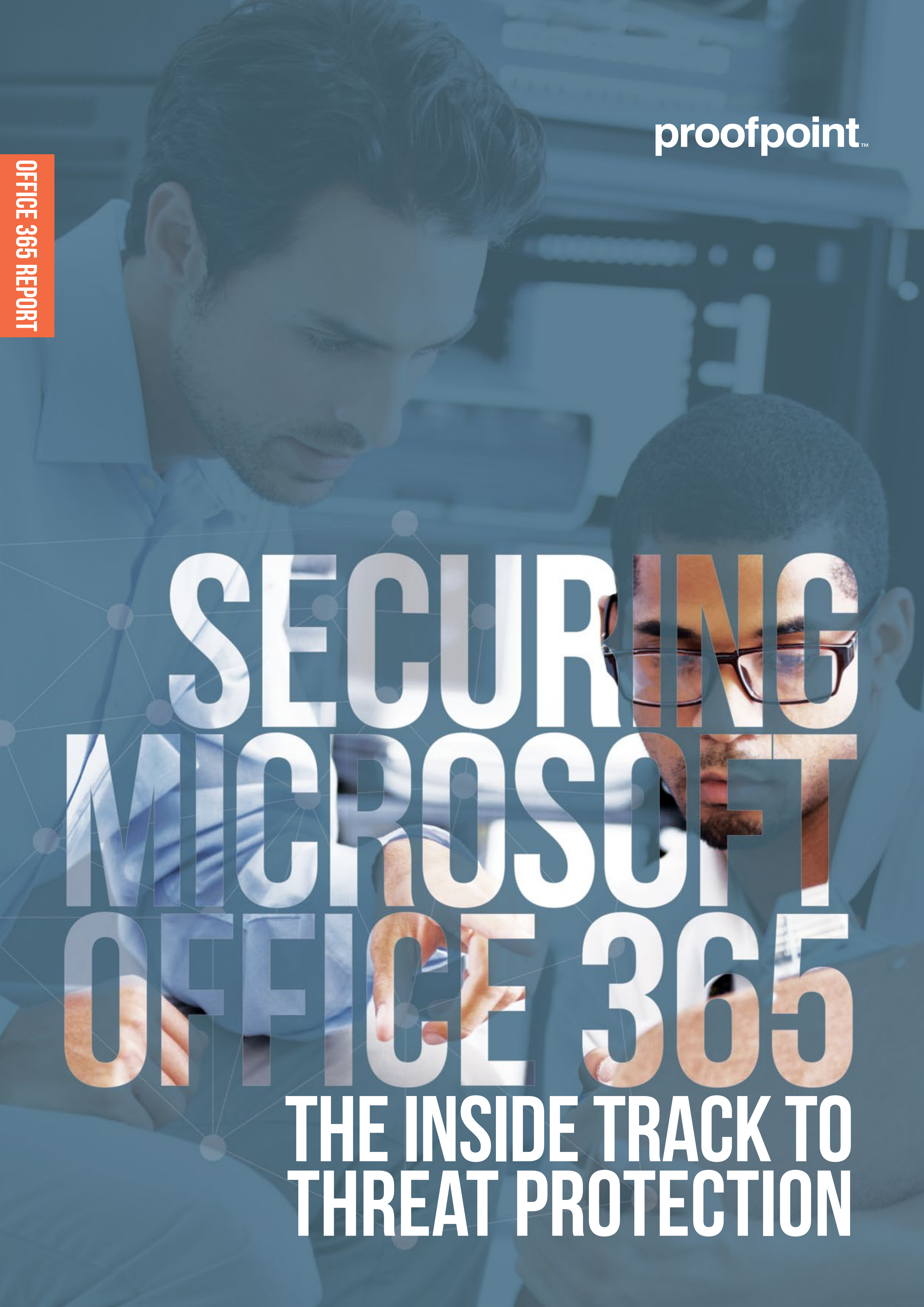


OFFICE 365 REPORT

proofpoint

# SECURING MICROSOFT OFFICE 365

## THE INSIDE TRACK TO THREAT PROTECTION

# TABLE OF CONTENTS

# SECURING MICROSOFT OFFICE 365

## 1. INTRODUCTION

Cloud is now a part of mainstream enterprise IT strategy. The benefits—flexibility, cost savings, rapid innovation and productivity gains—are simply too great to ignore.

