censornet.

Securing your Microsoft 365 environment.

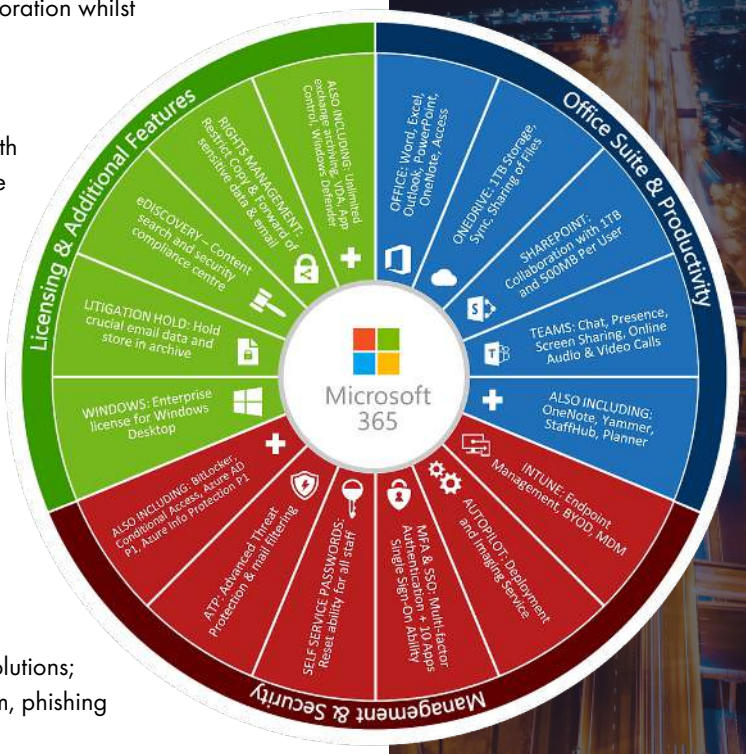
When your greatest strength becomes your biggest weakness

With hybrid working now the norm, a frictionless experience both inside and out the office is crucial. Microsoft 365 is an essential suite of tools for businesses, helping to enable effective communication and collaboration whilst supporting remote working.

Enabling SSO (Single Sign-On) across the Microsoft Ecosystem and connected SaaS Applications helps with this efficiency. However with Microsoft's position at the heart of the technology, it's still leaving businesses open to attacks.

The total threat landscape faced by organisations continues to grow, especially the threats targeting Microsoft users. Microsoft 365 alone has nearly 40 cloud-based methods malicious actors could use to obtain access, execute code, traverse the network undetected and exfiltrate data.

Microsoft 365 powers the modern workplace, but to stay ahead of today's threats, organisations need more. Gartner[1] and Forrester[2] both emphasise that a comprehensive defence requires additional security solutions; especially for web and cloud applications, email spam, phishing protection, and data security capabilities.



This document details some of today's threats relative to your Microsoft platform and why you should enhance your defences with additive solutions.

