YOUR OFFICE 365 JOURNEY

Securing every stage

With exclusive recommendations from
cloud migration and security leaders

censornet.

Contents

Transforming your Office 365 migration

For almost a decade, Microsoft's cloud service, Office 365 (O365), has been revolutionising the working lives of employees. With over 180 million monthly active users[1], O365's connectivity, agility and user experience have helped boost the performance of organisations in almost every sector, in every industry, across the globe.

But the cloud, and O365, carry risks. Despite its benefits, O365 cannot deliver the level of protection and availability that organisations truly need for advanced security and performance. The reality for most professionals migrating to O365 is a complex transition to the cloud, alongside challenges of cyber security, user experience and data management.

To help professionals defeat top migration challenges and deliver an uncompromising O365 experience, Censornet has combined its trusted cyber security expertise with exclusive insights from some of the cloud and security industry's most prominent thought-leaders, to bring you actionable steps and migration recommendations.

Whether you are preparing for, migrating to, or strengthening the performance of your O365 environment, this report will help you maximise the security of your O365 environment – whilst enhancing user experience – guiding you on how to:

- **Prepare and migrate to O365 securely.**
- **Overcome key migration challenges with tangible, step-by-step advice.**
- **Build an agile and secure O365 environment – even if you have already migrated.**

Are you ready to begin your Office 365 transformation?

[1] - https://office365itpros.com/2019/04/25/office-365-reaches-180-million-users/

INTO THE CLOUD

Your cyber security snapshot

The unwavering growth of O365

Today's working landscape is unlike anything we've seen before. In order to achieve greater agility, security and functionality for their business, organisations are rapidly increasing their investment in computing resources[2] from cloud providers such as Amazon, Microsoft and Google. With lower total cost of ownership than their on-premises counterparts, and with the promise of greater flexibility, it's no longer a question of if, but when organisations will adopt cloud ecosystems.

83% OF ENTERPRISE WORKLOADS WILL BE IN THE CLOUD BY 2020[3].

By user count, O365 is the most widely used public cloud service in the world. One in five corporate employees now use an O365 cloud service[4], and this number is expected to sky-rocket even further over the next few years.

But tension is building.

Despite O365's convenience and usability, organisations of every size are experiencing challenges that are preventing them from migrating to O365 successfully and securely. These roadblocks not only impact the delivery of the platform but are actively putting organisations at risk.

> "The biggest O365 adoption driver is business value – the amount of new solutions, capabilities and innovations that weren't available on-premises. They increase productivity and new ways of collaboration significantly."
>
> Ragnar Heil, Channel Account Manager, EMEA Central & Microsoft MVP

[2] https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

[3] https://hostingtribunal.com/blog/cloud-adoption-statistics/

[4] https://blog.goptg.com/microsoft-office-365-statistics

Common Office 365 migration challenges

Cyber security

O365 cannot defend organisations against sophisticated threats such as phishing attacks and CEO Fraud.

Compliance

Processes, workflows and data flows within O365 must remain compliant with regulations like GDPR.

User experience & availability

Slow performance, misconfiguration, outages and downtime of apps within O365 can impact entire organisations.

Data security & management

Unstructured data, data sprawl and loss within O365 and other cloud applications put organisations at huge risk.

ACCORDING TO IBM, THE AVERAGE TOTAL COST OF A DATA BREACH FOR AN ORGANISATION IS $3.92 MILLION[5].

[5] - https://www.ibm.com/security/data-breach?_ga=2.188655662.704062468.1571907511-261936100.1571907511&cm_mc_uid=4-2771413167815719075104&cm_mc_sid_50200000=80196561571907510429&cm_mc_sid_52640000=67897561571907510445

