censornet.

EMPOWERING THE PEOPLE

Critical Cyber Security Challenges

EMPOWERING THE PEOPLE:

Critical security challenges of 2020

We are at a new defining moment in the history of work and technology. Since the COVID-19 lockdown began, security and IT professionals across the globe have faced extraordinary challenges. Practically overnight, almost every employee became a 'remote worker', leaving most organisations in a position of increased exposure on an escalating scale.

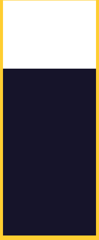
Now with uncertainty surrounding office returns, social distancing and local lockdowns, it falls to the IT security team to securely facilitate flexible and remote working to empower the people.

Only 34% of security professionals felt they were very prepared to support employees working from home securely

Organisations who were once dealing with a small group of remote or travelling users are now managing entire workforces who are operating from every conceivable location. Leadership and security teams are now universally facing the same challenge:

> **How can we help our employees to work productively, effectively and safely from wherever they are in the world?**

Interestingly, at the time lockdown was announced, 72% of professionals felt that the cloud had improved their organisation's security posture, putting them in a strong position to deal with increasing cyber threats. However, the major shift in work location and jump to adopt new tools has highlighted the risks associated with the cloud and meant that many have needed to radically re-evaluate their posture.



72%

of professionals felt that the cloud had improved their organisation's security posture

Our recent research has revealed that although many organisations are benefiting from productivity when adopting or leveraging cloud applications to support remote working, it has also created a complex threat landscape which needs to be addressed with some urgency.

Our findings also show that cybercriminals are unsurprisingly capitalising on this exposure, leaving a clear and immediate need for security professionals to take stock, exercise caution and ask the hard questions about the capability of their technology in the current climate.

Using insights gathered **from a survey of 300 cyber security professionals and the guidance of industry experts** within the Censornet team, this report explores the reality of the role of security during a global pandemic.

Read on to see how this transformational change has created both immediate and long-term security gaps that need to be addressed, as well as how your peers are strengthening their security and overcoming common challenges using tactics you can implement today.

Key areas:

CYBER SECURITY IN 2020:
An unpredictable landscape

EMAIL SECURITY:
Aligning strategy with user behaviour

THE REALITIES OF A REMOTE WORKING CULTURE

TACTICS FOR TODAY

With this information, we hope to inform and empower you, as security professionals, to adapt and thrive at a time when 'business as usual' is being continually re-imagined.

Section 1

CYBER SECURITY IN 2020

An unpredictable landscape

Cyber security in 2020

Since the pandemic began, the number of cloud solutions being used has skyrocketed. Platforms like Office 365 and G-Suite are helping organisations move to the cloud and away from traditional on-premises networks, and in some cases, fast-tracking digital transformation plans.

While offering clear collaborative benefits, cloud and hybrid environments can also bring their share of risk and although the security 'merits outweigh the flaws', the scale on which they're used (by users 'less familiar' with mobile working) leaves organisations alarmingly vulnerable to social engineering and sophisticated malware attacks.

A staggering **50% rise** in these attacks has sent a clear message that the vulnerabilities produced by the pandemic have not escaped the attention of cyber criminals. The new wave of less-informed remote users has created a surge in Business Email Compromise (BEC), Account Takeover (ATO), phishing and whaling attacks.

59%

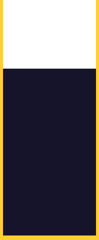
of enterprises expect cloud usage to exceed prior plans due to COVID-19*

As cyber criminals continue to modernise and diversify the technology and tactics used to attack, so must public cloud providers, security professionals and security vendors update their approach to defence. New vulnerabilities and weaknesses in the cloud-heavy working environment must be overcome to create confidence and empower the activities of their employees.

This should include an honest and brutal assessment of whether their technology meets the needs of their users in the current climate.

In this section, we'll take a look at the top security challenges and priorities affecting organisations to highlight areas of your current security posture which may need bolstering to deal with these changes.

We'll also include recommendations from our team of experts combined with some anecdotal customer case studies to illustrate what is being accomplished by forward-thinking professionals, who share similar challenges.



58%

of security professionals said their move to the cloud made security more complex

10%

believe that the cloud has made security worse

Top security challenges and priorities

Remote working may not be a 'new' problem to solve, but when suddenly motivated by public health and government law, a vast number of people who have a huge variance in security awareness were thrown into it, presenting a whole new set of challenges to address.

Many experts also believe that this radical culture change signifies the demise of the traditional office, which places the examination, understanding and control of 'user activity' among the top priorities for security professionals.

> "Right now, it's about battening down the hatches. Cyber security and IT professionals have prioritised function when it comes to the cloud; now it's all about strengthening security."
>
> Charles Milton, VP of Strategic Alliances at Censornet

Top 5 cloud security concerns in 2020:

1 DATA LOSS

2 CLOUD SERVICE PROVIDER IS COMPROMISED

3 UNAUTHORISED ACCESS/ATO

4 DOWNTIME

5 MALWARE

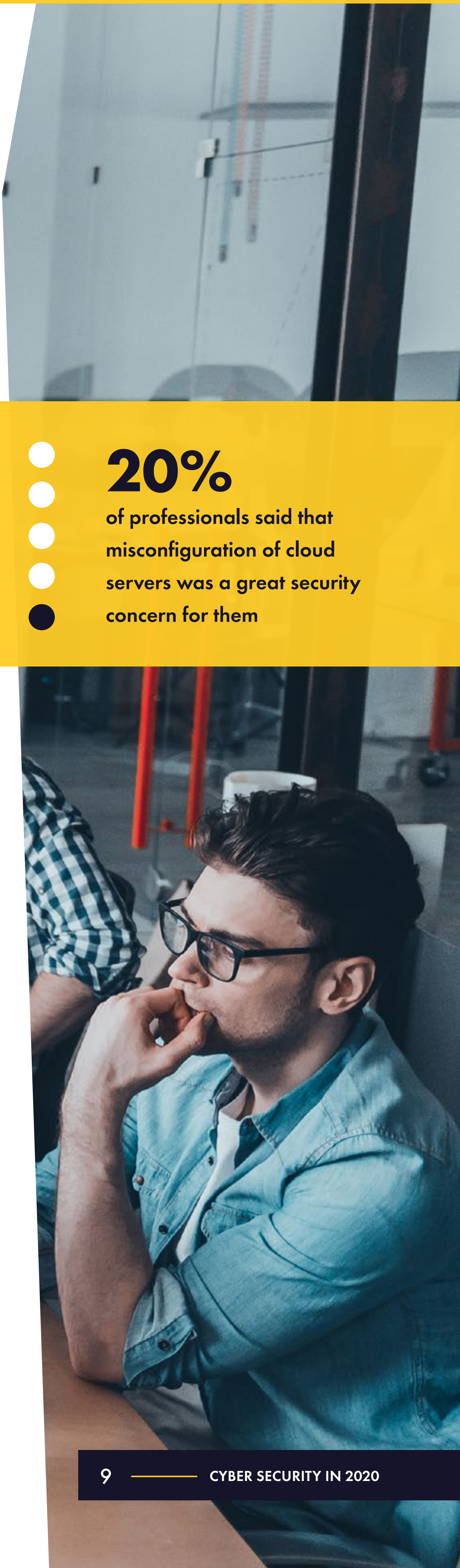
The three greatest concerns among security professionals in terms of cloud security are data loss (49%), that their cloud service provider is compromised (40%) or Account Takeover attacks (37%).

Tightening up system and security to avoid data loss

Data loss has topped the 'usual suspects' list of major security concerns for some time but with the number of remote users still rising, many organisations have been forced to mobilise entire workforces to the cloud with relatively little resource or time to focus on security.

Now remote access is considered the norm, and as data regulation continues to tighten, organisations must recognise the need to apply data security across all devices and all communication, collaboration and storage tools.

Although tough decisions have been made on which new systems, services and devices to deploy and which security protocols to prioritise to enable employees wherever they are working from, regular review of policies and configuration can keep security teams on top of data challenges in the application-focused 'new work nucleus'.



20%

of professionals said that misconfiguration of cloud servers was a great security concern for them

“With the blind spot that end-to-end encrypted mobile apps create the only option may be to use MDM (or EMM) solutions to force users back into the browser to restore visibility – and management.”

Richard Walters,
CTO at Censornet

“You need tools in place to control unintended data breaches. Use a CASB to block user actions that could later cause a data breach – like sharing organisational data externally.”

Ragnar Heil,
Channel Account Manager,
EMEA Central & Microsoft MVP

Steps for stronger security:

Once remote users have access to the tools to do their job, the next natural step is to perform a risk assessment on any new systems and services you may have deployed to expose any potential weaknesses.

Put policies in place to prevent unintentional or malicious actions in applications, such as unauthorised downloading of files or sharing of folders, with a CASB.

Apply data loss prevention tools across web, email and cloud applications to highlight and stop sensitive information from leaving the business or getting into unsanctioned hands.

Planning for the worst-case scenario

During the initial lockdown period, 40% of professionals identified the compromise of their cloud service provider as one of their top concerns

The overarching challenge CISOs and cyber security teams will have right now be protecting their institutions while enabling operations to go on without interruption which is understandable given the dependence on many third-party providers. Reassuringly, there is a far lower likelihood of platforms like Microsoft Office and G-Suite being compromised compared to traditional on-premises infrastructures. However, as we've experienced with COVID-19, you cannot assume anything.

Alarmingly, 25% of organisations don't currently have a contingency plan in place for downtime if the worst were to happen

And with remote working looking likely to play a bigger role in 'the new normal', it's imperative that disaster recovery and business continuity plans are updated to reflect changes in working practices.

This is not only to protect organisations in the event of an outage but also to prepare for the possibilities of wide-spread denial-of-service attacks or the inevitable next large scale data breach.

Steps for stronger security:

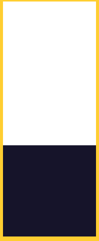
Put steps in place to reduce the impact of planned and unplanned outages on employees and helpdesk staff by keeping the most vital component to protect productivity up and running: email.

Providing users with emergency access to email, isolated from Microsoft infrastructure, can be a vital lifeline. Emergency Inbox solutions, via a webmail style interface, mean users can read and respond to new messages and review 30 days of sent and received mail, even when Exchange Online is offline.

For those who have to meet strict regulatory requirements or who are subject to audits, Email Archiving provides tamper-proof access to all historical email – with the ability to quickly search for messages.

Protecting user accounts

The potential impact of an Account Takeover attack is enormous, leading to sustained and varied impersonation campaigns. The rush to put everything in the cloud has only magnified the problem, with vast volumes of critical information and vital processes now behind a simple username and password. The attack surface has fragmented and moved outside the perimeter.



37%

of professionals cite unauthorised account access as one of their top concerns, so it's no surprise that authentication is high on the agenda

But with so many routes to harvesting login details and cracking accounts, it takes more than a password to keep an account secure. In fact, **BEC attacks accounted for 50% of cyber crime losses in 2019**, with the average attack costing $75,000* so it deserves our attention.

