEYOND

INTRODUCTION

Office 365 is a big part of a digital transformation that's changing the way we work, collaborate and create. It's a whole new way of doing business. And it comes with a whole new set of risks.

For many IT leaders, the move to Microsoft's cloud-based software platform will prove a career-defining project that will mean the difference between evolving their business or overseeing its stagnation.

The average enterprise uploads about 1.37 terabytes of information to Office 365 every month.[1] More than 17% of Office 365 documents contain sensitive information—including personally identifiable information, financial statements, business plans, and source code.[2]

But migrating to Office 365 doesn't just move your email and your data to the cloud. It also moves your threats. That's why keeping your data safe requires not just new tools, but a whole new mindset.

This e-book describes how Office 365 is changing the workplace, the new security challenges that come with it, and what you can do about them.

[1] Tara Seals (Infosecurity Magazine). "Microsoft Office 365 Increasingly Used for Sensitive Info." July 2015.
[2] Ibid.

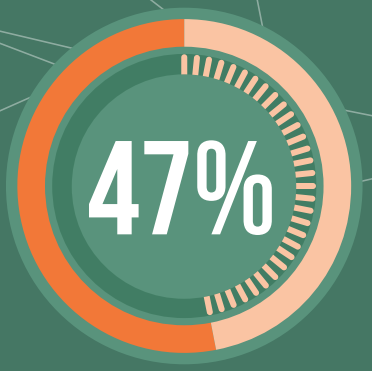
BUSINESS, TRANSFORMED

"If your organization is not embracing digital transformation, it won't be around much longer," said Dave Michels, a principal analyst at the research firm TalkingPointz. "There's simply nothing more important for organizational survival than digital transformation."[3]

Michels is not alone in his assessment. Digital transformation is already reshaping worker collaboration, business processes, and customer engagement. And in many cases, the impetus is coming from the top.

According to a recent Gartner survey, 47% of CEOs are being pushed by their board of directors to make progress in their digital business. And 56% say their digital efforts have already improved profits.[4]

Digital transformation is making workplaces more flexible. It's empowering workers. And it's reducing barriers to teamwork on a global scale.



of CEOs are being pushed by their board of directors to make progress in their digital business

of CEOs say their digital efforts have already improved profits

[3] Dave Michels (Enterprise Connect). "Digitally Transform…or Else." July 2017.

[4] Gartner. "Gartner Survey Shows 42 Percent of CEOs Have Begun Digital Business Transformation." April 2017.

ANYWHERE, ANYTIME EMPOWERMENT

Knowledge workers aren't the only beneficiaries of digital transformation. Workers in old-line industries are growing empowered with the tools and insight they need to act when it counts.

Consider Aston Martin, the luxury auto brand known as the carmaker of choice for fictional British Secret Service agent James Bond 007. The company uses Office 365 to better connect teams and departments. The platform is a big part of its plans to roll out seven new car models over the next seven years, the fastest development cycle in its 100-year history.[5]

"Things are going to happen by empowering passionate people to change the whole tempo of the company and the whole culture of the company," said Andrew Palmer Aston Martin's CEO, in a promotional video for Office 365. "Collaboration is a culture."[6]

[5] Angus Mackenzie (MotorTrend). "Second Century Plan: Aston Martin to launch 7 new models in 7 years." August 2017.

[6] Microsoft. "Aston Martin—Tools of the Trade." September 2017.

> “WE HAVE A DIVERSE GLOBAL COMMUNITY FEELING LIKE THEY ARE JUST NEXT DOOR WHEN YOU PICK UP THE PHONE OR SET UP A VIDEO CONFERENCE”
>
> – Jayson Style, Project Manager, BBC Media Action

GLOBAL COLLABORATION

In a global economy, companies have little room for silos, whether they’re by team, department, or region. So it’s no surprise that seamless global collaboration is a huge driver of many digital transformation efforts.

The time managers and employees spend in collaborative activities has ballooned by 50% or more over the last two decades, the Harvard Business Review estimates.[7]

BBC Media Action, BBC’s international development charity, recently migrated to Office 365. It uses the platform so that its more than 800 employees can more easily work together across 17 countries.

“We have a diverse global community feeling like they are just next door when you pick up the phone or set up a video conference,” said Jayson Style a project manager for the charity, in a case study.[8] The organization operates in Africa, Asia, Europe and the Middle East.

Without the right technology, physical resources, and structure, collaboration can become more of a drain than a gain. And without trusted, reliable connections, csollaboration beyond the physical office just doesn’t happen.