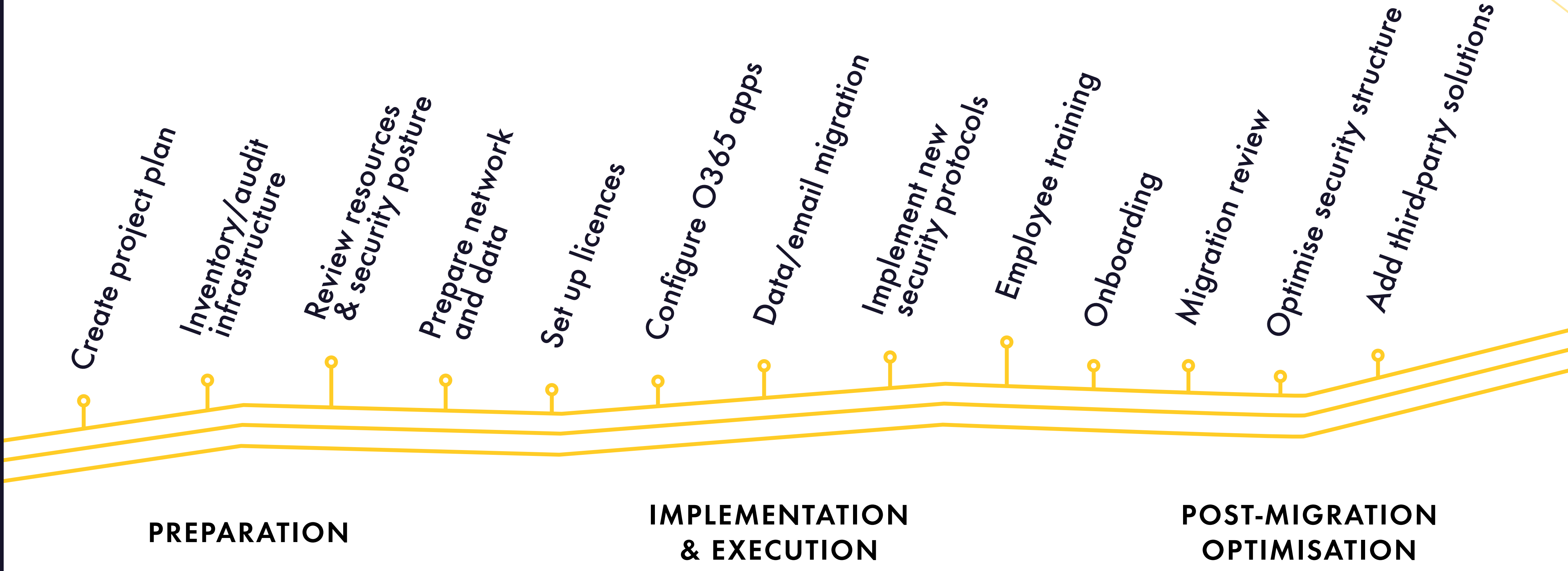
Building an unshakeable foundation for O365

> "O365 demands a complete mindset change. You need the skillset, toolset and mindset in the digital workplace."
>
> Michael Greth, SharePoint & Office 365 Specialist and Microsoft MVP

To deliver the flexible working environment that O365 offers, security professionals must create a strong foundation on which to build. This includes implementing procedures that will strengthen the performance and security of O365 at every stage of the migration journey – and beyond.

As we further explain in *Phase 1 – Preparation: Building a solid O365 infrastructure*, this begins by setting realistic and actionable targets against a migration timeline, and ends with the continual optimisation of O365's security features.

Your O365 migration timeline



Create project plan

Inventory/audit infrastructure

Review resources & security posture

Prepare network and data

Set up licences

Configure O365 apps

Data/email migration

Implement new security protocols

Employee training

Onboarding

Migration review

Optimise security structure

Add third-party solutions

PREPARATION

IMPLEMENTATION & EXECUTION

POST-MIGRATION OPTIMISATION

For small to mid-sized organisations, prepare for a 2-3 month timeline, enterprises 5-6 months[6].

> "Planning, and planning around user adoption are two pieces of advice I would give an organisation about to start their migration."
>
> Ian Moyse, EMEA Sales Director at Natterbox Limited

[6] https://www.quadrotech-it.com/blog/how-long-migrate-to-office-365/

PHASE 1

PREPARATION

Building a solid Office 365 infrastructure

Uncovering O365's blind spots

Before you start your O365 journey you must have a 360-degree understanding of the suite so that you can make effective security decisions throughout your migration. This includes understanding how O365 can make your organisation safer and more agile, as well as where you need to build on its security blind spots with additional solutions.

COMPLIANCE

Multiple 'Security Centres' provide insight into user interaction with apps and data.

BLIND SPOTS

- Multiple dashboards mean no single view of the entire O365 suite.
- SIM/SEM integration is needed for full visibility and a comprehensive audit trail.

DATA SECURITY

Data is secured at rest in Microsoft's data centres, while Azure Information Protection (AIP) makes data classification and Digital Rights Management (DRM) more accessible.

BLIND SPOTS

- DLP policies offer only partial coverage of O365 workloads.
- Limited content scanning can lead to data loss through malicious or accidental sharing.

AVAILABILITY

O365's component services are highly distributed, limiting the impact of downtime, and in the event of a failure, internal monitoring services drive automated recovery.

BLIND SPOTS

- Microsoft's uptime SLA of 99.9% allows for 8 hrs, 45 mins, 57 secs of downtime per year.
- Limited outage protection without third-party services on a separate infrastructure.
- Azure AD outages can have a significant impact on user and admin access.

