censornet.

SECURE REMOTE WORKING TIPS

BEST PRACTICE, TIPS, AND ADVICE TO SECURE YOUR ORGANISATIONS' REMOTE USERS

INTRODUCTION

During a live Q&A webinar in April, a panel of cyber security experts from Censornet addressed audience questions on securing remote users.

This eBook has been created as a helpful resource with tips and advice from the insightful webinar.

Topics covered include:

- Industry standards and best practice
- Split tunnelling
- Unmanaged devices
- Securing Microsoft 365, BYOD and Virtual Desktop Infrastructure (VDI)
- Secure cloud gateways
- Securing collaboration tools like Microsoft Teams
- The resilience of the cloud
- Load balancing
- Secure Authentication
- Remote working checklist

4 TOP TIPS

1_ Use MFA everywhere possible, particularly on privileged / administrator and other highly sensitive accounts

2_ Use split tunnelling to deliver a superior user experience and maximise performance

3_ Secure all devices with agents

4_ Use CASB to secure cloud applications and manage their use, ideally combined with federated identity

INDUSTRY STANDARDS AND BEST PRACTICE

There is plenty of best practice advice that can be drawn upon, including standards from the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), as well as guidelines from the National Institute of Standards and Technology (NIST).

ISO 27001 is all about building and maintaining an information security management system (ISMS). This generalist standard provides many relevant controls throughout the different areas it covers that can be interpreted and implemented as specific technical controls.

The NIST publications (NIST SP 800-46 Rev. 2 & NIS T SP 800-53 Rev. 4) on the other hand go into more detail specifically in relation to securing remote working and devices.

NIST SP 800-46 Rev.2
Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
More information >

NIST SP 800-53 Rev.4
Security and Privacy Controls for Federal Information Systems and Organizations
More information >

ISO 27001
The international standard for information security management
More information >

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO 27100

The international standard for information security management

Although ISO 27001 is not particularly prescriptive in detail and depth around the technical controls that need to be implemented across an organisation's IT environment, 6.2 of the standard refers to mobile devices and teleworking.

It simply states that a policy and supporting security measures shall be implemented to protect information accessed, processed, or stored at teleworking sites. However, there are other standards that are far more prescriptive in terms of technical controls.

ISO 27001 is focused on operational security, rather than how to build a secure environment or infrastructure in the first place.

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

The NIST publications (NIST SP 800-46 Rev. 2 & NIST SP 800-53 Rev. 4) on the other hand go into more detail specifically in relation to securing devices.

As a minimum:

- Ensure the **operating system (OS) is patched** and fully up to date (enable automatic Windows updates for example)
- **VPN client software must be updated** and current to ensure known vulnerabilities are not present in VPN client software
- **Anti-malware software, also known as Endpoint AV, needs to be installed** with automatic signature updates enabled where available
- Make sure the device is protected with a (personal) **firewall** - even if it's the basic firewall included with Windows (Windows Firewall)
- A **web security policy must be enforced** to stop access to inappropriate or malicious sites. Consider blocking downloads of dangerous file types, such as executables or PE files that may be malicious or represent unapproved applications
- Implement a **strong password policy alongside Multi-Factor Authentication (MFA)**, also known as two-factor authentication or 2-step verification. Many SaaS vendors support MFA

NIST SPECIAL PUBLICATION (SP) 800-46 REV. 2

NIST Special Publication (SP) 800-46 covers enterprise teleworking, remote access, and BYOD security, providing security considerations and recommendations for several types of remote access solutions. It recommends that all devices are secured against expected threats and offers advice on creating security policies.

NIST SP 800-46 - Four Remote Access Architectures

- Tunneling – includes IPsec VPNs
- Portal – includes SSL VPNs, Remote Desktop Services, VDI
- Remote Desktop Access (e.g. GoToMyPC, TeamViewer)
- Direct Application Access (e.g. Webmail)

Point 2.2 in the guide describes four remote architectures to consider for remote users:

1. Tunnelling

This includes the use of IPsec Virtual Private Networks (VPNs) which send and receive data via a tunnel across the public internet secured using encryption.