[7] Rob Cross, Reb Rebele, and Adam Grant (Harvard Business Review). “Collaborative Overload.” January 2016.

[8] Fujitsu. “Customer Case Study: BBC Media Action.” December 2016.

SECURITY RISKS: HOW ATTACKS TARGET PEOPLE

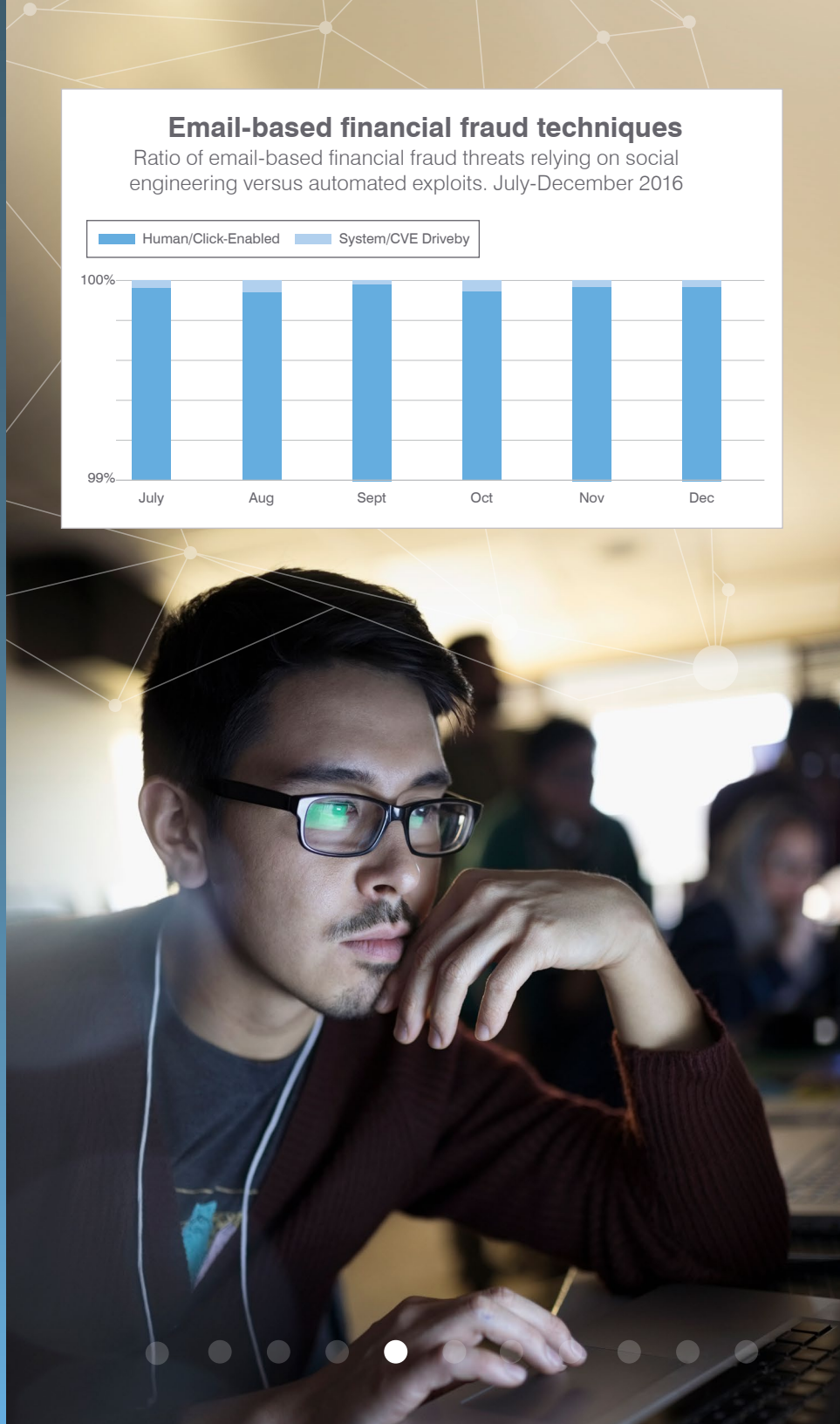
The shift to Office 365 highlights a growing trend in cyber threats: today's attacks target people, not just technology. Even the best-secured cloud and SaaS apps are vulnerable to threats that target the weakest link in today's mixed environments: the human factor.

HUMAN-ACTIVATED MALWARE

Most data breaches start with an email.[9] And most email attacks rely on a person to activate them, either by opening a boobytrapped attachment or clicking a link to malicious code.[10]

The Locky strain of ransomware, for instance, started with a Microsoft Word document disguised as an invoice. Embedded in the document was a malicious macro file. For the ransomware to run, the victim needed not just to open the document, but explicitly enable the macro by dismissing the usual pop-up warnings.