DATA MANAGEMENT

With careful planning, SharePoint and OneDrive organise and store documents centrally, and tools like OneNote can help organise informal, unstructured data.

BLIND SPOTS

- DLP policies aren't automatically enabled or easily assigned to single regions or groups.
- Data sprawl across O365 gives users unauthorised access to data.
- 80–90% of data in O365 is unstructured, moving the problem to the cloud.

USER EXPERIENCE

Easy file access from anywhere, added efficiency with collaborative tools like SharePoint and Teams, plus operability on a range of devices with dedicated mobile apps.

BLIND SPOTS

- O365 uses constant connections, putting stress on infrastructures like firewalls and proxies.
- Microsoft advises direct-to-internet connections, bypassing proxies and security controls.
- Bandwidth-intensive apps may suffer, leading to broken video and audio or long download times.

CYBER SECURITY

Security against traditional email attacks with Exchange Online Protection (EOP), while Advanced Threat Protection (ATP) adds Safe Attachments and Safe Links to block malicious files. Also, security updates are mostly automated.

BLIND SPOTS

- Limited protection against zero-day attacks and highly targeted threats like CEO fraud/ impersonation.
- Phishing catch rates are much lower than with third-party security solutions.
- O365 does not include web security, reducing protection against multi and cross-channel attacks.

Establishing a strong migration framework

Common O365 pre-migration challenges

Unaligned teams

Stakeholder expectations are not met, and teams are uncoordinated for project delivery.

Unprepared networks

Unaware of O365 requirements, networks and data are left unstructured for migration.

Data loss

Experiencing a breach or attack and subsequent data loss during cloud migration.

> "Integration between the old world and new world is important. You have to create a high-level roadmap that goes long term."
>
> Sven Ringling, Director at Adessa

We know that if ignored, these challenges can not only damage the long-term success of an O365 migration project but also put the immediate security of an organisation at risk.

To prevent these pre-migration challenges from disrupting your O365 deployment, we recommend implementing a detailed framework at the very beginning of your migration project. Not only will this create a strong foundation from which you can migrate, but it will also reinforce internal alignment between various teams.

To help you design your framework, and avoid common pre-migration pitfalls, our *Organisational Inventory and Migration Checklist* includes some of the most important steps organisations must take to prepare for O365. Organisations who migrate without this structure in place will accrue additional costs, require more resources and increase their risk of a security breach and data loss.

Organisational inventory and migration checklist

> One of the biggest challenges of migration is that people don't recognise that it's a significant move – it needs to be planned and staffed.
>
> Bernard Golden, Former Vice President of Cloud Strategy at Capital One

Set deployment goals and targets

To avoid misalignment and confusion, set expectations with internal stakeholders through a project plan outlining key timelines, budgets and goals for deployment – as well as reaffirming which O365 features you will implement based on employee needs. This step includes liaising with legal and procurement teams who can block cloud migration projects if they aren't consulted during the pre-migration phase.

Determine your unique requirements

Every organisation will have individual user, compliance, security and data management needs – in order to stay secure and compliant, you must determine if Microsoft will meet these or where additional resources will be necessary. For example, organisations within the finance or legal sector may need additional compliance capabilities over and above what O365 provides.

Run a network health and readiness test

Prevent network latency in O365 disrupting the performance of your organisation by using tuning protocols and solutions, such as Microsoft's Deployment Readiness Tool, for network/bandwidth assessments to see whether your existing and forecasted internet connectivity meets the requirements for O365. Meeting these specifications can often be achieved with network or internet egress infrastructure changes, otherwise you may need additional investment to optimise connectivity.

Inventory of your current environment

Whether you are adopting a cloud-only or hybrid environment, auditing your current infrastructure is a crucial step as it will indicate the scale of your migration. Identifying mailbox sizes and item counts, files/folders and all business-related content will also help you avoid risks such as data sprawl or Shadow IT.

Decide what data you are going to move

It's important to take a data-centric approach to migration and continue to use this model throughout your usage. During your preparation phase, remain compliant with GDPR requirements and streamline data management by identifying which records, emails and files you are going to move to the cloud, and which you will delete or archive.

Evaluate your current security posture

A critical part of pre-migration is analysing your security model to identify any areas of vulnerability. It's crucial to evaluate whether your existing controls and policies will remain the same post-migration, and if they are strong enough to ensure data and user protection in the cloud.