Administrator and other privileged accounts, finance team and executives accounts are the most sought after by cyber criminals as these provide the best launchpad for resetting and granting additional access to other cloud applications and initiating secondary attacks on suppliers, customers or colleagues.

The suitability of passwords alone to protect accounts has been in question for some time, but the step towards cloud environments is pushing more advanced contextual authentication to the forefront.

*Source FBI Internet Crime Report 2019

> “Use multi-factor authentication by default. This is to minimise the impact of credential capture and eliminate Account Takeover. Ensure MFA is set up for admin users and then wider employees – particularly for mobile users.”

Ian Moyse,
EMEA Sales Director,
Natterbox Ltd

Steps for stronger security:

Educate staff about password best practice i.e. not to use the same password for multiple accounts – particularly corporate and personal accounts.

Use advanced email, web and cloud application security to block phishing attempts that aim to steal login details.

Apply adaptive contextual MFA consistently across all areas of the environment so there is no weak link in the defences that would allow a hacker into your environment.

Staying one step ahead of malware

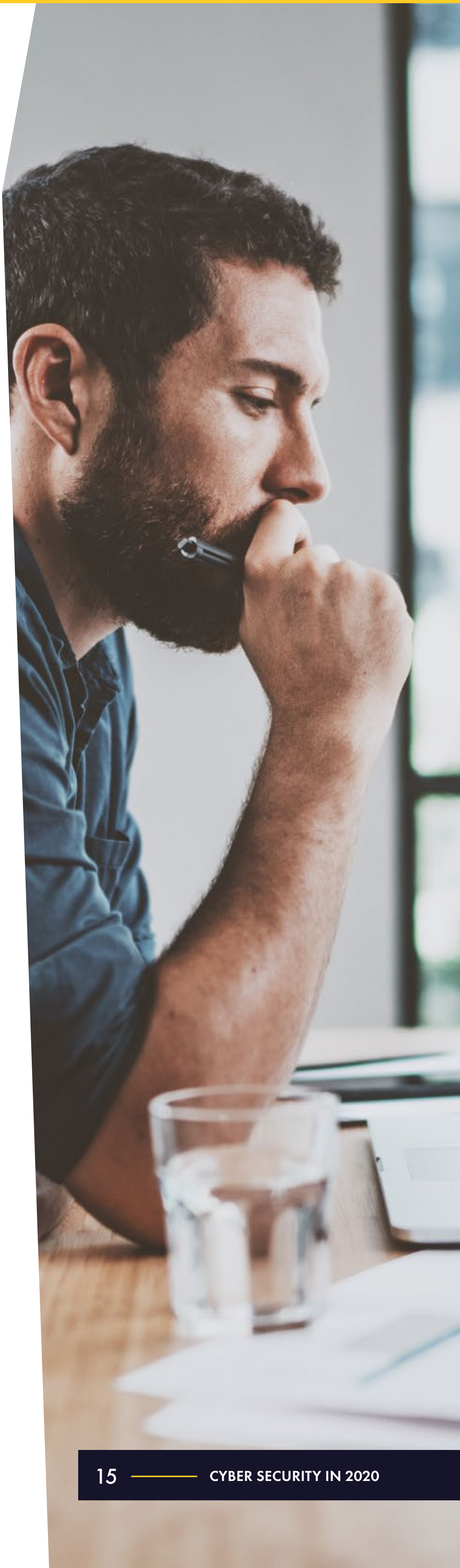
1/3
of professionals cite malware as a top concern

Malware is one of the most enduring challenges in cyber security. It comes in so many shapes and sizes and from all channels; as such, securing against it is a mainstay of any security posture.

Groups of cyber criminals have been exploiting the pandemic, shockingly even targeting vaccine research facilities with malware.

Email and web are well known as the most popular attack vectors, but due to the rapid adoption of cloud services, increasingly cloud-only malware written to propagate across cloud shares is a threat. While users are generally well educated about the risks of opening unsolicited or unfamiliar emails, or downloading materials from unknown sites, they are less likely to question whether content held within an application is 'safe' and/or 'genuine'.

It is therefore imperative to have security in place across multiple channels to protect from malware.



Steps for stronger security:

For every channel you are using, protection from malware should be deployed; that means protecting your organisation from malware threats coming in over email, from websites and cloud apps.

Threat intelligence also plays a part to block IPs and domains that are malware distribution points, as well as to prevent malware reaching out to command and control (2C) infrastructure.

For the best protection it is important that all core security tools talk to one another to share share security context, state data and events. By combining this data with threat intelligence which provides information on known bad files, security tools can make decisions based on the latest information. This can only be implemented with a consolidated security platform.

SECURITY LESSONS FROM THE NATIONAL PORTRAIT GALLERY

How they achieved full spectrum protection with consolidated security

Who?

Globally renowned art gallery in central London.

What was the problem?

The gallery needed to achieve Cyber Essentials certification to demonstrate to customers and shareholders alike that the Gallery has significant cyber security measures in place.

How did they fix it?

The National Portrait gallery chose to use MFA, email security, web security and CASB integrated in one **cloud security platform** to achieve the best security coverage and value, while reducing the burden on the security team.

The impact:

Not only are user accounts secure but the team is able to identify attacks and alert staff, block risky cloud and web activity, and stop multi-channel attacks by putting rules in place so that threats identified across different channels can be cross-referenced and blocked across web, cloud and email.

Read the full customer story:

FIND OUT MORE

"Censornet allowed us to prove that we had taken all the necessary measures to protect our employees from viruses and malware and that we were controlling who had access to sensitive data through MFA... It's definitely one of the best software purchasing decisions we have made."