2. Portals

This includes technology such as SSL VPNs but also Remote Desktop Services (formerly known as Terminal Services) frequently used by administrators to perform remote maintenance. Virtual Desktop Infrastructure (VDI) solutions are also covered, such as Citrix. The user is typically presented with some sort of landing page or portal or virtual desktop to onwardly access applications and services.

3. Remote Desktop Access

This includes solutions such as GoToMyPC or TeamViewer which gives a remote user control of a specific PC with keyboard, video, and mouse. These tools are used by support teams to provide ad hoc troubleshooting.

4. Direct Application Access

Webmail is referenced as the primary use case for direct application access as the publication was issued before widespread adoption of the cloud. Direct Application Access is now far more common as users have direct internet breakout locally to access applications such as Microsoft 365 or Salesforce.

NIST SPECIAL PUBLICATION (SP) 800-53 REV. 4

NIST SP 800-53 Rev. 4. provides more detail on specific security and privacy controls that should be implemented in relation to remote working (or teleworking). **Table 1** shows some of the key controls to implement with corresponding control numbers.

In terms of **remote access** NIST SP 800-53 highlights the need to document remote access, authorise access, monitor the use of remote access technology and to use encryption. Encryption is standard within all VPN solutions whether they are IPsec or SSL based.

The inclusion of two controls for **authentication**, IA-2 and IA-11, drives the point home that it is vital to the security of organisations that they can verify whoever is logging in is who they claim to be. IA-2 covers the use of Single or Multi-Factor Authentication (MFA). Passwords are the most common form of single factor. The use of certificates or hard/soft tokens should also be considered. Not only is MFA recommended at initial logon, organisations should also consider requiring remote workers to **re-authenticate**, particularly during long remote access sessions, if a user is online for longer than eight hours. Idle time is also mentioned - after 30 minutes of idle time, the advice is that users should again be asked to re-authenticate.