[1] Gartner Document ID G00735200
[2] Forrester Document ID: RES141598

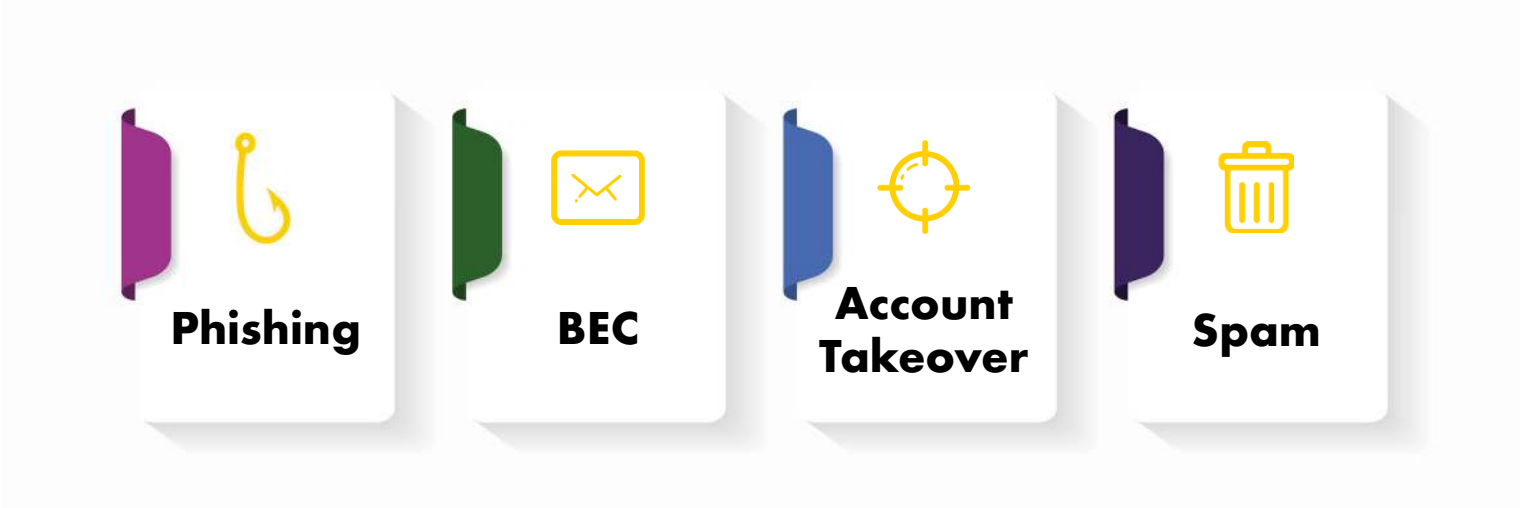
1. The Microsoft 365 Attack Channel

Today's cyber-criminal are targeting users, instead of spending precious time trying to brute force or hack into your network. Hybrid work offers prime opportunities to exploit human error. Unsecured personal devices, public Wi-Fi, and home distractions make it a breeze for attackers to use remote social engineering tactics like phishing to gain access to your sensitive credentials and data.

It's unsurprising then that 82% of data breaches involve a human element.[3] The data lost includes credentials (63%), internal company data (32%), and personal data such as customer names and addresses (27%).[3]

Microsoft's own 'Future of Work' report found that 80% of security professionals have experienced an increase in security threats since shifting to remote work.[4] 62% say that phishing campaigns have increased more than any other type of threat, with over 90% of attacks now starting with an email.

So, what are the main attack techniques targeting Microsoft 365?



[3] *2022 Data Breach Investigations Report, Verizon*
[4] *The New Future of Work, Microsoft Research*

2. Attacks targeting Microsoft 365

1. Phishing

Malicious actors are using phishing to socially engineer targets into giving away valuable information. These attacks are increasingly becoming multi-channel, designed to evade traditional scanners.

What may start as an innocuous email from a reputable brand soon diverts to website or cloud application to deliver its payload or harvest data. Over 90% of the domains used for this purpose are Gmail accounts, delivered through legitimate marketing automation services to evade early blocking.[5]

2. Business Email Compromise (BEC)

BEC is the latest threat to come from email attacks. Cybercriminals are pretending to be suppliers, business partners, executives, or even customers by using fake email addresses that look legit. Even worse, they may use a real email account that was hijacked, which can easily fool Microsoft 365.

> **BEC attacks have increased by 81% during H1 2022 compared to the previous period – and the total attack volume has grown by 175% during the past two years.[6]**

3. Account Takeover

A high-profile account takeover offers a wealth of intelligence, and a mass of information. Impostors are also increasingly using a compromised high-value target's Microsoft 365 account, such as a CEO, to exploit the inherent trust that comes with the identity and facilitate BEC attacks.

These attacks prove not only difficult to remediate, but often the financial and reputational damage can be insurmountable.