> "The difference between a successful move to O365 and months of misery often comes down to planning."
>
> Sean McDonough, Consultant at Bitstream Foundry & Microsoft MVP

Judiciously review your resources

After reviewing your current infrastructure, network capacity and security models, you must examine whether you will need third-party solutions to assist in your migration or additional security solutions to ensure the optimum performance and protection of O365. A poorly configured O365 migration could cost an organisation far more than just their time if they were to suffer data loss or a security breach.

PHASE 2

MIGRATION

Delivering a secure, seamless transition into Office 365

The cost of underestimating Office 365 migration

> "Don't under (or over) estimate the complexity of migration."
>
> Ragnar Heil, Channel Account Manager, EMEA Central & Microsoft MVP

It can be easy for professionals to underestimate the complexity of an Office 365 migration – under time pressure and with limited resources. But overlooking or misunderstanding critical steps leaves organisations vulnerable to cyber attacks and data breaches, and employees without access to business-critical O365 features.

Follow these six key steps to overcome common migration challenges of data security, user experience and fear of misconfiguration, and deliver a secure, seamless transition into the cloud.

> "The biggest migration roadblock is one of adequately and sufficiently understanding the details of the O365 onboarding and migration process, and all that it entails."
>
> Sean McDonough, Consultant at Bitstream Foundry & Microsoft MVP

6 steps to migration success

STEP [1] Set up licences and identity management

After setting up O365 subscriptions and licences for users, it's crucial to check that access rights and permissions are set correctly. This will ensure that users will only have access to data they need based on their functional role (or group membership) as well as preventing employees from accessing or sharing unauthorised data.

Censornet recommends...

If you are adopting a hybrid identity model and have already set up user identities in your on-premises Active Directory, you can create users in Azure Active Directory, and sync them to Active Directory on-premises. If you are moving to Azure AD and syncing users and objects from AD on-premises then this may be an opportunity to carry out a directory review (removing any duplicate or invalid users or objects) to ensure a "clean" transition.

> **"To make sure users can start easily on the Monday morning after migration, without any issues, they should have access to the right licence, the right permissions, the right content within the right workload."**
>
> Ragnar Heil, Channel Account Manager, EMEA Central & Microsoft MVP

STEP [2] Securely configure your O365 network

To successfully move to the cloud, you need to ensure that your internet connections are optimised to reduce the round-trip time (RTT) from your sites to the Microsoft Global Network. To facilitate this, Microsoft recommends allowing O365 traffic to bypass proxies and packet inspection devices as this shortens the network path to O365 entry points – improving connectivity and user experience.

Cloud migration pitfalls

Network latency, poor connection quality and disrupted services within cloud platforms such as O365, are often the result of overloading legacy network infrastructure such as firewalls, due to the number of concurrent connections the platform creates/ requires. This can lead to a frustrating experience for users and an increase in helpdesk and support calls.

> “Don’t underestimate traffic flow between your users and the cloud service.”
>
> Bernard Golden, Former Vice President of Cloud Strategy at Capital One

STEP [3] Coordinate the logistics of migration

Prioritise compliance

Having made an inventory of the data, files and emails you are going to migrate, and having tagged your data with the right classifications during the preparation phase, you must now implement safeguards to guarantee this data will be migrated, stored and used in a compliant manner. To ensure your O365 tenant is hosted in a data centre suited to your needs, you will need to ensure Microsoft's geo-location feature is active during migration.

Review your timeframe

You may need to consider a staged migration approach to move data as Microsoft caps the amount of data you can transfer in a single day (Exchange Web Services limit is 400GB a day for importing[7]). This allows you to move mailboxes in batches, or if you are a smaller organisation with less data, you may be able to implement a cutover migration, which facilitates a single batch move.

Cloud migration pitfalls

> "Everyone should realise that when you're using a cloud-based service of any kind, there's a shared responsibility for security. There's no way that Microsoft can be as expert at your business as you are – you have to bring that knowledge."

Bernard Golden, Former Vice President
of Cloud Strategy at Capital One

This is crucial to your O365 migration. Under European GDPR law, you are liable for the protection of data – and a penalty could cost you up to £20m or 4% of your annual turnover[8].

Censornet recommends

Avoid a 'lift and shift' approach. Tag your data in pre-migration with the right classifications to ensure that it is moved correctly with the right security policies.

[7] https://sharegate.com/blog/office-365-migration-pitfalls

[8] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties#targetText=What%20is%20the%20-maximum%20administrative,global%20turnover%20%E2%80%93%20whichever%20is%20greater.

STEP [4] Evaluate your O365 security model

The gaps in O365's default security settings, alongside O365's lack of web security, will leave you vulnerable against sophisticated threats post-migration. To create the strongest security model possible for your organisation, you must review third-party providers who can protect your internet and network connections before you are active in the cloud.