TABLE 1

NIST SP 800-53 Rev. 4
Remote Working – Relevant Controls

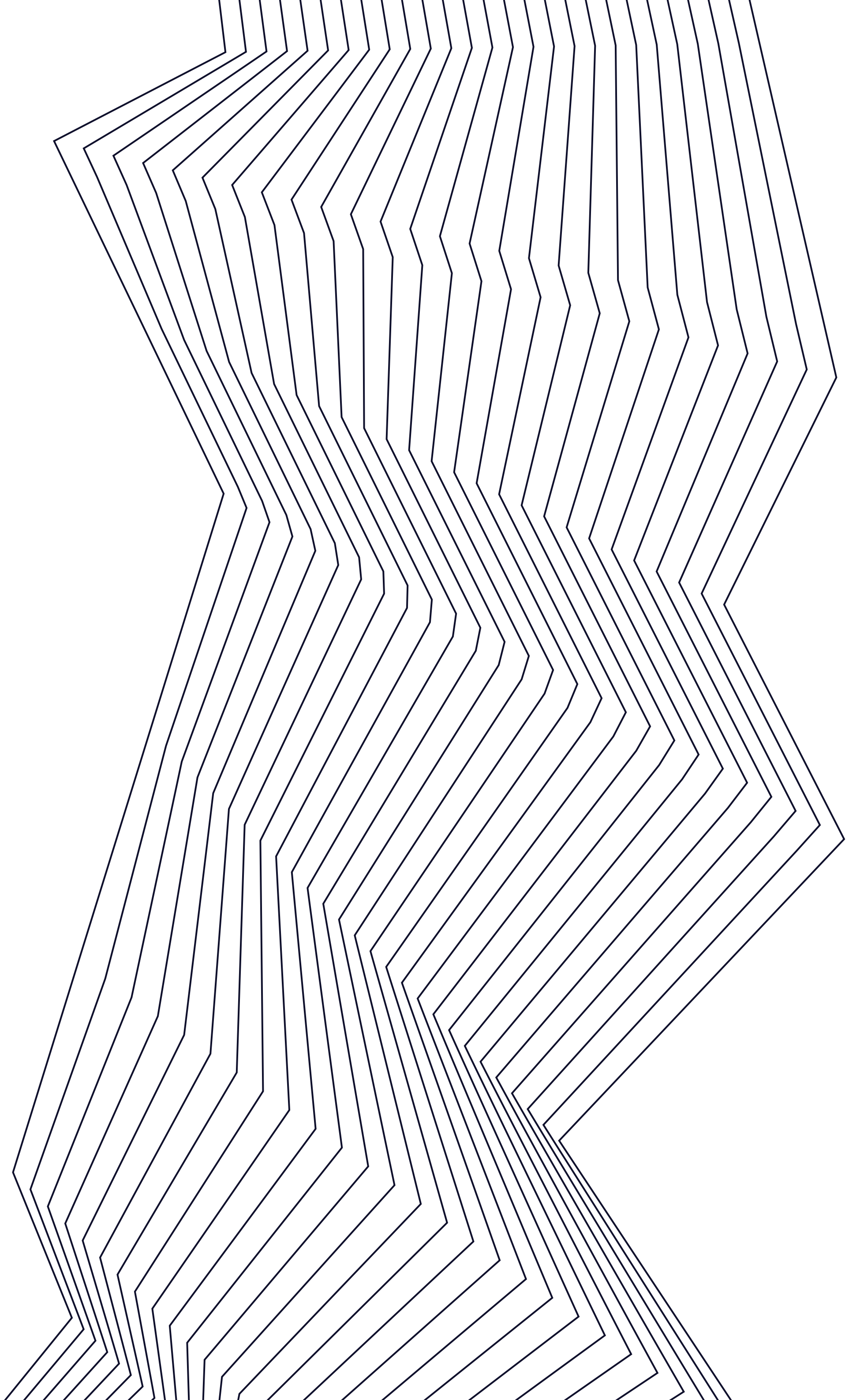
CONTROL	SP800-53	IMPLICATIONS
Remote Access	AC-17	Documenting remote access – authorizing access, monitoring, encryption etc.
Identification and Authentication	IA-2	Single or Multi-Factor Authentication – passwords, certificates, hard/soft tokens
Re-Authentication	IA-11	Require remote workers to re-authenticate during long remote access sessions
Risk Assessment	RA-3	Assess risk when selecting a remote access solution (tunneling, app portals, direct application access)
Boundary Protection	SC-7	Network segmentation, monitoring and controlling communications at key boundary points
Transmission Confidentiality and Integrity	SC-8	Protect transmissions through use of cryptography

NIST SP 800-53 REV. 4 CONTINUED...

Risk Assessment. When selecting an architecture or a technology, or combining various technologies, a risk assessment that considers the confidentiality, sensitivity, and to what degree data associated with a particular application is regulated should be carried out to determine the level of security and the controls that should be implemented.

Boundary protection covers the use of network segmentation to separate publicly accessible infrastructure from internal infrastructure. Key boundary points will be determined by the architecture and technologies used for remote access.

Within SP 800-53 there are a series of controls relating to **transmission confidentiality and integrity**. These controls are about protecting data in transit, linking back to the controls in AC-17 that cover encryption, which is standard within all VPNs almost by definition.