> **"Microsoft has continuously improved its email security capabilities, yet there are gaps.**
>
> **Security and risk management leaders must understand the strength and weaknesses of Microsoft's email security capabilities to determine whether it can meet business requirements."[7]**
>
> **Gartner**

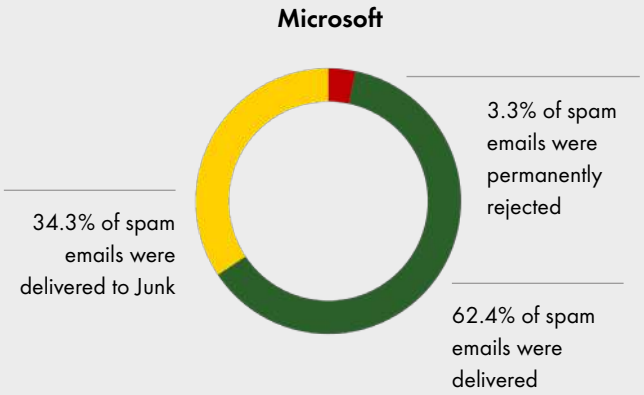
[5] Threat Spotlight, Olesia Klevchuk
[6] H1 2023 Email Threat Report, Abnormal
[7] Quick Answer: Is Microsoft's Email Security Capability Good Enough?, Gartner

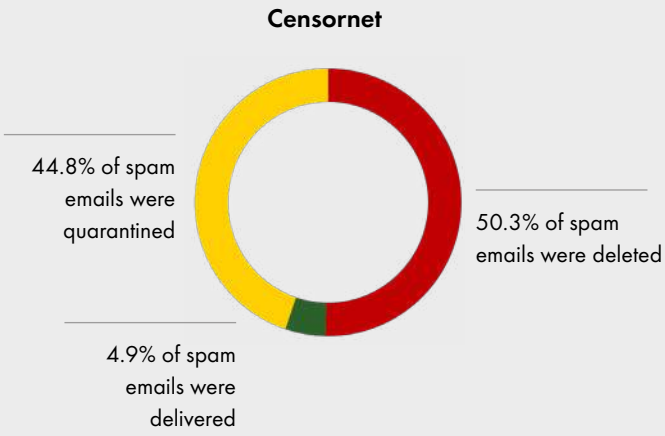
4. Spam

Unwanted emails may not always intend harm, but they pose a significant threat to your team's productivity. According to research, among every million emails sent through Microsoft Exchange Online Protection (EOP) and Advanced Threat Protection (ATP), around 11.6% are irrelevant messages or spam that Defender fails to filter out.[8]

For mid-sized businesses that receive between 5-10 million emails annually, this translates into a substantial amount of spam. Even more troubling, these organizations also receive over 13,000 corrupt emails that contain malware, or impersonation attacks, putting their cyber security at risk.

> **In recent testing, Microsoft 365 was compared to Censornet to measure delivery rates of real-world Spam campaigns. Microsoft rejected 3.3% of content vs. 95% by Censornet.**





> **"When it comes to email your users need to be right all the time, the bad guys only need to be right once"[9]**

[8] *Email Security Risk Assessment, Mimecast*
[9] *H1 2023 Email Threat Report, Abnormal*

3. A false sense of security

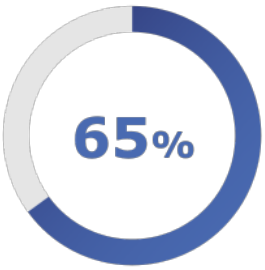
Cyber security, and protecting Microsoft ecosystems, must be addressed in the boardroom as a whole-business decision. In the age of hybrid working and modern digital threats, relying on a "good enough" strategy is no longer viable.

Striving for more than "good enough" however risks a huge increase in operational burden. This is at a time where the UK is facing a significant cyber skills shortage, with over 14,000 open positions currently unfilled. It's unsurprising that in 2023 organisations are prioritising spend on automation and security consolidation to address the gap. Whilst the Microsoft 365 platform is improving, it falls short of this priority. The interface continues to be complex, with numerous siloed management portals and a lack of intuitiveness.