Cloud migration pitfalls

Poorly defined security models within public cloud platforms are a cyber criminal's dream. If you experience a data breach, impersonation attack or phishing scam, it is likely to be a result of not taking additional action to defend against the blind spots in O365.

Enforce MFA

Microsoft experiences over 300 million fraudulent sign-in attempts to their cloud services every day[9]. To protect accounts – particularly admin and privileged accounts and the data within your cloud – you must make Multi-Factor Authentication (MFA) a priority during O365 configuration to prevent attacks such as Account Take Over (ATO). For advanced security, use a third-party solution that can provide MFA across multiple Microsoft and non-Microsoft services, systems and applications.

> "The vast majority of organisations will improve their security when they move to the cloud."
>
> Sven Ringling, Director at Adessa

Strengthen DLP strategies

Take proactive action against data loss, sprawl and leakage in O365 by reviewing your DLP policies to ensure they are allocated to specific groups and regions as this is not automatically enabled. By implementing permission policies, you will not only ensure that the right access is easy for employees, but you will also reduce the risk of data being accidentally accessed or shared externally with the wrong people.

[9] https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

STEP [5] Train O365 advocates

Lower the security risk of human error and promote O365 adoption by providing employees with comprehensive training resources that will allow them to navigate O365 safely and efficiently. This should include education around how to spot social engineering attacks, best practices in storing and sharing data securely, as well as encouraging key stakeholders to act as O365 advocates – encouraging adoption by sharing with teams the relevance of these tools.

> **"Don't underestimate the user. They are more IT aware than ever before, but they are more susceptible than ever."**
>
> Ian Moyse, EMEA Sales Director at Natterbox Limited

STEP [6] Make O365 mobile-friendly

> **"You have to completely rethink your organisation to get all the benefits of the new platform. If you don't, you'll just have the same chaos on a technically more advanced platform."**
>
> Michael Greth, SharePoint & Office 365 Specialist and Microsoft MVP

To ensure that your employees can use all of O365's cloud/remote features, establishing the Mobile Device Management (MDM) service before O365 goes live is imperative. This will ensure that when mobile users access O365 on the go, they do so safely and securely.

PHASE 3

OPTIMISATION

Strengthening your Office 365 security posture

Improving O365's security and performance

O365's out-of-the-box configurations aren't designed to suit your organisation's unique needs or protect you from sophisticated threats. Microsoft is designed to build its security 80% of the way – they leave the other 20% for their partner ecosystem. If you want extended governance, extended capabilities and extended security then you must optimise O365's basic configurations, and review where third-party security solutions can enhance the protection and performance of your cloud environment.

> "O365's baseline of security doesn't mandate that it is right and secure enough for your level of acceptable risk in your business. You need to build on it."
>
> Ian Moyse, EMEA Sales Director at Natterbox Limited

Whether you've just migrated to O365 or have been using it for some time, now is the time to take action. This means using all available resources from Microsoft to improve your security posture and identifying which areas of your landscape will need additional third-party security solutions.

Post-migration advice

Use Secure Score to review your configuration and action Microsoft's recommendations. Regularly review dashboards and reports in O365's Security & Compliance Center, Compliance Manager, Cloud App Security and any SIEM tools you possess to implement new security practices based on their results.

Identifying warning signs and optimising O365

One of the most effective ways of protecting your organisation from advanced security threats and poor user experiences is by identifying warning signs of O365's misconfiguration or vulnerabilities. By identifying these signals, you can then optimise the configuration of O365 and implement additional third-party security solutions to create a truly powerful O365 environment for your employees.

To ensure that your organisation doesn't fall victim to an O365 data breach, attack or outage, you must look out for and fix these top four post-migration warning signs.

IDENTIFY

Slow-performing apps

If you're experiencing scenarios like broken video and audio in Teams, it is likely a result of network bottlenecks that happen when the traffic profile changes, overloading security infrastructure elements such as firewalls and content gateways. It is likely that your network doesn't meet O365's bandwidth requirements or hasn't achieved a direct-to-cloud connection.

OPTIMISE

O365's network connection

To reduce latency, Microsoft recommends breaking users out to the internet, bypassing proxies and packet inspections, to get direct access to the Microsoft Cloud. However, as O365 does not provide web protection, you will need additional security solutions that not only protect your data as it travels through these direct-to-cloud networks, but also implement URL filtering to block access to inappropriate, offensive, or malicious content across your organisation.

IDENTIFY

Phishing emails in inboxes

If you've recognised an increase in the volume of phishing emails and impersonation attacks entering your inbox, it is likely a combination of missing custom rules and configurations in Exchange Online Protection (EOP), and EOP's lower catch rate (compared to third-party solutions), which means it is unable to block these sophisticated threats from entering your cloud environment.