Nicky Dowland,
Head of IT at the National Portrait Gallery

Section 2

EMAIL SECURITY

Aligning strategy with user behaviour

86% of professionals agree that email security threats have become more sophisticated over the past decade

Email is the primary starting point for the majority of cyber attacks: that hasn't changed.

Any opportunity cyber criminals have to create new social engineering campaigns, they'll take, and this pandemic has opened the door to a seemingly endless world of unlawful possibility.

Among the most popular are CEO Fraud and Business Email Compromise (BEC) attacks. Although these types of threats may be well known, the sophistication and personalisation of the attacks in the current climate mean that email security strategies must also be reviewed and held up to scrutiny. This includes taking 'employee behaviour' into account, understanding where employees may need further education, and what tactics can be implemented immediately to block attacks from entering the kill chain this way.

To do this effectively, we need to look at people, processes and technologies.

> "Defending against email threats needs to be a perfect combination of people, process and technology."

Richard Walters,
CTO at Censornet

1. People

73%

of professionals say they trust employees to follow best practice, yet...

87%

said that most threats could be prevented if employees followed best practice

Mitigating against the threat of natural human error during remote working is a challenge capable of keeping most security professionals awake at night. However, we equally need to be accepting that many employees have had to adapt to new environments under pretty extraordinary circumstances.

Even with previous training and the best intentions, it's perhaps unfair to place too much responsibility and expectation on 'personal' understanding of email attacks or security. This is why reviewing your user training strategies is vital.

Steps for stronger security:

With many employees adapting positively to remote working, they are equally likely to be more receptive to 'contextual security education' and user awareness training which will help them to spot scams and new innovative phishing techniques designed to trick them.

This could prove particularly useful and potentially prevent remote users falling victim to advanced threats such as 'invoice fraud' ATO and COVID-19 specific scams.

> **"Often, tagging subject lines of messages and banners at the top of message bodies is enough to make the user stop and think."**

Richard Walters,
CTO at Censornet

2. Process

48% of professionals either strongly or somewhat agree that their organisation would be more secure if they didn't use email

In the name of productivity, use of cloud communication platforms like Slack, Microsoft Teams and Exchange Online is changing the way that many businesses work. In fact, 56% of professionals now believe that cloud applications for communication are more secure than email.

Our research has shown that 'Remote Culture' is clearly affecting and contributing to the demise in confidence in email. Take CEO or Invoice Fraud as an example.

Employees would have previously been able to verify an 'urgent bank transfer' request with relative ease by walking over to a person's desk or asking a fellow team member. Now they rely on the authenticity of email credentials which are easily replicated by scammers.

Steps for stronger security:

To help prevent these types of attacks, it's important to establish or modify security processes so that they include different layers of checks to compensate for new ways of working.

For example, employees should flag requests for payments above a certain amount using a method other than email either with a phone call or online video meeting.

3. Technology

85% of respondents thought that their current email security solution was adequate or comprehensive

Although many organisations feel their current security solution covers email threats, it's vital to evaluate their effectiveness through a COVID-19 and a remote working lens. After all, the technology in place today must help protect against human error and the vulnerabilities presented by a remote culture.

Legacy email security solutions are not designed to tackle the complexity of highly sophisticated targeted attacks or handle complicated mail flow, and though some professionals may feel the security offered by technology companies who specialise in other areas is adequate, layering on advanced email protection is recommended by industry analysts, experts and even Microsoft.

"In security and compliance areas more focused third-party providers are likely to offer better capabilities than relying solely on what Microsoft has to offer"*

Steps for stronger security:

Conduct an honest assessment of your email security solution and evaluate if it truly lives up to the standard of protection required.

If your current solution lacks the layers of algorithmic analysis, threat intelligence, executive monitoring and real-time link scanning needed to defend against advanced email threats, you may need to upgrade to improve your security posture.

This upgrade can also bring enhanced image content analysis and data loss prevention features, and improved control over mail flow while providing an effective way of blocking advanced threats from entering inboxes wherever the user is, even in platforms like Microsoft 365 and Exchange Online.

*Osterman Research 2019 'Using third party solutions with Office 365'

SECURITY LESSONS FROM ONECOM

How they blocked sophisticated attacks with email security

Who?

Onecom is a UK leader in business telecoms.

What was the problem?

They needed a centralised way to protect their remote workforce from cyber threats on email, while saving time and resources.

How did they fix it?

To do this, Onecom chose to invest in an ultra-modern layered **email solution** that integrates with threat intelligence to catch sophisticated phishing attacks. Time-of-click protection from malicious links in emails was also used to give certainty of security wherever the user is and whenever they access the email.

The impact:

Advanced layered email filtering catches dangerous messages before they reach the inbox. By implementing 'time-of-click' protection from malicious links in emails, employees can now work safely and confidently from wherever they are in the world.

> "Employees have all the same filtering on their email as anybody that would've been using a standard set up in the office, even if they're at home."

Alan Stanley,
Head of Technical
Operations at Onecom

View the full customer story:

FIND OUT MORE

Section 3

THE REALITIES OF A REMOTE WORKING CULTURE

THE REALITIES OF A REMOTE WORKING CULTURE

91% of professionals are confident that their cloud security solutions are effectively protecting people at home

The new culture in which we work is remarkably complex – it has many different technical, behavioural and cultural characteristics compared to working exclusively in an office.

While it's encouraging to see so many professionals confident that their cloud security solutions are protecting their workforces, our research shows a disconnect between the perception of how well protected an organisation is when employees are working remotely and the truth behind the risks they face.