TIPS & FAQS

SPLIT TUNNELLING

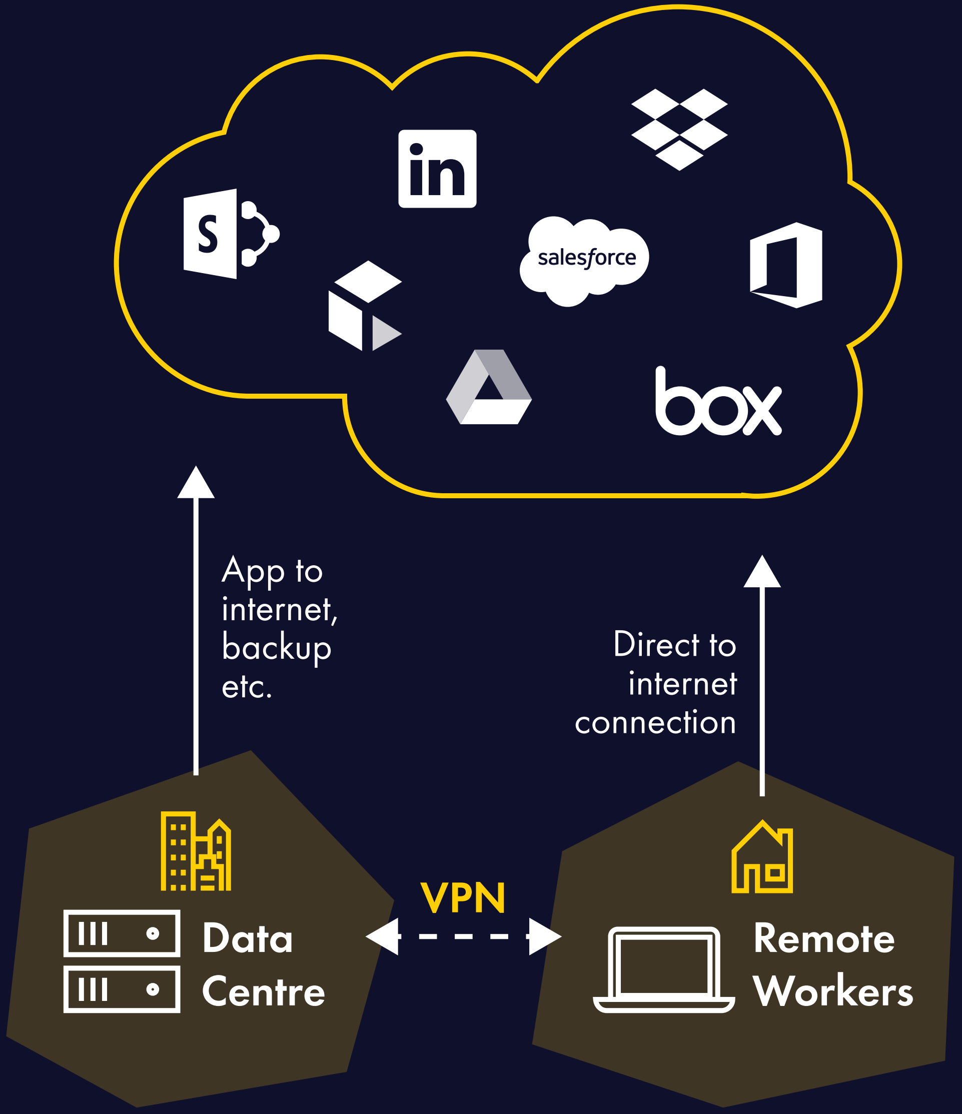
One of the things that is not mentioned in the NIST document is **split tunnelling**, which is now a very common configuration.

Remote users, as illustrated in the bottom right hand corner of the diagram, are able to access applications and data within a data centre environment – or private cloud – over a VPN.

Users also have simultaneous access to cloud applications using local direct internet breakout.

Microsoft's own best practice advice for Microsoft 365 recommends direct to internet connections whenever accessing Microsoft 365 applications and data. Split tunnelling enables users to access on premises applications whilst accessing cloud apps directly and therefore meeting Microsoft's recommendations.

Censornet's unique architecture supports split tunnelling and therefore direct to internet connections, with agents on endpoint devices used by remote workers. Data centre environments can also be protected using the Censornet Cloud Gateway to protect application to internet traffic (when data is backed up to the cloud or moved into cloud CRM or other cloud apps for example).



RISKS AND SECURITY OF UNMANAGED DEVICES

If remote users are using untrusted, unmanaged personal devices then the state and health of that device is likely to be unknown. Software on the device may be unpatched and out of date, the device may be poorly configured, security software may not be up to date or even installed at all, and there is a possibility that malware is present on the device. Therefore, allowing access to corporate systems, services and data is risky.

How to mitigate the risks from unmanaged devices:

- Many VPN solutions include client integrity checking or posture management features. Before a device is allowed remote access the state and version of AV software running on the device, for example, is checked. If AV is missing or out of date the device may be given restricted access to enable the user to install up-to-date AV software before being granted access to on premises applications and data.
- Implementing a Virtual Desktop Infrastructure (VDI) solution helps eliminate the risks associated with unprotected devices and provides an environment where users can login to a managed and protected virtual desktop.