OPTIMISE

O365's cyber security

For the 92% of professionals who want the ability to block advanced threats, zero-day threats and ransomware attacks[10], it is imperative that you implement third-party solutions to prevent threats, like advanced phishing attacks, from wreaking havoc across your entire organisation. These should include:

Web security

To protect you from sophisticated malware threats, you will need third-party web security with advanced threat protection as O365 does not include web security.

Advanced email protection

Alongside enforcing email encryption policies, you should look for a third-party email security provider that takes an ultramodern, multi-layered approach to email security, incorporating a range of tools and technologies to protect against the entire spectrum of email threats.

CASB access controls

You will need a solution that provides granular access controls to every feature and function for greater control over cloud applications and users.

Integrated threat intelligence

Threat intelligence is becoming increasingly relevant and valuable in identifying threat actors with a history of registering and weaponising domains. Consider vendors that demonstrate integration with multiple threat intelligence feeds.

[10] - https://assets.cloud.im/prod/Content/docs/ZEROSPAM-WP-Supplementing-the-Limitations-in-Office+365.pdf

IDENTIFY

Users accessing restricted data

If your employees have access to data that they previously did not have on-premises, it is likely that you haven't established policies or access controls that are in-line with your organisations needs, and you could be at risk of a data breach. If employees copy data to other locations that activity exacerbates data sprawl.

OPTIMISE

O365's MFA

You can protect all users from scenarios like ATO and data leakage by implementing MFA across every service, system and application your employees will use as O365's MFA does not work on non-Microsoft services.

> "The biggest challenges I see tend to revolve around maintaining a consistent identity strategy for users as the organisation goes through the O365 onboarding process and decommissions some of their own network/server assets."

Sean McDonough, Consultant at Bitstream Foundry & Microsoft MVP

IDENTIFY

O365 downtime

Unfortunately for Microsoft users, experiencing downtime whilst using O365 features is inevitable. Not only is the outage of services like Azure and Exchange Online frustrating, but without access to critical services like email, the productivity and profitability of your entire organisation can come to an immediate and costly stop. According to Gartner, the average cost of network downtime is around $5,600 per minute, or $300,000 per hour[11].

OPTIMISE

O365's availability

Microsoft's SLA of 99.9% means that your organisation will experience 8 hours and 45 minutes of downtime each year. To ensure your organisation's backup capabilities are able to maintain email services even during a Microsoft outage, you will need to implement proactive strategies such as the use of Emergency Inboxes.

[11] - https://www.itondemand.com/2018/05/29/costs-of-downtime/

Enhancing O365's security and performance

One of the most common misassumptions we see professionals make post-migration is that O365's default security settings are enough to protect their organisation against today's complex threat landscape and sophisticated attacks.

Microsoft's cloud infrastructure does allow third party solutions to stregthen O365's blind spots with additional best-of-breed security. By leveraging the use of third-party security on top of Microsoft's foundations, you can create a powerful, secure O365 environment that will help workforces become more flexible, collaborative and productive.

> "Microsoft is an 80/20% company – there's always room for higher security."
>
> Michael Greth, SharePoint & Office 365 Specialist and Microsoft MVP

