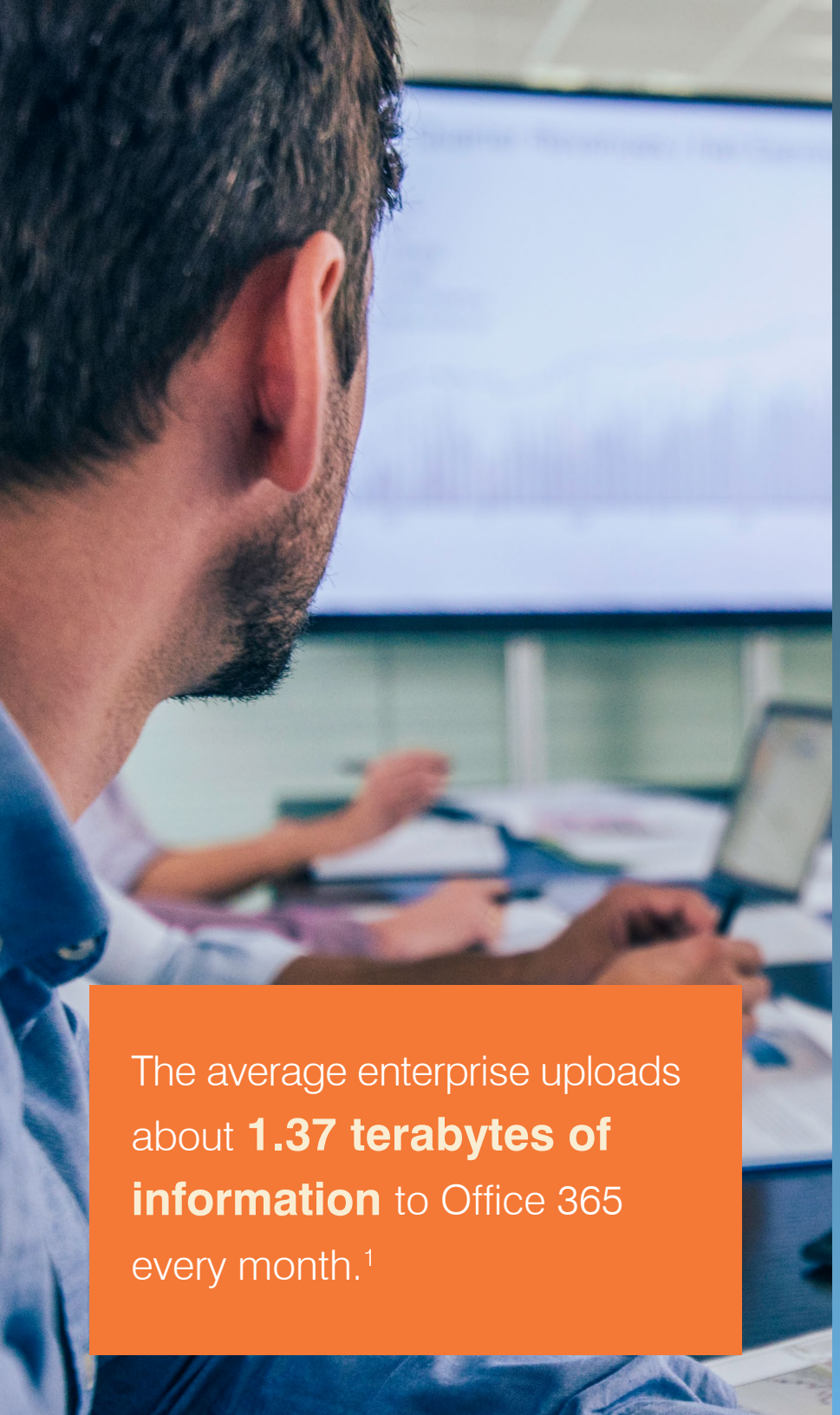
proofpoint®

MOVING THE GOALPOSTS

HOW OFFICE 365 CHANGES COMPLIANCE— AND WHAT YOU CAN DO ABOUT IT



The average enterprise uploads about **1.37 terabytes of information** to Office 365 every month.[1]

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. The success of this shift 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 change your email and your data infrastructure. It also changes the way you must think about compliance.