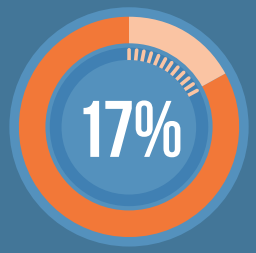
The email tricked recipients into enabling the macro by displaying gibberish in the document and instructing the reader to "Enable macro if data encoding is incorrect." That bit of social engineering overcame any hesitation the user might have after reading Microsoft's usual security warning.



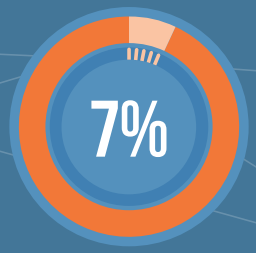
[9] Verizon. "Data Breach Digest (2017)." April 2017.
[10] Proofpoint. "The Human Factor 2017." May 2017.

MOST POPULAR BEC SUBJECT LINES

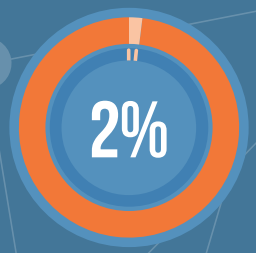
= Request



= Urgent



= Bank



= FYI

EMAIL FRAUD

Email fraud—also known as impostor email or business email compromise (BEC)—is another kind of attack that gets through otherwise well-protected email systems. Email fraud relies solely on human engineering.

Email fraud is hard to catch, even with Office 365's built-in security tools. That's because it is sent in low volumes. There's usually no payload to sandbox, no URL to check, and no reputation to look up. These attacks target workers using manipulation alone.

A fraudulent email appearing to come from the CEO asks your CFO to wire money. Your finance manager receives new account information from what seems to be a legitimate vendor. An HR colleague gets a request from her "boss" for employee tax records.

CREDENTIAL PHISHING AND ACCESS ABUSE

Cloud apps are only as secure as the people who have access to them. As organizations move to the cloud, stolen credentials provide anywhere-access for attackers. By hijacking the right accounts, attackers have free reign of your data and deep insight into your business processes, which helps them launch other targeted attacks.

It's no wonder that stolen credentials are both the top attack method for threats against cloud apps—and conversely are one of the top objectives in such attacks.[11]

That's why protecting your data also means protecting access to it.

[11] Verizon. "Data Breach Investigations Report 2017." June 2017.

UNSAFE ADD-ONS

As SaaS applications become mainstream, they're quickly becoming the new frontier of IT consumerization.

Their ubiquity has fueled the growth of SaaS app stores such as Microsoft's AppSource. These marketplaces offer a wide range of third-party apps that connect with users' SaaS deployment for added features and capabilities—often without the direct involvement of the users' IT department.

According to our research, more than half of all enterprise workers use third-party apps that connect into their organization's cloud services. The workers install three third-party apps on average, and 25% of these apps access their organization's email and files.

Even well-protected SaaS infrastructures can be compromised by advanced social-engineering schemes.

Mainstream cloud app vendors such as Microsoft and Google strive to secure your data. They set up and enforce technical and procedural data security controls to limit employee access to corporate data.

[11] Verizon. "Data Breach Investigations Report 2017." June 2017.

EVEN WELL-PROTECTED SAAS INFRASTRUCTURES CAN BE COMPROMISED BY ADVANCED SOCIAL-ENGINEERING SCHEMES.

UNSAFE ADD-ONS (continued)