DEFENCE 365

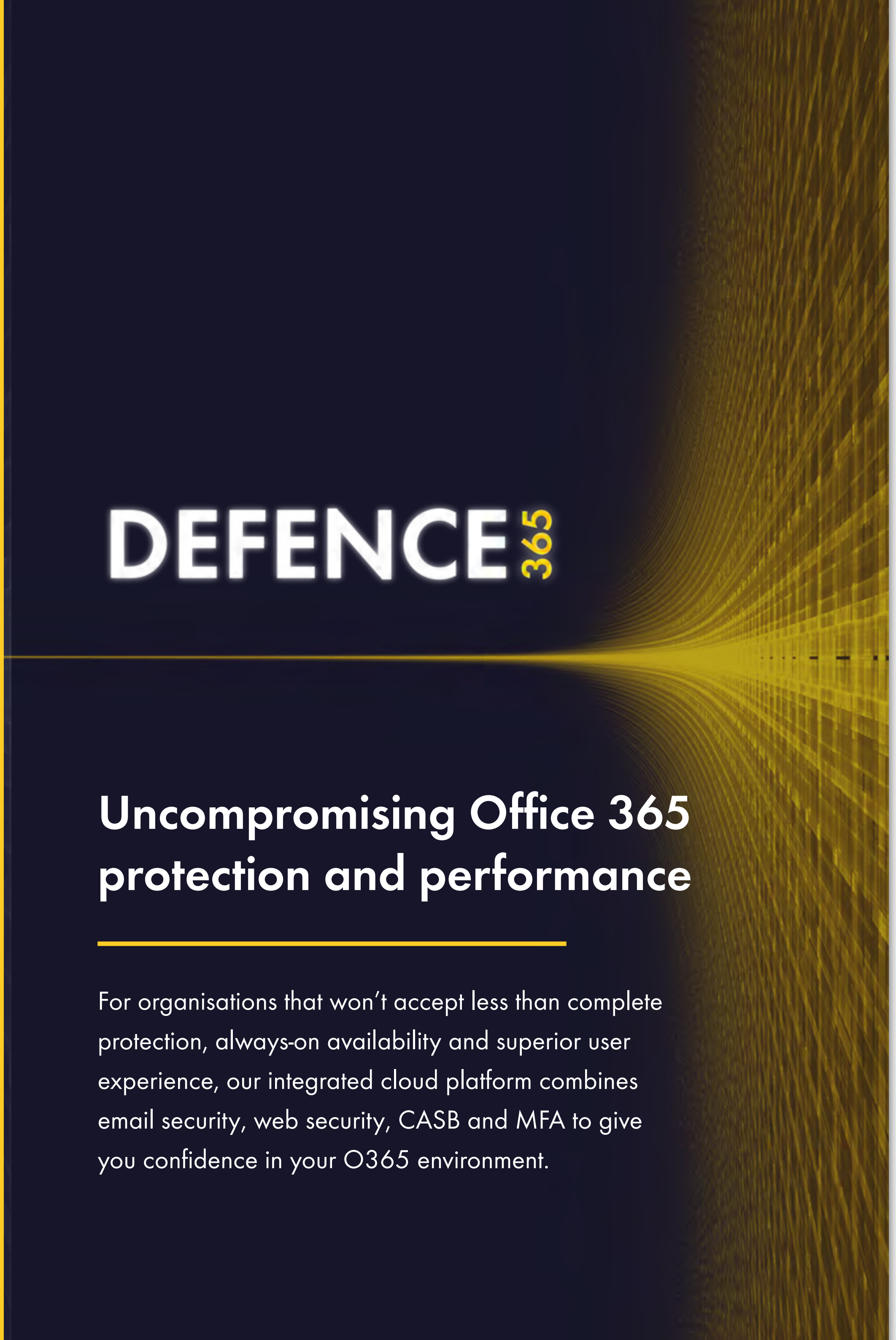
Delivering a truly secure O365 environment

We know that migrating to the cloud can be an exceptionally demanding task for security and IT professionals. Under pressure to deliver the transition quickly and with limited resources, it's not uncommon for critical steps to be overlooked – impacting not only the security of your O365 environment but the user experience of the suite.

But there is a way to regain control.

By implementing a clear migration framework that guides you through every step of your O365 journey, you can overcome challenges such as cyber security threats, data security/ management, user experience and availability – and build a strong foundation for your O365 suite.

With the support of third-party security solutions, organisations can eradicate the vulnerabilities in O365's defence and deliver an O365 suite that can truly transform the agility, performance and security of entire organisations for years to come.



DEFENCE365

Uncompromising Office 365 protection and performance

For organisations that won't accept less than complete protection, always-on availability and superior user experience, our integrated cloud platform combines email security, web security, CASB and MFA to give you confidence in your O365 environment.

Uncompromising cyber security

Our integrated security defends against attacks anywhere and then proactively blocks them everywhere else. Where O365 has you covered against traditional spam, Defence365 defends against even the most sophisticated threats for full protection across your entire network.

Uncompromising user experience

For an undisrupted, high-performing user experience, without latency, Defence365's unique architecture enables Microsoft's recommended direct-to-internet connections whilst still maintaining high-level security.

Uncompromising availability

Defence365 ensures critical business continuity for your organisation, protecting you from the outages of elements of the O365 service and eradicating downtime through an Emergency Inbox and Compliant Email Archive.