The cloud makes some aspects of compliance easier. Microsoft's infrastructure is highly secure and complies with numerous rules, standards and laws when storing and processing your data.

But the cloud complicates other aspects of compliance. The way you create, process and use data must also comply with an ever-growing set of rules. And that grows more difficult with every new cloud platform, collaboration tool and sharing service.

With the cloud, compliance requires not just new tools, but a whole new mindset.

This e-book describes how Office 365 is changing the workplace, the new compliance 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

In today's digital economy, your success hinges ever more directly on your ability to transform your business.

"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.

It's no wonder that an estimated 60% of organizations are knee-deep in major system and technology upgrades to get closer to customers through their supply chains.[5] That's despite lingering concerns over security and compliance.[6]

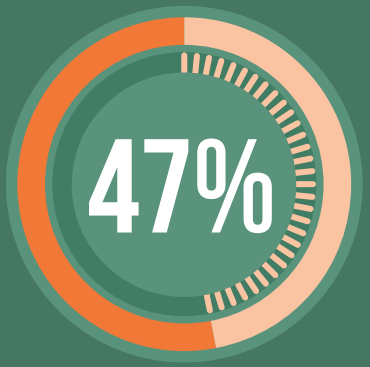
[3] Dave Michels (Enterprise Connect). "Digitally Transform…or Else." July 2017.

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

[5] Inbound Logistics. "Supply Chain Report: Why Suppliers Hold Back." June 2017.

[6] Ibid.

ACCORDING TO GARTNER



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

Photo credit: Mike Strand, licensed under Creative Commons Attribution 3.0 Unported license.

"WE'VE TRANSFORMED OUR STORES THROUGH TECHNOLOGY BY GIVING OUR LEADERS ALL THE COMMUNICATION, INFORMATION AND DATA THEY NEED AT THEIR FINGERTIPS, WITHOUT TETHERING THEM TO A DESK"[7]

–Sue McMahon, Macy's group vice president of retail communication

ANYWHERE, ANYTIME EMPOWERMENT

Retail giant Macy's uses Office 365 to empower leaders at individual stores with real-time data that helps them make decisions on the fly.

"We've transformed our stores through technology by giving our leaders all the communication, information and data they need at their fingertips, without tethering them to a desk," said Sue McMahon, the retailer's group vice president of retail communication.[7]

BOLDLY GOING BEYOND THE ENTERPRISE

Unlike traditional IT infrastructure, the cloud was built for connecting to the outside world. Today's hybrid IT architectures makes collaborating with vendors, partners, customers easier than ever.

Ad-hoc teams can quickly assemble across departments, regions and even organizations to solve a problem on the spot. Businesses can digitize processes to automate manual tasks and free up their best people for more strategic projects. And complex supply chains can link to one another to detect and resolve emerging issues weeks before they become problems.

The result: business that is much more responsive to market changes, shifting customer needs and tastes, and global events.

GLOBAL COLLABORATION

Henkel, a 141-year-old consumer goods giant, touts Office 365 as a big part of its efforts to improve business cohesion and agility.

"Our people can work faster, more effectively and they can collaborate much better," said Markus Petrak, the company's corporate director. "People share documents just by a click. We can form project teams much faster. People can connect to each other wherever they are."[8]

[7] Sue McMahon (writing for the Microsoft Office 365 blog). "Macy's sets the standard for empowering employees using Office 365." November 2016.

[8] Markus Petrak (Henkel). "Henkel advances digital transformation journey with move to Office 365 E5." November 2017.

NEW ARCHITECTURE, NEW RISKS

But digital transformation isn't just changing the way people work. It's changing the nature of business risk.