SECURING EMPLOYEES WORKING FROM DIFFERENT HOME LOCATIONS

Whichever architecture and technology, or combination of architectures and technologies, are chosen, it is recommended that a split tunnelling model is supported, only sending traffic that's destined for the application in the data centre over the VPN with local breakout for all internet traffic. This model delivers a superior user experience and accelerates performance of Microsoft 365 for example.

METHOD 1 - VPN into a corporate location protected with a gateway When providing internet access via a VPN rather than local breakout, as well as to secure application to internet traffic to and from the data centre, instrument gateway-based protection using the Censornet Cloud Gateway. With gateway protection security policies are applied to all internet traffic. It is possible to provide content filtering, DLP and malware scanning, and image content analysis to protect staff from NSFW images and videos.

METHOD 2 - Deploy an agent on the endpoint
In the current climate - with more and more people working from home – implementing protection with endpoint agent software that provides both Web and Cloud Application Security (CASB) is increasingly common. Agents enable organisations to comply with Microsoft best practice advice for accessing Microsoft 365 over direct to internet connections without sacrificing security. Application performance, and therefore the user experience, is improved.

Enabling agents on endpoints will give you the visibility and control to:

- Prevent access to malicious websites, inappropriate content and manage time spent on websites that impact productivity
- Stop users downloading unsanctioned applications, by blocking executable files
- Restrict specific actions within cloud applications, such as sharing sensitive information via cloud storage apps
- Support and protect direct to internet connections for remote / mobile users

SECURING MICROSOFT 365, BYOD AND VDI

Securing Microsoft 365 - particularly when users are using personal devices - is a significant challenge, even for larger organisations with significant resources. But there are several ways in which BYOD can be accommodated without putting the organisation's information assets and networks at risk.

Implementing a **Virtual Desktop Infrastructure (VDI)** solution enables users to use their personal devices to access a centrally configured and managed environment. Once configured, it ensures that the organisation's infrastructure is isolated from potential threats posed by the state of personal devices. Elements deployed within the VDI solution are updated centrally and where possible automatically, reducing the ongoing overhead on smaller IT teams.

Another solution is to use cloud application security (or Cloud Access Security Broker (CASB)) combined with Identity as a Service (IDaaS), sometimes called Cloud Identity and Access Management (IAM), that supports federated identity. Federated identity standards replace passwords with tokens or assertions to authenticate to applications, including Microsoft 365.

Some of the common federated identity standards include Security Assertion Markup Language (SAML), OpenID Connect (OIDC), OAuth and Microsoft Active Directory Federation Services (ADFS).

Using IDaaS combined with CASB ensures that all cloud application access is over channels that are instrumented, or protected, with CASB. As users no longer have a username and password to log in, they cannot pick up any device and simply log in to cloud apps. Whenever they log in the session is redirected via the Identity Provider (IdP) to the application and the session is therefore subject to CASB management for both visibility and control.

Another consideration is the use of mobile apps. Many cloud applications have corresponding mobile apps – including some Microsoft 365 apps, salesforce, Dropbox, box, LinkedIn, for example. Mobile apps increasingly use end-to-end encryption through the implementation of SSL pinning, making CASBs 'blind' to user activity and interaction with data via those mobile apps. CASB API mode can restore visibility across a subset of cloud applications.

Another approach is to use **Mobile Device Management** (MDM) or **Enterprise Mobility Management** (EMM) solutions to enforce policies on mobile devices that prevent users from using mobile apps and forcing them back into the browser, where CASB coverage is 100%. Microsoft's MDM product, Intune, is included in some Microsoft 365 plans.

MDM, or EMM tools, require users to enrol devices and give the organisation the ability to remote wipe some or all data, leading to a natural reluctance from some individuals to use MDM, particularly if they have large amounts of personal data such as photos and videos on their devices.