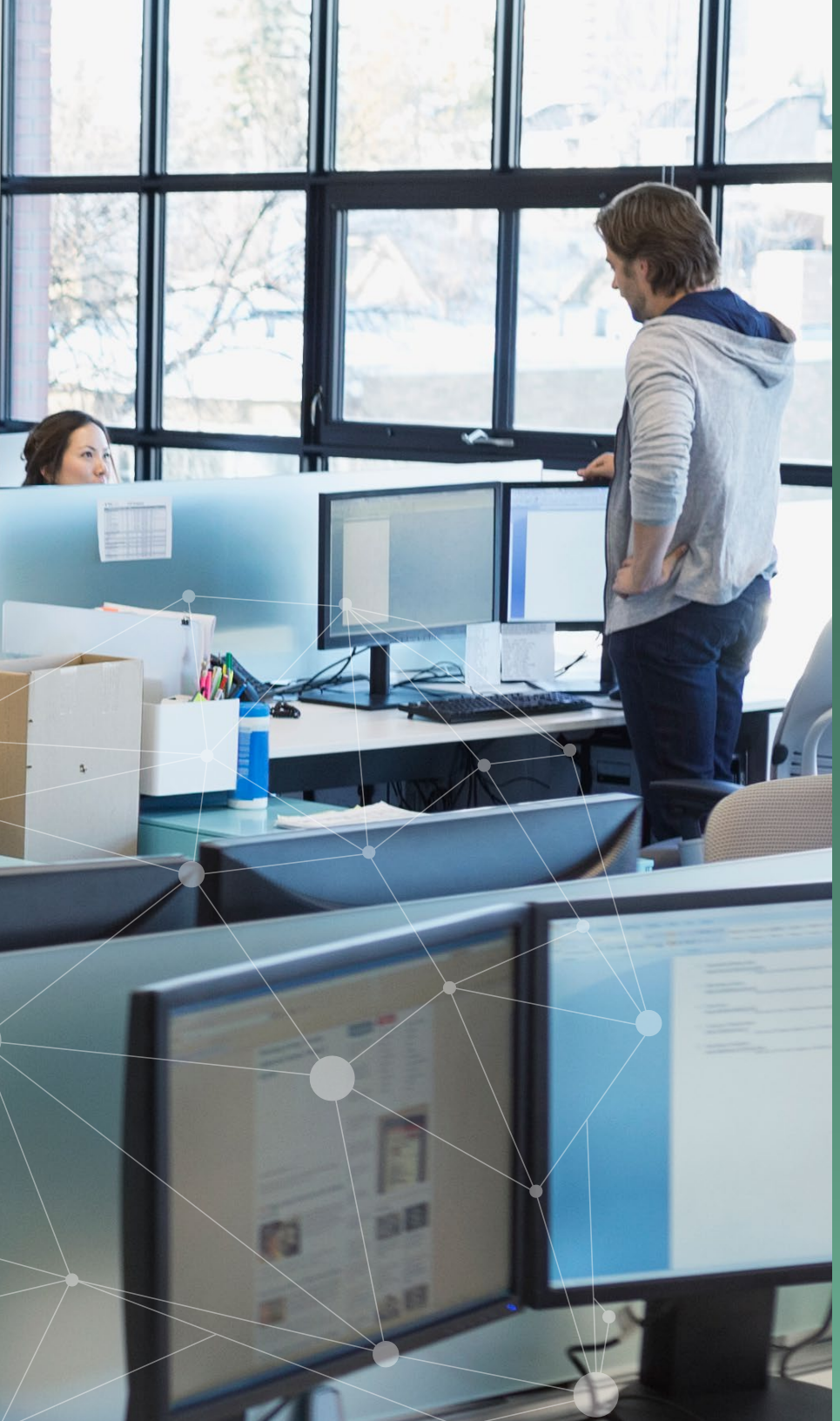
That's not the case with many third-party apps. Often, these apps do not provide a security policy. As it extracts your data into its own environment—even if temporarily—your data now resides in an environment that is unlikely to match up to the rigorous standards of the mainstream SaaS app vendor it connects into.

Worse, your risk does not stop at overtly malicious apps. Often, and without your explicit consent, third-party apps misuse or abuse your permission grants.

Some permissions are benign and even necessary. An app might copy your data into its own servers, because it needs to send push notifications to the user's mobile email client. You might see it collect your prospect's data, because it needs to upload a business card as a sales lead.

But many third-party apps with hidden motives misuse this access or treat it carelessly. Usually these rogue apps are driven by financial gain, such as selling your prospect's information to a spam list.

With or without your users' consent or knowledge, these apps can put your organization's data, users, privacy, and compliance at risk.