But security is rightly front of mind for senior IT decision-makers in making this shift. The cloud brings challenges in opening up new vectors of attack and potentially putting confidential and valuable corporate data and assets at risk. Nowhere is this more critical than with transition to the cloud of one of the most popular productivity suites—Office 365.

Email remains a key target for attackers who rely on sophisticated social engineering techniques and the fallibility of employees to infiltrate networks with both malware-free and malware-based attacks such malicious URLs and attachments in emails. That's according to various research including the most recent Verizon Data Breach Investigations Report.

That puts Office 365 squarely in the sights of attackers. has built a pretty robust security foundation into Office 365 but most large organisations will want the reassurance of an additional layer of protection on top of that to fit with their own wider organisational security posture and requirements.

The respondents in this Proofpoint survey come mainly from UK organisations with 4,000 or more employees ranging from FTSE 100 corporations, major banks and high street retailers to NHS Trusts and local authorities. We asked senior IT decision-makers—from CEOs and CIOs to IT security managers—in those organisations about the security issues around Office 365.

In this report we will explore Office 365 adoption trends concerns around issues such as threat protection, intelligence and response. We will then recommend what additional security measures organisations can take to securely deploy Office 365 and reap its full benefits.

## CLOUD AND OFFICE 365 GO MAINSTREAM FOR UK ORGANISATIONS

**The benefits—flexibility, cost savings, rapid innovation and productivity gains—are simply too great to ignore.**

### Does your company currently use cloud-based applications?

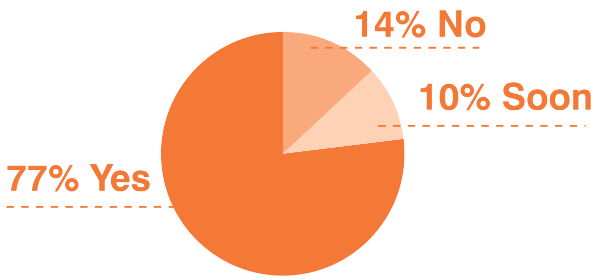


Figure 1: Does your company currently use cloud-based applications?

Our survey shows the scale of the move to embrace cloud computing as a mainstream part of IT infrastructure and for the delivery of applications to end users. More than three-quarters of respondents are currently using cloud-based applications.

### Have you implemented Office 365 in your organisation?

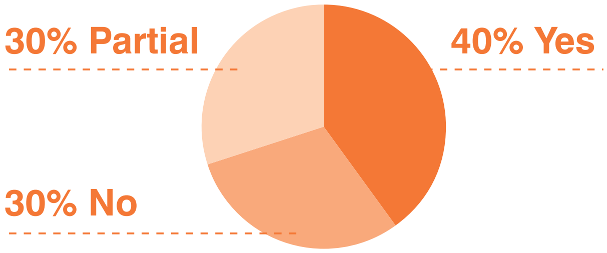


Figure 2: Have you implemented Office 365 in your organisation?

Our survey also shows just how fast organisations are moving to Microsoft's cloud-based Office 365 platform. More than two-thirds of respondents have already implemented Office 365 or are in the process of rolling it out, while the remainder plan to do so in the near future.

That has huge implications for IT security, which many organisations are not fully aware of.