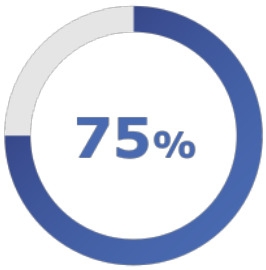
As a security-minded organization, being proactive against attacks is crucial. Quick access to insights, detailed analytics & reports, and granular controls over users' activities is essential. And whilst Security Awareness Training is an integral part of any security strategy, it can't be relied on to cover Microsoft 365 shortfalls. You need to be proactive in intercepting incoming threats and restricting unauthorized data flow out of your organization.

The highest increase in spending is expected in these areas:[10]

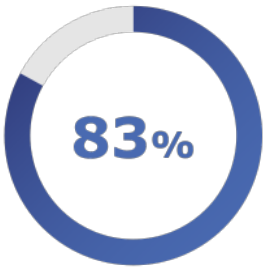
Organisations embracing automation are looking for:[10]



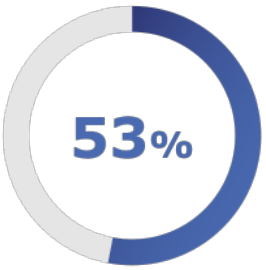
Partially Automated



Integrated



Fewer Solutions



Prevention, Detection & Response

[10] *2023 Bitdefender Cybersecurity Predictions, Bitdefender*

5. You can't secure what you can't see

Today's threat landscape enables cyber criminals to curate attacks across multiple channels. As users have become increasingly familiar with SSO and federated identity platforms such as Google and Microsoft (with and without MFA), a popup to sign into these services is no longer treated with suspicion. Compromised user accounts are then used to exploit access to sensitive data and resources inside the business often undetected.

> **There are over 300 million fraudulent sign-in attempts to Microsoft cloud services every single day.**[11]

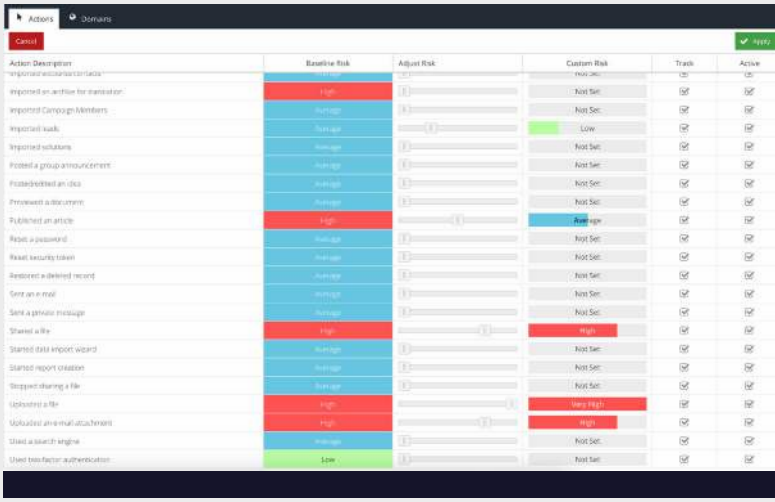
Many are due to credential stuffing, where attackers attempt to sign in using an email/password combination obtained from a 3rd party data breach. As 64% of users use the same password for multiple accounts, this tactic is proving fruitful.[12]

With all this in mind, an integrated security platform is essential covering Email, Web, Cloud Applications, DLP, and Identity management. Autonomous platforms can also prevent and respond to threats that target Microsoft 365 environment.

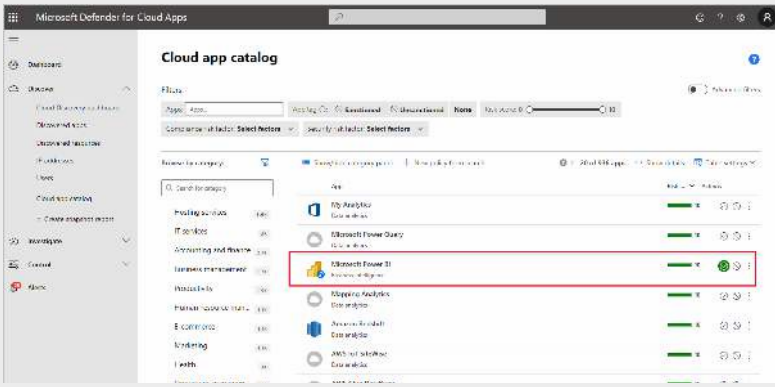
Granular Activity Visibility

As users take advantage of cloud collaboration and productivity tools such as Outlook, Teams and OneDrive, securing the flow of data can be a challenge. Security teams need to identify and protect the data users create and share across the different channels. With Microsoft 365 tools alone, this is unrealistic.