There are obvious pros and cons to different architectures and combinations of technology. A risk assessment can help make informed choices based on an organisation's unique attributes, operations and risk appetite. Some applications and data may be assessed as so sensitive that access is restricted to corporate owned devices. Other applications and data may be less sensitive with access from personal devices considered acceptable.

SECURING COLLABORATION APPLICATIONS

Up until about 18 months ago the majority of organisations implemented cloud application security, or CASB, purely to discover which applications were being used and to provide visibility into how users were interacting with cloud applications and more importantly associated data. Perhaps in part triggered by the introduction of GDPR, organisations have since moved beyond visibility and towards managing what users can do within cloud applications. Apps that allow users to upload, download, send, attach, transfer, or share files are a particular concern.

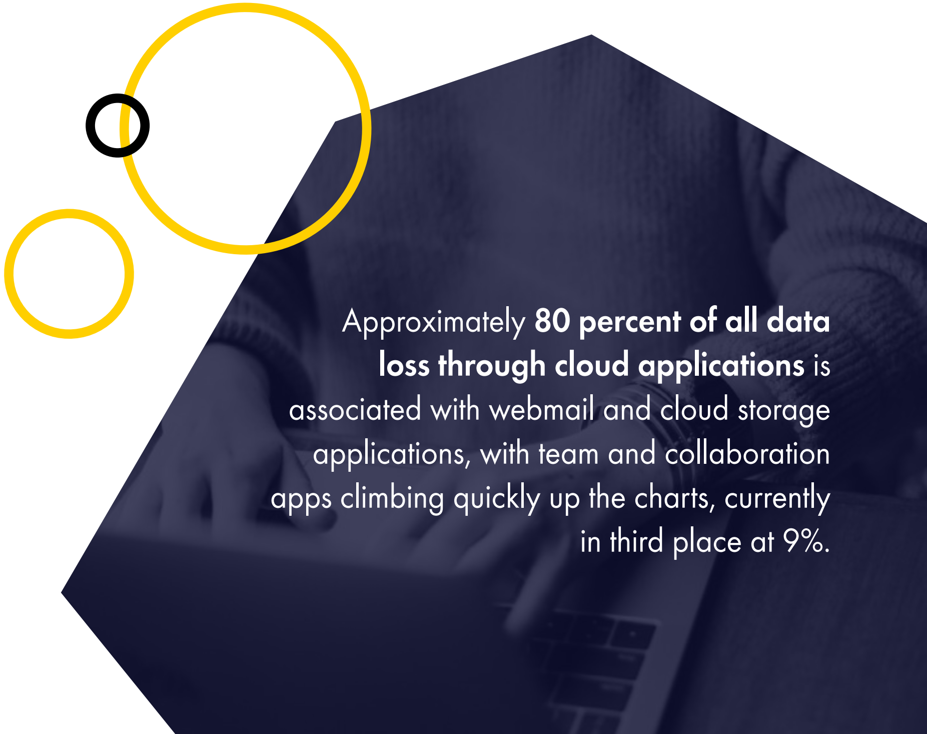
The recent push to homeworking has driven a 70 percent spike in usage of Microsoft Teams

The main challenge for security professionals when unleashing users onto collaboration apps, like Microsoft Teams, is **data security**. Team and collaboration apps provide another route for employees to share and send files to other users and meeting attendees, so there is an inherent risk of sharing the wrong data with the wrong person, by accident, through negligence or with intent.

For highly regulated industries, such as financial services, keeping an audit trail of conversations and recordings of meetings is a key requirement. For some organisations there is an absolute hard compliance requirement to record all conversations, all chats that relate to financial transactions and to retain them for long periods of time.

Cloud applications security (CASB) combined with IDaaS is the suggested solution. Implementing CASB and IDaaS ensures all access to team and collaboration applications is via an instrumented or managed channel with security and monitoring controls provided by CASB technology.

Some thick client or desktop applications, as well as some mobile apps, use HTTP and HTTPS under the covers. Therefore, some CASBs will have the ability to manage a subset of thick client applications and mobile apps and be able to block certain actions. However, not all CASBs are equal and the features and functionality provided by different CASB vendors varies significantly. To achieve the highest level of security around the use of such applications, the solution is to not allow the use of the applications at all. Using browser-based versions of the applications ensures 100% CASB coverage with the ability to block actions in real-time.