Modern infrastructure is more complex and fragmented than ever, leaving potential compliance gaps. Regulated data may sit on dozens of different cloud and SaaS platforms. And they may all have different discovery, protection, archiving and retention capabilities.

The loosely knit, adaptable architecture helping to transform business operations also means new kinds of compliance risks.

In this environment, your email might live on Microsoft Office 365. Your sales customer-relationship management (CRM) software might run on a SaaS environment such as Salesforce.com. And you probably engage customers through social-media platforms such as Twitter and Facebook.

SECURITY RISKS ARE COMPLIANCE RISKS

You can't discuss compliance without considering security. Virtually every compliance rule requires monitoring and protecting sensitive data.

Frictionless collaboration, one of the biggest benefits of Office 365 and the cloud, also means fewer barriers to unsanctioned access and accidental sharing.

RISKY CLOUD APPS AND ADD-ONS

Office 365 and add-on apps make it easy to connect workers around the globe. But they're only as secure and compliant as each app publisher chooses to make them.

Office 365 add-ons from Microsoft's AppSource market, for instance, make it easy for users to enable more features. But it also gives the app developers—including those with malicious intent—potential access to data hosted in Office 365.

This outside access to files, email and data creates obvious privacy issues.

WHAT IS COMPLIANCE, ANYWAY?

In a broad sense, business compliance means abiding by any laws or standards that govern the way you capture, use, store and dispose of data.

Compliance rules can cover everything from customer privacy to legal requests to employee communications. Achieving compliance often includes being able to prove you're compliant.

Today's businesses fall under numerous, often overlapping, guidelines and governing bodies—PCI, HIPAA, GDPR, FINRA, SEC and countless others. But most rules fall under two categories:

- Protecting sensitive data from falling into the wrong hands
- Ensuring that important data is properly captured, retained, made available when needed, and disposed of properly

Digital transformation is making both more difficult in two critical ways. It's increasing the number of points where data is shared. And it's expanding the types of data that must captured or monitored for supervision.

In **63% of attacks that use legitimate credentials** to access sensitive data, it **takes months or years to detect** the breach.[9]

COMPROMISED CREDENTIALS

It's an old security truism: your credentials are the keys to the kingdom. As infrastructure moves to the cloud, compromised credentials can cause even more headaches.

In 63% of attacks that use legitimate credentials to access sensitive data, it takes months or years to detect the breach.[9]

In September 2017, for instance, security researchers uncovered an email fraud scheme in which attackers stole companies' Office 365 credentials. Using the compromised accounts, the attackers sent emails to people within the same firm. They exploited the trust of unwitting recipients that the emails were from a colleague they know.

For every compliance issue companies know about, countless others go unrecognized because compliance tools can't see them.

Organizations often ask Proofpoint to assess potential security and compliance issues. In one case, we found that college administrator's account was logged in from the anonymous Tor network. Given the non-technical nature of account holder's job, the security team quickly deduced that the person's credentials had been compromised.

[9] Verizon. "Data Breach Investigations Report." April 2017. This figure includes insider attacks by employees.

SHARING MADE EASY. TOO EASY.

OneDrive, Box and other cloud file-storage services let users share files to anyone in the world at the click of a button. For siloed departments spread across far-flung geographies, this frictionless collaboration can be empowering.

It can also put your compliance at risk. In one of our risk assessments, we found that a high-ranking IT executive had accidentally shared more than 10,000 internal files publicly. File-sharing interfaces may show that a folder is being shared, but to whom and how widely is not always obvious.

COMPLIANCE CHALLENGES IN THE CLOUD ERA

Securing data is only part of the compliance challenge. You also must collect, store, archive and retain it according to the laws and standards that apply to you.

Today's compliance solutions must go deep. They must dig into the details. The require a mature and working understanding of the rules and advanced approaches to addressing policies.

The one-size-fits-all defaults of Office 365 may not be suited to your unique compliance challenges.