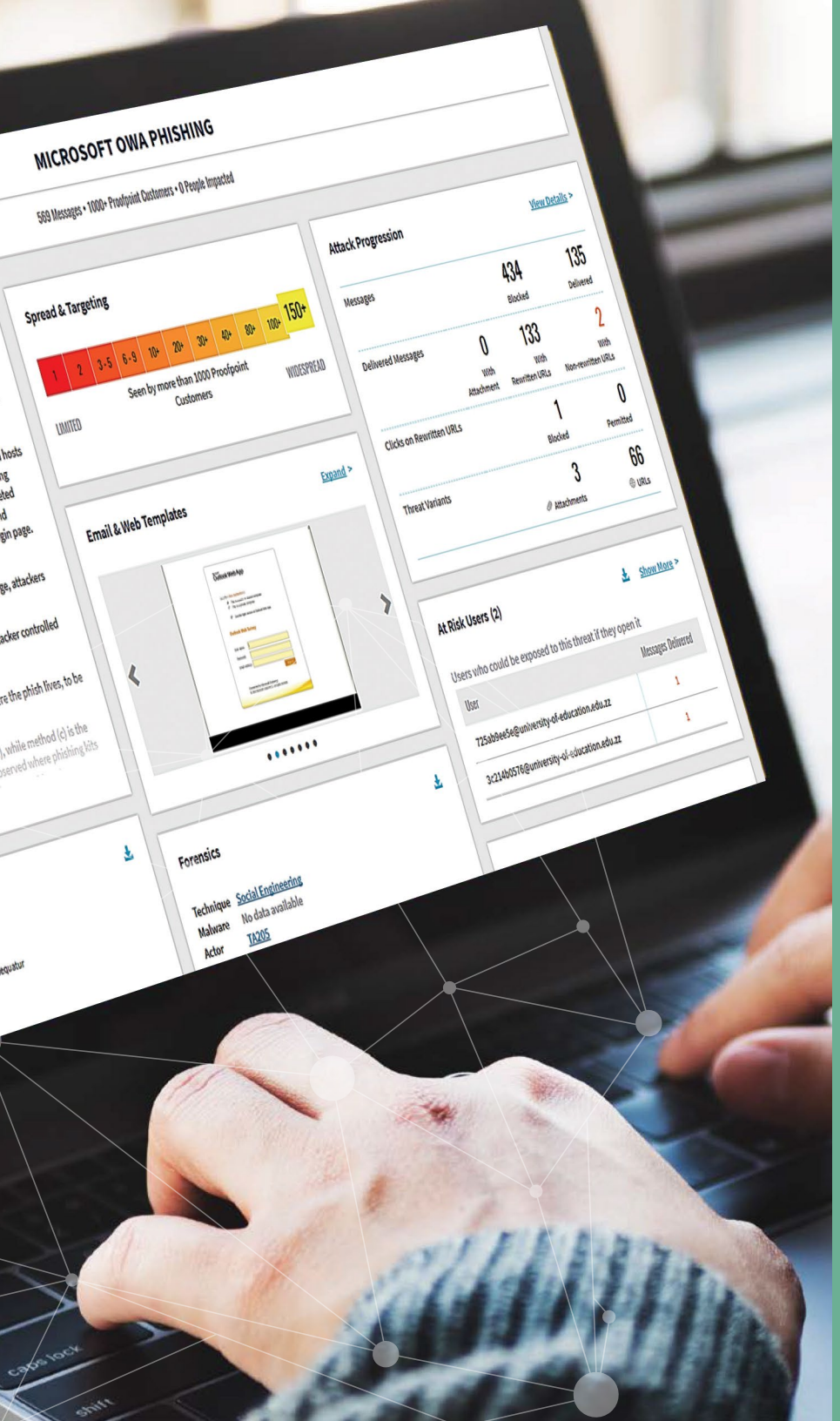
SECURITY THAT WORKS ACROSS ALL THE INFRASTRUCTURE YOU RELY ON

Cloud-based productivity and SaaS apps make it easy to connect workers around the globe. But they're only as secure as each service provider chooses to make them.

The one-size-fits-all defaults of popular cloud platforms such as Office 365 and G Suite may not be suited to your organization's unique security challenges.

"Technology vendor management leaders are challenged to manage the proliferation of niche cloud-focused and digital business vendors," says analyst firm Gartner. "[Which] are threatening the consistency of vendor performance and increasing risk."[12]

[12] Luke Ellery (Gartner). "Six Key Steps to Developing Effective Vendor Management Governance." April 2017.



A NEW APPROACH TO NEW RISKS

A modern security solution must offer broad, coordinated, omnichannel protection against today's most advanced threats. That means it must prevent, detect, and stop threats that exploit not just technical flaws, but human nature. And it must work everywhere your organization does.

An effective defense is one that can learn from every attack, adapt quickly, and anticipate future threats. Broad-ranging threat intelligence that helps connect the dots of an attack is critical. It should help determine who's attacking, what methods and tools they're using, and what they're after.

And because no security tool can catch all threats, your defense should help you respond quickly when something gets through. Automating forensics and intel-gathering can help your security team ignore false alarms, prioritize true threats, and stop attacks before they cause lasting harm.

proofpoint™

LEARN MORE

To learn more about how Proofpoint can make your move to Office 365 successful, visit proofpoint.com/office365

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.