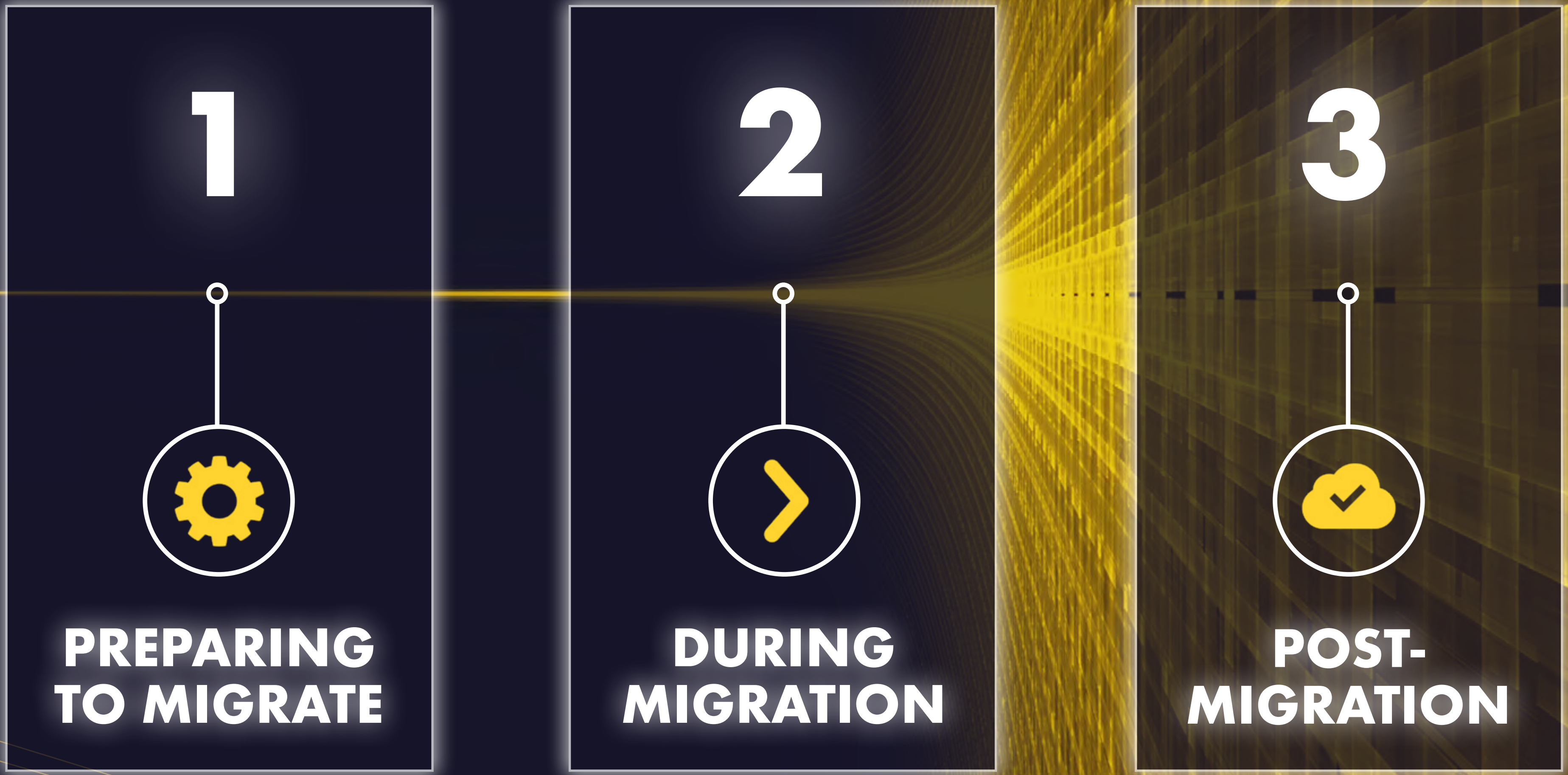
Uncompromising data security and management

With the convenience and flexibility of the cloud comes the risk of losing data and control. With unrivalled insight into users, the ability to manage access and activity on a granular level and data security across all services, Defence365 provides the ability to secure and manage your data, avoiding data sprawl and protecting the modern workforce.

Underpinned by compliance

The essential capabilities needed to ensure compliance, including comprehensive reporting, integration with SIM/SEM solutions and unrivalled insight into user activity in cloud apps.

For every stage of your O365 journey



1

PREPARING TO MIGRATE

2

DURING MIGRATION

3

POST-MIGRATION

censornet.

Cloud security transformed

Defence365 is brought to you by Censornet, the leading force in innovative and automated cloud security that offers robust, consolidated solutions for organisations of all sizes.

Censornet's cloud security platform integrates email and web security, CASB (Cloud Access Security Broker) and adaptive MFA (Multi-Factor Authentication), alongside the Autonomous Security Engine (ASE) – providing full spectrum threat protection for your organisation and users, no matter where they are.

Award-winning cyber security provider

Trusted by over 1,500 organisations

100% cloud-based security solutions

Ready for uncompromising O365 performance and protection?

Visit **censornet.com** or email **defence365@censornet.com** to find out more information about Defence365.