## 2. THE SECURITY RISKS AND CHALLENGES OF MOVING TO OFFICE 365

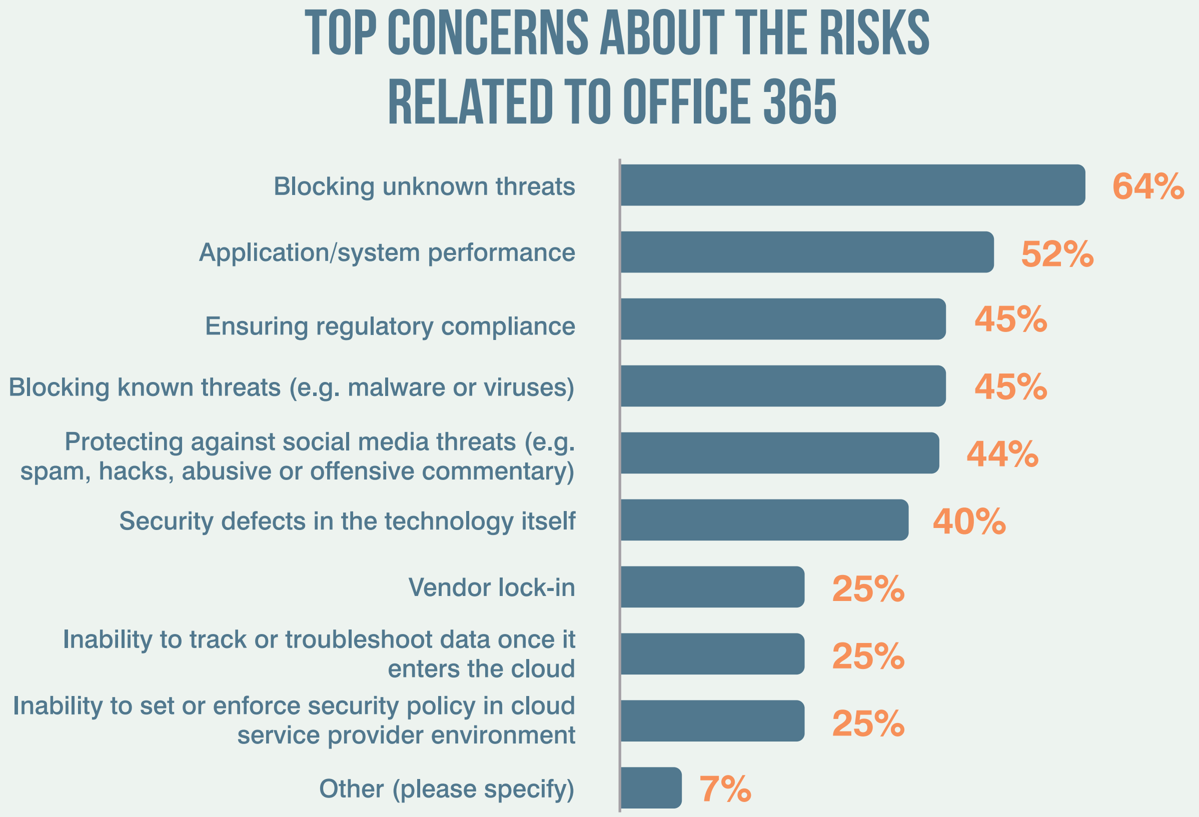
Organisations can shift cost and infrastructure pain to the cloud and boost workforce productivity when they move to Office 365 but that doesn't mean handing off accountability for security too. There is a solid core of in-built security in Office 365, including Microsoft's recently announced advanced security management features, but organisations shouldn't just assume these meet their own protection, archiving, continuity and compliance needs. The buck still stops within each organisation when it comes to security accountability.

Email is the foundation of Office 365 and, as a mission critical communication tool for organisations, it remains a target for attackers. People are still the weak link when it comes to security and email provides many ways for attackers to infiltrate organisations, inflict damage with malware-based or malware-free approaches and steal valuable data or assets.

### How does Office 365 stack up when it comes to the capability of its in-built security?

Our survey reveals that many organisations have concerns about some of the potential risks associated with deploying Office 365 (Figure 3). Topping the list of concerns is the risk from unknown threats (64 per cent) but traditional known threats such as malware and social media-related threats from spam and hacks also feature prominently.

OUR SURVEY REVEALS THAT MANY ORGANISATIONS HAVE CONCERNS ABOUT SOME OF THE POTENTIAL RISKS ASSOCIATED WITH DEPLOYING OFFICE 365.



TOP CONCERNS ABOUT THE RISKS RELATED TO OFFICE 365

Figure 3

It's a similar picture for advanced threats, with nearly half (49 per cent) of respondents concerned or very concerned about using Office 365 to detect and block zero-day and advanced persistent threats. This is particularly worrying given that these advanced targeted attacks represent one of the most dangerous threats facing organisations today. They often start with a spear-phishing attack where a carefully crafted, almost-personalised email tricks an employee into clicking on a URL to download malware or open a malicious attachment.