Approximately **80 percent of all data loss through cloud applications** is associated with webmail and cloud storage applications, with team and collaboration apps climbing quickly up the charts, currently in third place at 9%.

THE RESILIENCE OF THE CLOUD

The cloud in general has the capacity to cope with the recent large-scale change to working patterns and practices. Despite some issues during the initial shift to remote working, GoToMeeting and Microsoft Teams were among many that were caught off guard by the spike in usage, these early issues have largely been overcome. Some limitations remain but these are localised to specific regions or countries.

The main issue has been around bandwidth availability when working remotely. With significantly more users working from home contention on consumer broadband or ADSL lines has impacted performance. Many users will have worked around this by switching to cellular data or using 4G routers and dongles.

During the initial weeks of lockdown some organisations took proactive action to reduce burden on infrastructure – such as Netflix reducing the quality of their video to cope with the demand. This is an option for other providers if they experience capacity issues.

For organisations who were already liberally using the cloud the volume of data is the same whether working from the office or at home – the user is still consuming the same cloud applications – although traffic patterns and profiles will be different. More people have moved to the cloud in recent weeks, but the cloud service providers have capacity, and initial issues seem to be dissipating.

As a cloud platform, Censornet ensures resilience with a cross-provider strategy using three of the major tier one cloud providers. Using world class service providers including IBM (with 10+ locations worldwide), Amazon and Microsoft, enables consistent, lightning fast response times across the whole platform globally.

Censornet Cloud Gateways can be used in conjunction with many load balancing solutions. Through our partnership with loadbalancer.org, all customers have a cost-effective load balancing solution available with deployment guides and step-by-step walkthroughs. If a load balancing solution is not available simple proxy auto-config (PAC) file logic can be used as an alternative to achieve the same outcome.

When adopting a new cloud solution, it is recommended that an amount of due diligence is performed to allay any concerns around uptime, availability, and performance.

SECURE AUTHENTICATION

Knowing that users logging into your systems are who they appear or claim to be is more important than ever.

A valid email address is now used as the username across the majority of systems, services, and applications. Email addresses are easily validated and unique. However, given the seemingly constant stream of large-scale breaches, millions of email addresses and passwords are available on the Dark Web. Organisations should therefore strongly consider using more than just a password to protect user accounts.

Enabling context-aware or adaptive Multi-Factor Authentication (MFA) wherever possible protects accounts with more than just a password and requires users to enter a One Time Passcode (OTP) when logging in. OTPs are typically delivered in SMS text messages, by email or via a mobile app. Even if a malicious actor obtains a user credential, they are unable to gain unauthorised access to the user's account.

Numerous threat intelligence solutions are available that include monitoring of the Dark Web and forums for compromised email addresses. Subscribing to these services can identify stolen usernames but also identify repeat offenders who perhaps would benefit from additional education. Where budget is not available for these services there are free resources available including websites such as haveibeenpwned.com where individual email addresses can be manually checked against known breaches.

Implementing MFA does not reduce the need for strong passwords.

If an organisation has an adaptive MFA solution in place - that examines contextual information about the user, the device, location, time of day, day of week, when the user is trying to authenticate, then changes to password policies may be considered. Whilst the length and strength or complexity of passwords should not be altered it may not be necessary to change passwords as frequently. For example, it may be acceptable to relax password change policies forcing users to change passwords every 60 or 90 days instead of 30.

Strong passwords are still highly recommended as it is common for MFA solutions to be bypassed or disabled for specific users from time to time. The user may have lost or forgotten their mobile phone for example and be unable to receive One Time Passcodes via text or in an app on their phone.