In this section, we explore the realities and behaviour of remote users when working from home and the tactics you can implement today to ensure your security strategies reflect their activities.

New employee behaviours and Shadow IT

Whether it's a result of more flexible working hours, fewer restrictions or more relaxed access policies on work laptops, the boundaries between work/life activities have never been more blurred.

Since lockdown was announced, **67%** of respondents have identified that employees are engaging in unproductive activity on the web, such as using streaming services at work like Netflix or Amazon Prime Video **(35%)**.

Many of the security professionals surveyed also admitted that they were engaging in behaviours including:

22% USING STREAMING SERVICES AT WORK

22% USING WORK CREDENTIALS FOR PERSONAL ACCOUNTS

11% VISITING ADULT SITES AT WORK

While the impact this behaviour has on staff productivity may not be the direct responsibility of security professionals, the natural consequences of Shadow IT, in tandem with 'less informed' remote users, has led to a lack of due diligence, resulting in an increase in stolen credentials and Account Takeover attacks.

Account breaches, particularly those of high-ranking staff or administrators with elevated privileges, carry risks to data, productivity and access, with sustained attacks possible when the intruder stays below the radar. As diverse working locations become the norm, and with so many credentials out 'in the wild', organisations are going to need more than passwords to secure accounts and inboxes.

34% have found employees using work credentials for personal accounts such as e-commerce sites, social media, gaming etc.

Steps for stronger security:

To protect user accounts from these threats, many organisations are implementing context-aware or adaptive Multi-Factor Authentication (MFA) wherever possible.

It is important to interrogate the context of the login to challenge users based on unusual behaviour to reduce user friction. If the login is requested from a strange location, time, day or device the authentication solution should pick this up and ensure further verification before allowing access.

SECURITY LESSONS FROM CAPSTICKS

How they secured remote working with MFA

Who?

Capsticks is a leading national law firm, specialising in Healthcare clients.

What was the problem?

The IT team wanted to strengthen its remote working environment with more advanced login protection to protect user accounts and confidential data – without creating user friction.

How did they fix it?

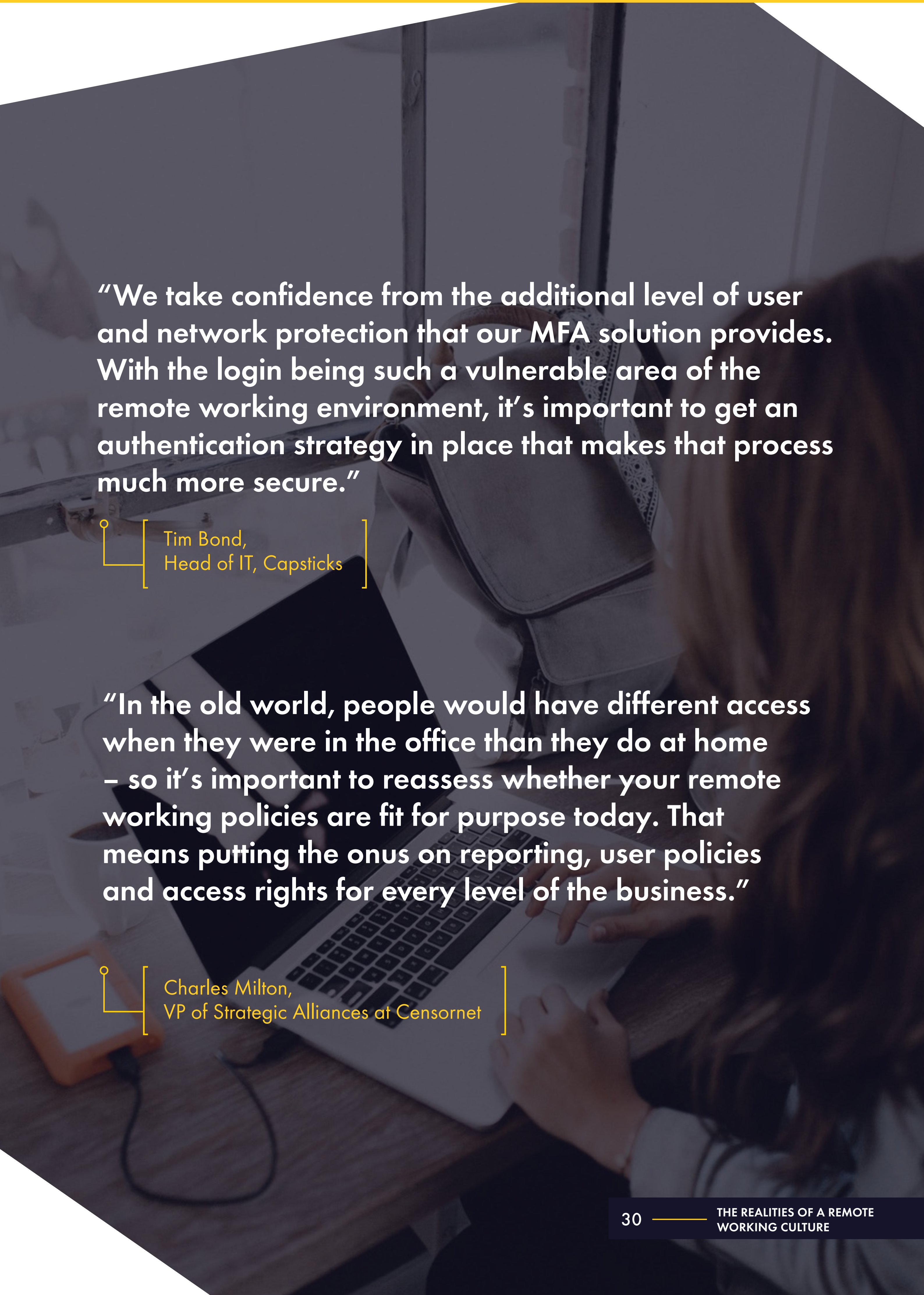
To secure systems with more than just a password, Capsticks chose an adaptive **multi-factor authentication** solution that uses real-time generated one-time passcodes and automatic fail-over across multiple delivery methods to provide secure authentication for its virtual desktop infrastructure solution and web based email client.