Some of these advanced targeted attacks include dangerous ransomware such as Locky, which encrypt all a victim's files, and there is a rising trend for so-called imposter phishing emails (see box out).

Not only is the ability of Office 365 to detect these attacks a concern but there also appears to be little confidence among users in its in-built capability to then respond and deal with them. Only 27 per cent of respondents are very confident in Office 365's email gateway product to detect and block known threats. Likewise just 10 per cent are very confident in Office 365's ability to provide real-time security intelligence for incident response.

The killer punch in all this is the prospect of actually being attacked and breached is high with more than half of respondents saying it is likely or certain they will have to respond to a major security breach in the next year (Figure 4).

HOW LIKELY DO YOU THINK IT IS THAT YOUR ORGANISATION WILL HAVE TO RESPOND TO A MAJOR SECURITY BREACH IN THE NEXT 12 MONTHS?

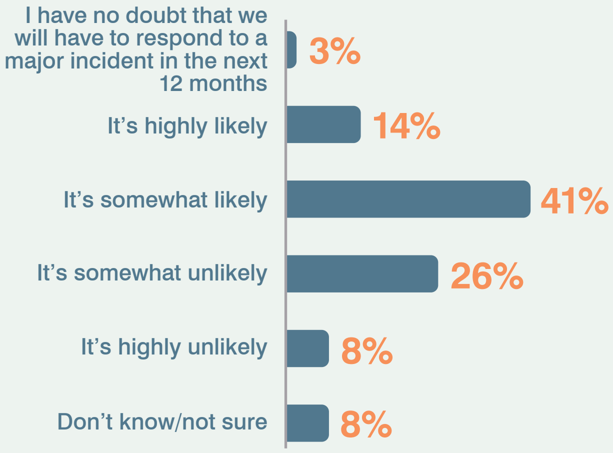


Figure 4

## BEWARE NEW ADVANCED SECURITY THREATS

### Imposter attacks

These are socially engineered imposter emails, also known as business email compromise (BEC) or CEO fraud. Attackers can essentially spoof the target organisation's email domain and trick an employee into clicking on a URL or opening an attachment in the email because it appears to come from someone else within their own organisation. A word of caution, however: the vast majority of BEC cases don't rely on malware. That means if your standard Office 365 email security relies only on malware detection it will fail to spot and prevent most BEC attacks. Our threat intelligence report for Q1 2016 found that 75 per cent of imposter email phishing attacks rely on fake 'reply-to' spoofing to trick users into believing messages are authentic, showing these attacks are evolving and becoming increasingly mature.

### Ransomware

This type of malware, which encrypts the victim's documents until a ransom is paid, has grown dramatically over the past 12–18 months. One of the most recent families of ransomware to wreak havoc is Locky. Our threat intelligence report shows almost a quarter (24 per cent) of document attachment-based email attacks in Q1 2016 featured Locky. Dridex was the only malware payload used more frequently. Locky is usually delivered via financial spam email with a malicious Word attachment. The ransomware is embedded in Word macros and when enabled it infects the victim's computer and encrypts files.

It's not just about malicious security threats, however. There are other potential risks facing organisations deploying Office 365. Take email continuity. However reliable Office 365 is, the very nature of cloud-based services is they can be hit by outages and failures. There have been two recent Office 365 outages in December 2015 and February 2016, for example. Email is mission-critical and organisations risk employees not being able to access, send or receive important emails without extra security, backup and recovery in place. The other risk from these continuity failures is that during outages employees still need to get their work done and will turn to unauthorised personal cloud email and storage services to send and share files, which IT will have no visibility or control over.

Information protection is also an important consideration. While Office 365 provides some basic functionality in its email security capabilities, an organisation's data often also resides in file shares, storage area networks (SANs), network attached storage (NAS) and SharePoint. Employing multiple solutions can result in mismatched policies, inconsistent enforcement and disjointed reporting.

Archiving in Office 365 also poses issues organisations need to evaluate and address. There are differences between Office 365 and on-premise servers with some services and data not archived, and the eDiscovery process may not have the real-time and iterative search capabilities needed. That can lead to problems when it comes to audit and discovery for legal and compliance reasons, where the organisation may be required to search for and recover conversations or data.