AN EXPLOSION OF DATA—AND DATA SOURCES

In the past, employees generated records from a handful of sources—email, files and documents, and perhaps the occasional database record.

With new forms of cloud apps, social media, and messaging apps, compliance now requires dealing with hundreds of sources.

Most of Office 365's compliance features are limited to that platform. That leaves enterprises with no easy way to apply consistent recordkeeping, e-discovery, and supervision policies across all of the digital channels their workers use.

According to IT experts, Office 365 also does not provide a unified compliance experience.

"Instead, there is an ever-changing roster of capabilities that differ by product and product version," writes Osterman Research. "This creates unnecessary complexity and risk in an area already fraught with enough business risk and operating stress."[10]

CLASSIFICATION THAT HASN'T KEPT UP

Fast, easy, accurate classification is the bedrock of streamlined compliance. Knowing what information belongs to which compliance category was never easy. In the cloud era, it's even harder, often calling for a custom integration to each source.

Office 365 supports some of the basic methods of classification such as regular expressions and dictionaries. But without more advanced classification abilities, it can create a mountain of false positives and needless work.

[10] Verizon. "Data Breach Investigations Report." April 2017. This figure includes insider attacks by employees.

A NEW APPROACH: COMPLIANCE FOR MODERN BUSINESS

Regulated industries must comply with ever-changing rules—even if your infrastructure provider doesn't. That's why today's cloud and hybrid environments and new digital channels call for a new, people-centered approach to compliance.

TAKING A PEOPLE-CENTERED VIEW OF RISKS

Today's attacks target people, not just technology. Staying secure and compliant means taking into account the individual risk each user represents.

Some people in your environment might have access to your most sensitive information but have diligent security habits, such as knowing not to click unsafe URLs or open attachments. Others might have less access but pose a higher overall risk because they access email and files from unknown devices or open every email they receive.

TAKING A PEOPLE-CENTERED VIEW OF RISKS (continued)

In other words, a people-centered approach treats people as individuals. Some users may need to log back in if accessing their Office 365 account from a different device. Others may need to reenter their second authentication factor more often.

People-centered security and compliance also means correlating a broad array of risk factors to manage access for your people and the third-party add-on apps they use.

Unusual behavior on an account with no access to sensitive information, for instance, might be a cause for concern. But the same behavior on an account with higher permissions or access to more sensitive data should trigger a more urgent alarm.

TAKING THE GUESSWORK OUT OF COMPLIANCE

In today's cloud and hybrid infrastructures, knowing where your data is, who has access to it, and how it's being used is more complicated than ever.

Compliance and security tools should automatically keep sensitive data out of the wrong hands. They shouldn't hinge on manual slogs or split-second judgement calls by your staff. And your data should stay safe whether you've been breached or someone accidently emails or over-shares confidential information.

Automated, policy-based access control, encryption, and simplified data retention, e-discovery, and review can free up workers to do what they do best.

EFFECTIVE COMPLIANCE MEANS ENSURING THAT YOUR RECORDKEEPING, E-DISCOVERY AND SUPERVISION EFFORTS COVER ALL THE CHANNELS YOU USE.

COVERING ALL THE CHANNELS THAT MATTER

In today's digital economy, people do business on multiple channels—inside Office 365 and beyond it. Effective compliance means ensuring that your recordkeeping, e-discovery and supervision efforts cover all the channels you use.

Many e-discovery requests, for instance, require all business communications, not just those within Office. Satisfying those discovery requests in a timely and complete manner can be difficult with Office 365 alone.

Only a compliance solution with deep, broad visibility into your data can capture, protect, and retain all the data you're responsible for—and in an audit or legal scrutiny, prove you did it all properly.

PUTTING IT ALL TOGETHER

To harness the benefits of digital transformation, your compliance approach must give you visibility and control over your data on and off premises. It should protect the way they work—everywhere they log in, every device and platform they use, and every channel on which they communicate. And it should empower workers by taking the guesswork out of compliance.

Above all, people should be at the center of your compliance efforts.

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.