Cyber security needs to be frictionless, so preventing data loss and misuse requires real-time context and insight into user intent. Simply blocking access to SaaS applications (e.g. cloud file sharing) will result in users finding a way round the restrictions. Instead of blanket bans, it's important to understand the risk profile and set policies accordingly to enforce actions that may put your business at risk. The two diagrams on the right show the difference in controls for Censornet vs Microsoft.



Censornet CASB individual action-level granularity within SaaS application catalogue



Defender for Cloud Apps application-level risk score only

[11] *Microsoft*
[12] *2022 Annual Identity Exposure Report, SpyCloud*

6. The value of a consolidated platform

A full Microsoft 365 deployment is a substantial investment for any business, even without – as Gartner describes – shadow costs. Not adding security technology to the bill might make it appear more palatable at first, but failure to fully secure that initial investment will cost operational time, money and increase your risk posture over time. Microsoft 365 licensing options can be overwhelming, but it's often possible to save money by selecting the right mix of native and 3rd party solutions.

> There are dedicated 3rd party websites like m365maps to help decipher the product matrices.

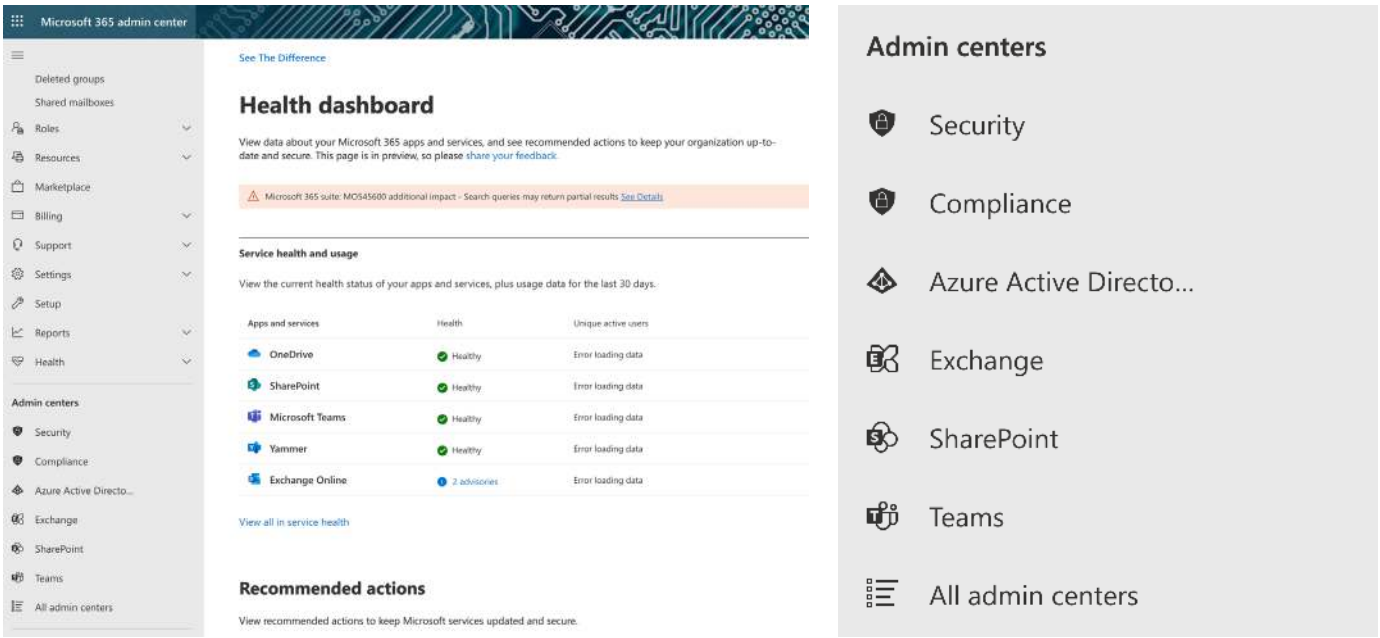
Take away the complexity

Simple day-to-day operations with Microsoft 365 quickly become complex and time-consuming tasks. Whilst the overall Admin Center includes a dashboard and limited controls – users roles, billing and reports – individual features such as Web Security, CASB, Email and DLP are in separate portals. It can be challenging to know where policies are hosted, with numerous overlapping and conflicting configurations. A lack of out-of-box policies, difficulty finding settings for web content filtering, and no at-a-glance view of security posture only increases the cognitive friction.

It becomes even more complex outside of the Microsoft ecosystem as limited functionality restricts even simple processes. Users opting for 3rd party browsers for example do not have the same level of security as Edge, and discovery of activity on devices that do not run Windows Defender requires an ingestion of Firewall logs.