## 3. HOW TO SECURE OFFICE 365

Microsoft offers a number of value-added services for Office 365, such as email security and email archiving for Exchange Online. However, based on your own security strategy and goals your organisation might well need a more robust layer of security on top of those in-built capabilities.

In the face of increasingly advanced and targeted attacks, additional third-party security can provide the insight, intelligence and visibility needed to quickly identify, understand and respond to these threats. There are also the business continuity risks to email access and archiving issues to address.

**Email malware threats**
Office 365 relies on URL reputation to detect links in emails that might lead to compromised websites with malicious executable code or which have been set up for phishing. However, today's more advanced malware-based threats require dynamic analysis and sandboxing to fully detect threats in unknown URLs before unwitting end users click on them.

**Actionable intelligence**
Office 365 doesn't provide insight as to whether an attack is part of a campaign affecting other organisations or is a targeted attack against you. It simply notifies that something is blocked or not. Actionable forensic intelligence can identify who is being targeted, what threats have been received and help orchestrate a response.

**Continuity**
Email is a mission critical application for most organisations. So what happens during an outage? It is vital to enable employees to continue receiving and sending emails without being impacted by the downtime. Remember it's not just about the disruption of not being able to access email but the risk to corporate data of employees resorting to unauthorised and unmonitored personal email to remain productive. Look for products that can mitigate the risk of downtime and lost productivity and maintain email access through automatic failover and recovery.

**Smarter attack response**
Advanced threats move rapidly through an organisation's infrastructure. This infrastructure includes the Office 365 tenant, as well as the broader infrastructure. For example, if a user clicks on a malicious link in an email delivered by Office 365 it may install ransomware on the user machine and at the same time tries to communicate with a command and control server to exfiltrate information. In this case, consider built-in workflows that support rapid containment activities such as blocking CNC traffic, isolating infected machines by taking them off the network, and moving users into restricted permission groups.

Also consider solutions that will address emails that have already been delivered to an Office 365 account. They could feature automatic or on-demand extraction, depending on your comfort level, but should at minimum move the email out of the reach of the end user.

The ability to detect the threat and then respond rapidly is vital. So it's a concern that nearly two-thirds of respondents told us they can only automate containment of up to three-quarters of advanced threats. And a significant number of those say they are only able to automate for fewer than half of attacks (Figure 5).

Organisations should evaluate how Office 365 fits with their business and legal requirements for email security, compliance, archiving and disaster recovery. These are the three key areas organisations will likely have to invest in additional security capabilities to secure their Office 365 deployments:

IN THE CONTEXT OF YOUR 'INCIDENT RESPONSE FRAMEWORK' WHAT PERCENTAGE OF ADVANCED THREATS ARE YOU ABLE TO AUTOMATE CONTAINMENT?

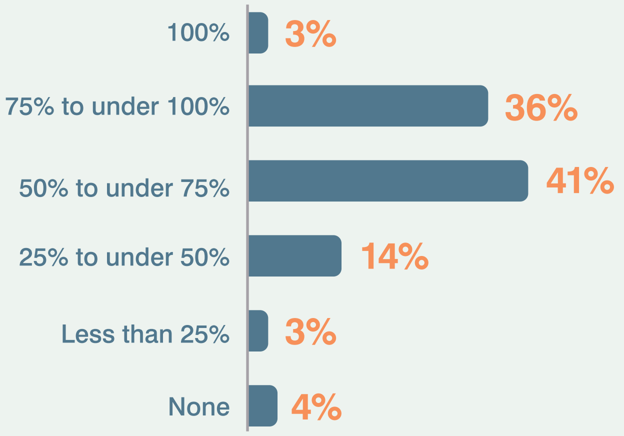


Figure 5

**Threat attack protection**
Malicious URLs and attachments in emails can evade traditional antivirus to deliver ransomware and other advanced malware. Any security technology needs to be able to use a combination of sophisticated techniques that include real-time checks against emerging campaigns and new threats, static code analysis that looks for suspicious behaviour and dynamic malware analysis that sandboxes malicious URLs and attachments in virtual environments for observation. Careful consideration should also be placed in assessing how malware-free attacks such as highly targeted BEC and credential phishing are handled.