The impact:

MFA effectively secured authentication for Capsticks, providing confidence that user accounts and network access are secure, without disrupting the daily working lives of employees. Not only did this lower help desk calls, but it also helped to boost the firm's productivity.

View the full customer story:

FIND OUT MORE



"We take confidence from the additional level of user and network protection that our MFA solution provides. With the login being such a vulnerable area of the remote working environment, it's important to get an authentication strategy in place that makes that process much more secure."

Tim Bond,
Head of IT, Capsticks

"In the old world, people would have different access when they were in the office than they do at home – so it's important to reassess whether your remote working policies are fit for purpose today. That means putting the onus on reporting, user policies and access rights for every level of the business."

Charles Milton,
VP of Strategic Alliances at Censornet

Unintentional data loss and security breaches

Although the confidence in cloud security providers is improving, 'user behaviour' remains a significant concern. 76% of our respondents reported employee behaviour in the cloud that could be putting their organisation at risk.

The most common risky behaviours are:

41%

USING THE SAME PASSWORD

33%

STORING SENSITIVE DATA IN THE CLOUD WITHOUT THE PROPER PROTECTION IN PLACE

26%

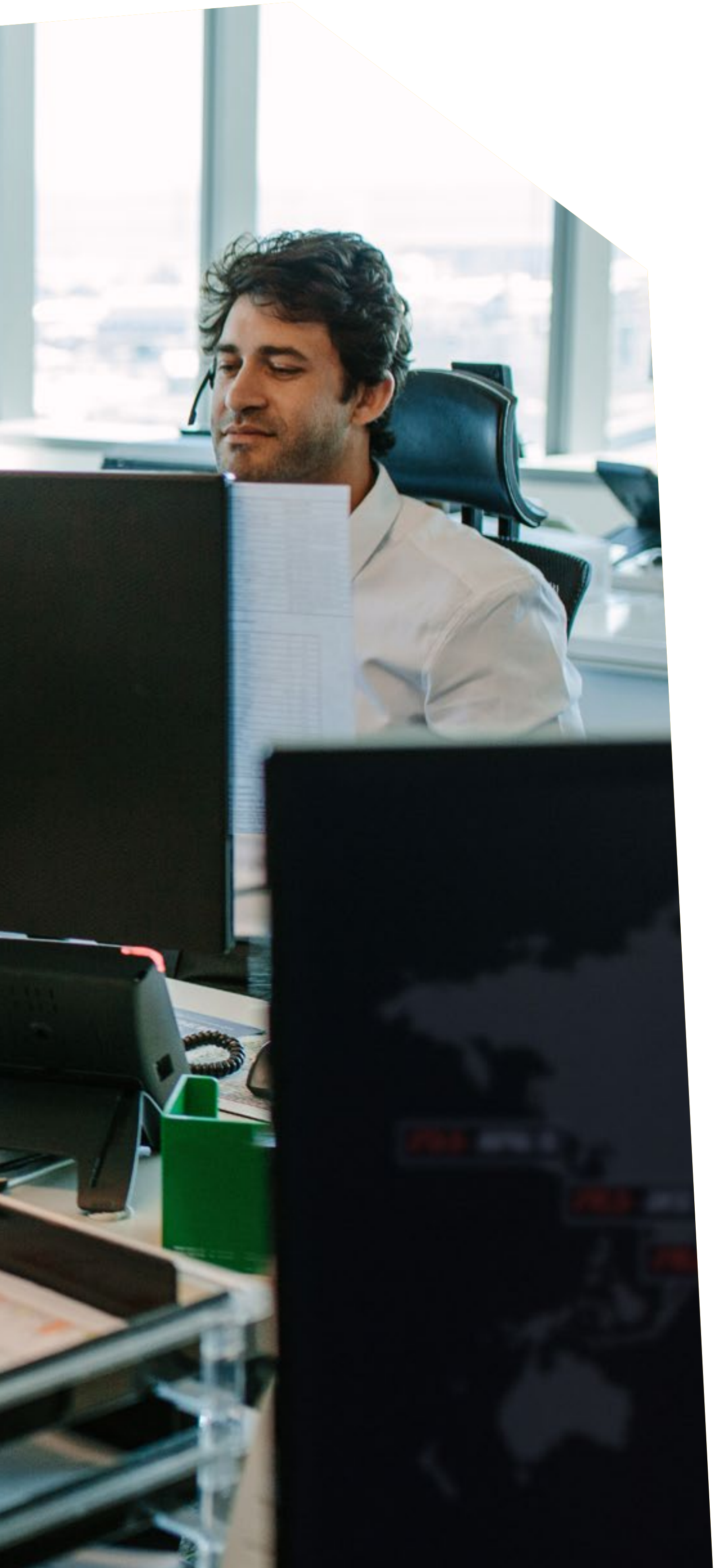
SHARING LINKS TO DOCUMENTS IN THE CLOUD WITHOUT AUTHORISATION

With remote working becoming more of a necessity than a choice for many organisations **(and with 36% of companies hosting their Active Directory in the cloud)**, the risk of ATO, non-compliance, unauthorised data sharing or data loss are not only major concerns but risks of considerable scale.