This complexity, alongside the time to on-board, pushes down Microsoft 365's time-to-value. With extensive technical documentation, administrators have to invest precious time in configuring the platform to get the most out of it. For the mid-market organisation this is simply unfeasible.

So, what should the key considerations be in a Microsoft 365 estate..?



Microsoft 365 Admin Centre Dashboard and listing of individual portals

7. M365 Considerations

Data Protection

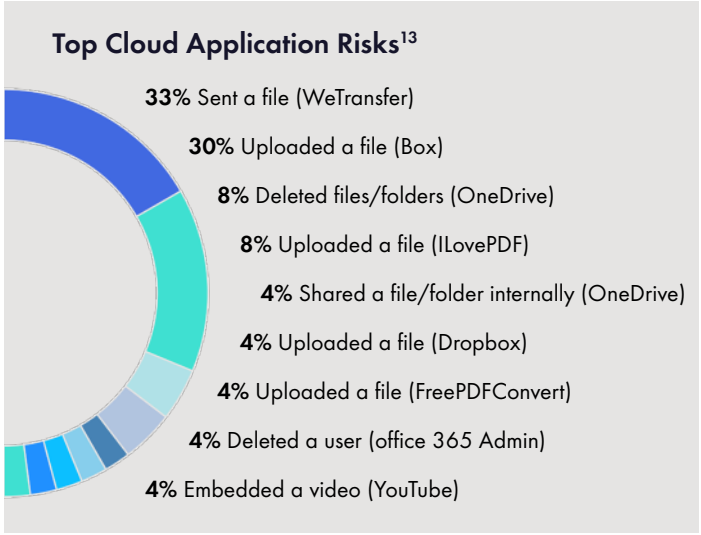
Considering the 'human element' as part of your visibility and controls is crucial to mitigate the risk of data leaks. The **most common insider incident is data exfiltration (62%)** and whilst this may stem from malicious intent, the overwhelming majority is inadvertent loss.

An insider threat is a relatively unique scenario in cyber security. Unlike the usual cat-and-mouse experience of defending against external attackers, here you are defending the business from someone on the inside. This is often an uphill battle – the user won't necessarily raise warning signals and potentially has access to significant sensitive data.

The only way you may be able to identify a potential threat in advance is through behaviour and activity (e.g. file uploads to cloud storage, excessive email attachments.) Failure to monitor closely could mean that the real damage is done before you even recognize an incident has occurred. The corporate liability associated with a data breach is significant, so you need to cast a critical eye over your policies.

> **Review your compliance module's capability to discover and classify sensitive data, report policy violations, and enforce rules for data exfiltration through Email, Web, and Cloud Applications.**

There is no single solution to securing data against the insider threat – you must pair discovery, visibility, reporting, enforcement and remediation in a single platform. Microsoft 365 businesses need to consider the risk of their DLP solution not covering all channels of employee communication, as well as operational burden of accessing detailed event reports and analytics should a policy be triggered.