**Threat visibility**
Visibility is key to tracking down threats, improving security and, ultimately, supporting business objectives. Organisations need to know the who, when and what device of an attack and the context to prioritise alerts and take the appropriate action. Forensic insights such as real-time visibility about which users clicked on which link from what device, DNS look-ups and registry key changes help IT security respond faster to advanced threats and prevent widespread compromise. You cannot respond to what you cannot see.

**Threat intelligence**
Intelligence puts organisations one step ahead of the attackers. It enables a more proactive security posture to detect, block and investigate threats before they hit the organisation's infrastructure and data. Third-party security intelligence should provide actionable, real-time global IP and domain reputation feeds with a database of globally detected threats and malware analysis. Good threat intelligence also helps with enforcing custom security policies and improving fidelity. It cuts out the noise to reduce false positives from existing intrusion detection and prevention systems and firewalls.

**Threat response**
This piece of the jigsaw is about a centralised, joined-up incident response process that brings together all the relevant threat information in one place and orchestrates containment of the threat. Key features should include a dashboard to easily view all critical threats and open incidents at a glance, incident scoring to help with prioritisation and reporting of real-time trends about malware and infected users. It should also be able to recognise threats where a verdict changes to malicious, then quickly move these emails out of the reach of users. Instead of manually researching a detected security threat using disconnected tools and manually implementing containment measures, threat response needs to be integrated so that security teams can quickly engage enforcement points such as network security, web security, or user access assignments to orchestrate response in a scalable and impactful way.

## PROOFPOINT THREAT PROTECTION FOR OFFICE 365 HELPS YOU:

- **Stop 99.9 per cent of advanced threats before they reach your users**
- **Maintain email continuity to minimise the impact on productivity and avoid introducing new security risks**
- **Gain threat visibility at an organisation, threat and user level to prioritise actions**
- **Respond to compromise with automated threat quarantine and integration with your security ecosystem for rapid response**

### WANT TO LEARN MORE?

www.proofpoint.com/office365

## 4. SUMMARY - NEXT STEPS

As enterprise cloud adoption rises, many organisations are also switching from their traditional on-premise deployments of Microsoft's Office productivity suite to the cloud-based Office 365. It offers clear benefits in terms of flexibility, productivity and cost savings, but this shift brings security risks.

Malware detection capability, threat visibility, intelligence, response and continuity are all critical areas to address in any Office 365 deployment, particularly in the face of the increasingly advanced and sophisticated nature of the threat landscape today.

Organisations must tackle these issues if they are to have full confidence in their wider security strategy. Consider augmenting Office 365 with additional third-party security in four key areas:

1. **Threat attack protection**
2. **Threat visibility**
3. **Threat intelligence**
4. **Threat response**

## 5. FURTHER RESOURCES

Business email compromise claims another C-level job (blog)
www.proofpoint.com/us/corporate-blog/post/business-email-compromise-bec-claims-another-c-level-job

Beyond vanilla phishing - imposter email threats come of age (blog)
www.proofpoint.com/us/threat-insight/post/Beyond-Vanilla-Phishing-Impostor-Email-Threats-Come-Of-Age

The imposter in the machine: Understand the motives and mayhem of imposter emails (whitepaper)
www.proofpoint.com/us/id/ImpostorEmailMachine

Breach mitigation: Hardening Office 365 against data loss (webinar)
www.proofpoint.com/us/id/Webinar-Q315-Office365-DLP

Best practices for migrating to Office 365 (whitepaper)
www.proofpoint.com/us/id/PPWEB-WP-Office365-Osterman-MigrationBestPractices-2015-2

Shielding Office 365 from Advanced Threats (webinar)
www.proofpoint.com/us/webinar-q315-office365-advancedthreats

Office 365: CXO's guide to security and archiving challenges (whitepaper)
www.proofpoint.com/us/id/WP-Q314-Office365-Osterman

Office 365: What you need to know (webinar)
www.proofpoint.com/us/id/Webinar-Q215-Office365

Verizon's 2016 Data Breach Investigations Report
www.verizonenterprise.com/verizon-insights-lab/dbir/2016

## ABOUT PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organisations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information.

**More information is available at www.proofpoint.com**.