Advanced threats such as web-borne malware and unmanaged user interactions within the cloud also pose strong security concerns for organisations dealing with authorised and Shadow IT as many users work interchangeably between websites and applications without realising they are doing so.

How and where the protection is applied is under review as a combination of VPNs, split tunnels and direct-to-internet connections mean endpoint protection, rather than centralised protection, is required.

65% of security professionals believe the cloud gives them less visibility and control of sensitive data



Steps for stronger security:

To regain control of data stored in the cloud, implement a Cloud Access Security Broker (CASB) solution that works with a vast number of business applications such as Office 365, Dropbox and Salesforce so you can protect your whole cloud infrastructure from one place.

From here, security teams get granular insight into user activity to see exactly when and where data is being handled inappropriately, and by whom. CASB provides the information needed to tackle behaviour through education, and the tools to put policies in place to manage standard and privileged user access and actions across all business applications.

CASB puts the security team back in charge and helps to satisfy the needs of the compliance team, reducing the risk of data loss and data security breaches while enhancing protection with cloud security, data loss prevention and image content analysis features.

SECURITY LESSONS FROM ST ANNE'S

How they improved data visibility and control with integrated CASB and Web Security

Who?

From domiciliary care and assisted living, to support with mental health and substance abuse, St Anne's Community Services deliver support of all kinds, across the north of England to those that need it the most.

What was the problem?

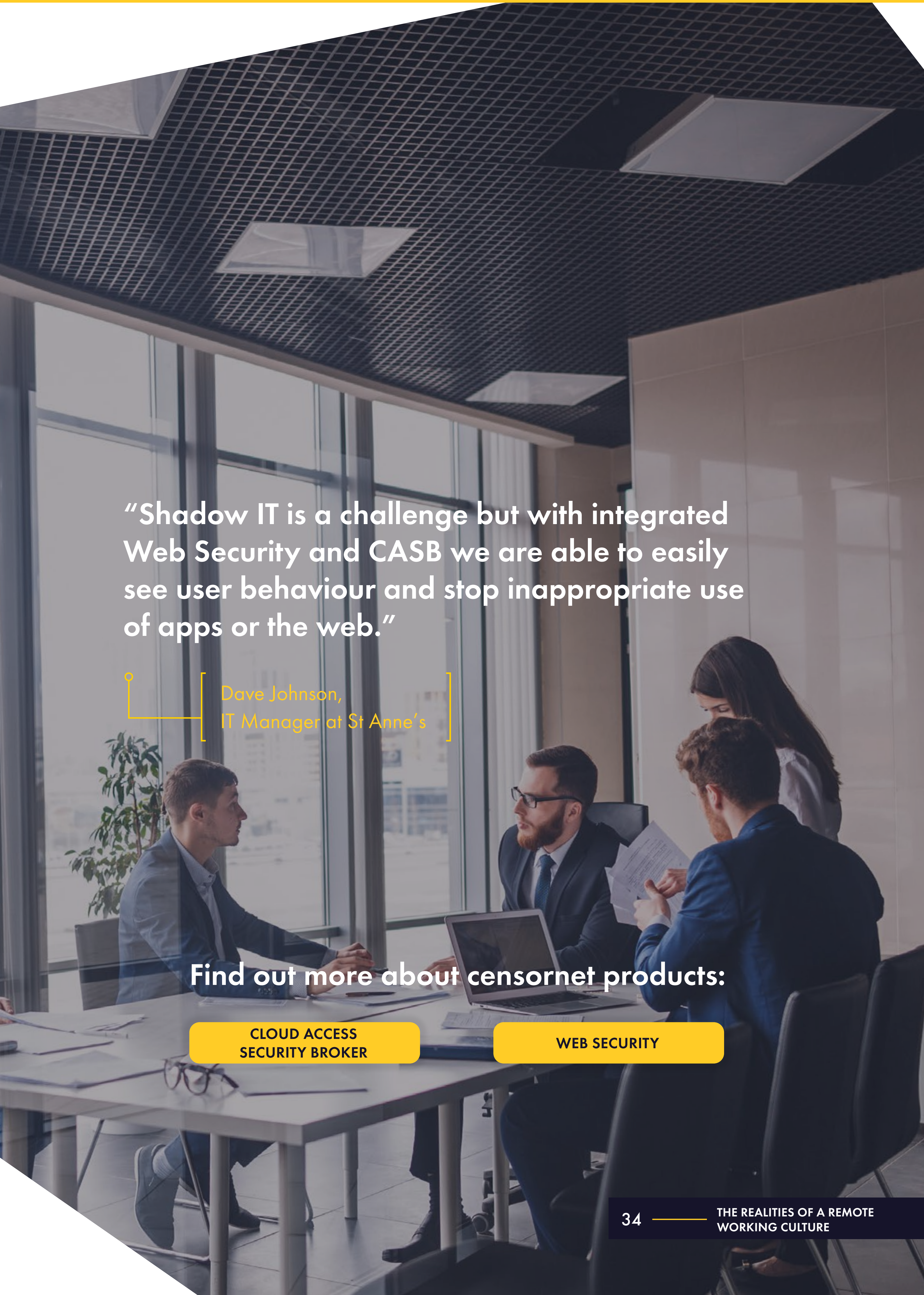
Remote carers experienced possibly the toughest challenge over recent months, at a time when stopping work was simply not an option. St Anne's made the decision to simplify and strengthen data security across eight locations, allowing their carers to work safely, from wherever they were most needed.

How did they fix it?