4 STEPS TO REDUCE THE IMPACT OF USER LOGIN CREDENTIALS BEING AVAILABLE ON THE DARK WEB

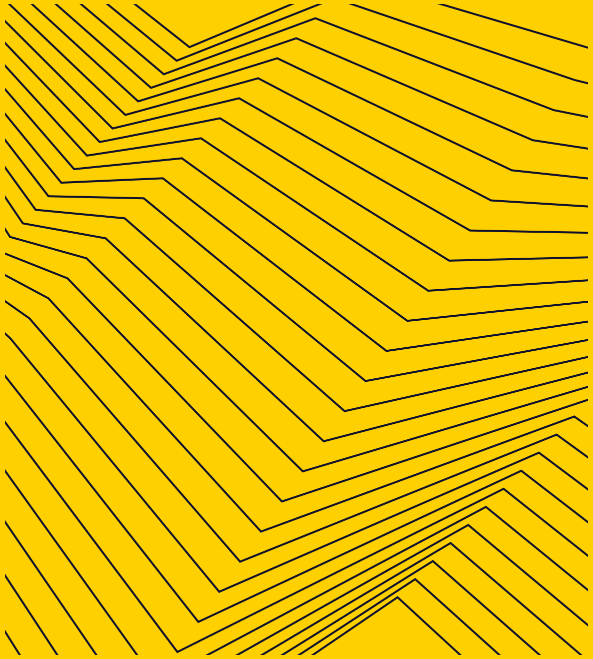
1_ Wherever possible enable context-aware or adaptive MFA solutions. This prevents access to user accounts even if credentials are lost, stolen, or otherwise obtained (through guessing, cracking or phishing for example)

2_ Some threat intelligence providers monitor the Dark Web, participate in forums, and alert companies when identities appear where they should not. But they are not within every organisation's budget.

3_ Build a database of stolen identities and update it regularly. Run access logs against the database.

4_ Free services such as haveibeenpwned.com are a good place to start if budgets are limited.

WHAT IS THE ONE THING THAT WILL MAKE THE BIGGEST DIFFERENCE DURING THIS TIME?



Enabling **Multi-Factor Authentication (MFA)** everywhere it is available and implementing it in front of cloud applications is the single most impactful step organisations can take to improve their security posture. This is highlighted repeatedly in security surveys and reports including the Verizon Data Breach Investigations Report (DBIR).

MFA should be considered critical for administrator accounts. If your organisation uses IaaS and/or PaaS solutions - such as Amazon Web Services, Google Cloud Platform or Microsoft Azure - MFA should be enabled immediately to protect privileged accounts. If attackers gain access, they have the ability to annihilate the entire virtual enterprise within minutes.

It goes without saying that Censornet customers should enable MFA to protect all admin accounts on the Censornet platform.

During this period of uncertainty, it is more important than ever to ensure you have the correct solutions in place to secure your workforce when working from home.

Review the remote working checklist which highlights the key areas that should be considered to ensure your business can continue to operate effectively and securely at this time.

REMOTE WORKING CHECKLIST

- Ensure all users devices have endpoint antivirus installed and are up to date.
- Review existing VPN settings and policies to ensure users only have access to the things they are meant to.
- Be wary of allowing VPN access from untrusted devices, if however, you are allowing users to work from personal devices and VPN into the office, then ensure you're posture checking these devices on your VPN solution – for example, checking they are running up to date AV.
- Consider enabling split tunnelling for users to access the internet and applications like Microsoft 365 directly from home and only send specific traffic over a VPN to applications that need it i.e. on-premises applications.
- Re-instrument gateway protection directly on the endpoint using agents to provide web and cloud application security and ensure head office protection is not sacrificed or bypassed for users working from home.
- If your VPN environment cannot cope with the increase in user capacity, then consider the other options you have for providing remote access to internal applications – such as Remote Desktop Services (RDS), or Virtual Desktop Infrastructure (VDI).
- Review your authentication process to ensure you have adaptive Multi-Factor Authentication (MFA) in front of your cloud applications and any connections back to your corporate environment.
- Resist short term changes to firewall rules which could weaken your security posture.

censornet.

Leveraging cloud security can expedite a secure remote working environment, and with Censornet everything is consolidated into one platform, allowing you to monitor and secure your workforce wherever they may be.

To discuss how Censornet can help securely enable your remote workforce, contact us today
+44 (0) 845 230 9590 or drop us a line at **sales@censornet.com**

We would love to hear from you.