To do this, they chose to invest in an integrated **web security** and **CASB solution** that would provide them with an additional level of security over their Microsoft Azure and Office 365 products, as well as protecting their mobile workforce with zero-touch configuration. The solution's follow-the-user filtering helped to block dangerous content and malware, stop multi-channel attacks and prevent unsanctioned in-app activity.

The impact:

With security in place across web and cloud applications that is always connected, always available, and always updated, St Anne's staff can focus on what really matters, knowing they are safe from multi-channel cyber attacks, shielded from carrying out unauthorised in-app activity and protected from harmful content.



“Shadow IT is a challenge but with integrated Web Security and CASB we are able to easily see user behaviour and stop inappropriate use of apps or the web.”

Dave Johnson,
IT Manager at St Anne’s

Find out more about censornet products:

CLOUD ACCESS SECURITY BROKER

WEB SECURITY

Section 4

TACTICS FOR TODAY

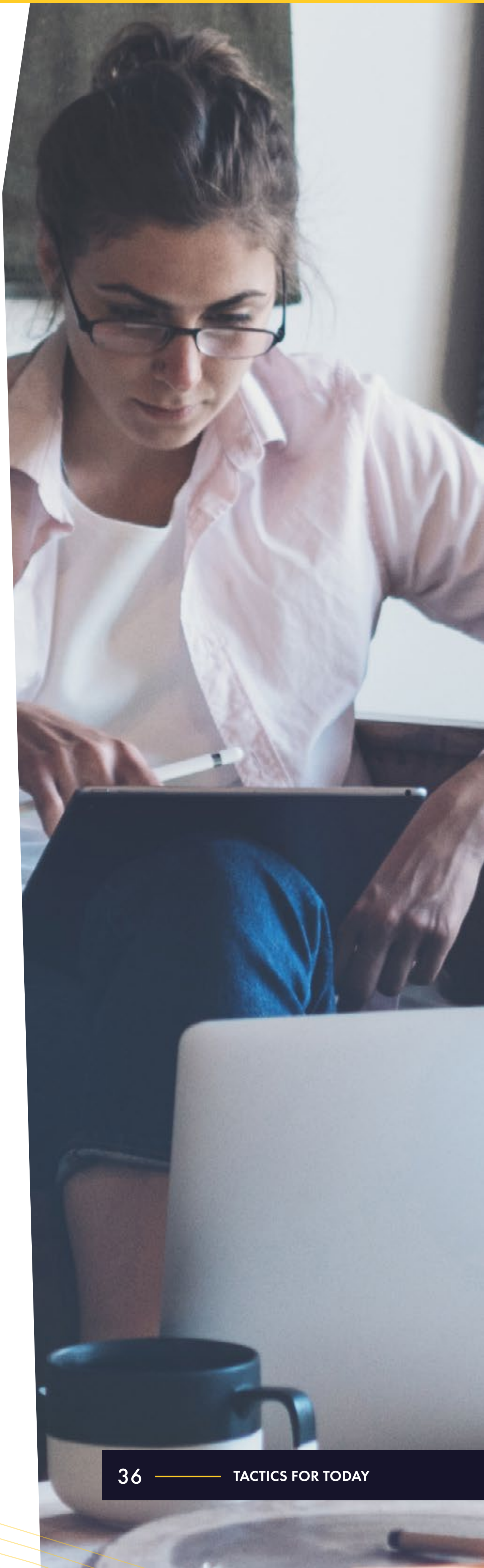
In 2020, security and IT professionals have embodied what it means to work with resilience, adaptability and strength. Faced with arguably the biggest change we're likely to see in a lifetime, this pandemic has truly marked the end of business-as-usual as we know it.

Love it or loathe it, remote working is to whatever extent here to stay, and with the pace of cyber crime showing no signs of slowing, the importance of carving out time to review the effectiveness, context and relevance of security solutions in place has never been greater.

It's becoming common knowledge that traditional security products will struggle to provide 'contextual protection' to remote users and with the now ubiquitous 'Public Cloud Platforms' firmly in the sights of cyber crime, it's in the hands of public cloud providers, security professionals and the security industry as a whole to step up and update their approach to defence.

The big lesson of 2020 is to be ready for anything and everything. The insights in this report have highlighted the challenging role cyber security professionals must perform in a dynamic landscape where expectations and risks are both high; however, by following the advice from experts and peers on strengthening your security posture you can empower the people in your organisation by securely facilitating collaborative, flexible, cloud-dominant and remote working.

To help kick off your review process, we've compiled a list of top tactics you can implement immediately to ensure your security posture is in the best possible shape.



Your 2020 security checklist

- USE EMAIL SECURITY THAT INCLUDES ULTRA-MODERN LAYERS OF DEFENCE ✓
- IMPLEMENT VOICE OR VIDEO/ONLINE TRANSACTION CHECKS TO PREVENT FRAUD ✓
- UPDATE YOUR SECURITY EDUCATION AND USER AWARENESS TRAINING TO INCLUDE COVID-19 SPECIFIC ATTACKS AND PHISHING SCAMS ✓
- USE A CASB SOLUTION TO GIVE YOU VISIBILITY AND CONTROL OVER DATA IN THE CLOUD ✓
- MAKE SURE CONTEXT-AWARE MFA IS GIVEN TO ALL USERS ✓
- REVIEW USER POLICIES AND ACCESS RIGHTS TO ENSURE THEY REFLECT CURRENT NEEDS ✓
- USE MDM OR EMM SOLUTIONS TO ENFORCE POLICIES ON MOBILE DEVICES ✓
- USE VPNS AND ENABLE AGENTS ON ENDPOINTS TO SECURE AT-HOME NETWORKS ✓