Granularity of visibility is crucial – can you identify all the 3rd party SaaS Applications your users are accessing and the content within files leaving the business to build a risk profile that you can use for compliance and mitigate the risk of a regulatory penalty?

Questions to ask when boosting your Microsoft 365 security:

1. How heavily does your business rely on email as a source of communication, and what is the impact if there is an outage (or customer/prospect emails lost due to an outage)?
2. What business continuity tools do you have to maintain email communication flow during a service outage?
3. What risks (security, compliance) come from users resorting to personal email services to get work done?
4. Do you have access to high-level at-a-glance reporting to quickly identify anomalies and potential incidents, and provide executive/board reports detailing risk posture?
5. How much time can you afford to spend supporting users on message tracing (i.e. searchable logs, archive eDiscovery, responding to requests for undelivered messages such as quarantine/false positives)

[13] *Censornet Customer Dashboard*

External Threats

Cyber attackers exploit the very tools your employees depend on for their everyday work, exploiting known gaps. Sophisticated tactics continue to circumvent Microsoft Email defences, for example, with nearly 20% of phishing messages successfully reaching their target.[14] It's essential to implement additional layers of security.

> **The costliest initial attack vector in 2022 was phishing, followed by business email compromise.**

Average cost and frequency of data breaches by initial attack vector[11]

Imagine the productivity lost in cleaning up email incidents that should have been blocked, or the time spent investigating data leaks caused by a compromised credential that has been harvested. The financial and reputational cost of a fragmented threat response due to lack of visibility across the attack surface or inefficient reporting can be irreparable.

> **It takes an average of 277 days to detect and contain an incident**

Operational Costs

Organizations need to take into account the burden on IT and Security administrators when evaluating capital expenditure.

You only need to look at online news outlets and even Microsoft's own social media feeds to see how common service outages are.

Although Microsoft 365 comes with a 99.99% uptime SLA (and service credits for lower availability impacts), there are exceptions that organisations must be aware of – Virus Detection, Spam Effectiveness and False Positives for example.

Spam is generally accepted as a subjective classification, and Microsoft relies on the user to provide evidence. Only after this evidence shows spam effectiveness has fallen below 99% for more than 1 week can you claim service credit. Consider a company of 250 employees that will, by 2026, receive 30,000 emails per day. That means 300 unwanted or malicious emails before falling below the uptime SLA. In a landscape where it only takes one email to cause a breach, 300 is worrying.

Compliance

In 2016, Europe's General Data Protection Regulation (GDPR) went into effect, holding organizations publicly accountable for non-compliance. Whilst Microsoft's software service platform complies with most regulations, there are limitations like email archiving capabilities. Easily accessible and searchable historic email data is crucial in a legal dispute, but with Microsoft 365 requires an additional subscription.

When evaluating your capabilities, you should consider how quickly and easily you can instigate a legal-hold, then collect and collate all the communication records from specific users or departments, not just from Email but potentially cloud SaaS services too.

[14] *Keeping Your Emails Secure: Who Does it Best?, Avanan*
[15] *Cost of a Data Breach Report 2022, IBM*

Risk

A modern, integrated approach to threat protection and security posture management is essential for managing the challenges of today's threat landscape. Data is the primary currency, so you need consider all potential channels that data could be exfiltrated maliciously, or accidentally. Managing the human factor is essential by balancing Security Awareness Training, internal policies, culture and technology.

Security vs. User Experience is always a compromise, and you need to be comfortable with a certain level of risk-appetite. Setting too many restrictions on your users will generate friction. Gartner research shows that over 90% of employees who admitted undertaking a range of unsecure actions during work activities knew that their actions would increase risk to the organisation but did so anyway.[16]

> **By 2027, 50% of CISOs will formally adopt human-centric design practices into their cyber security programmes to minimise operational friction and maximise control adoption.[16]**

Managing risk starts with adopting Data Loss Prevention strategies. In addition to enforcing document information security classification, DLP scans the contents of files searching for specific Personally Identifiable Information (PII) or additional information deemed sensitive to the organisation. The Censornet DLP solution makes this task a breeze, by using the same integrated visual rule builder to create, apply and enforce DLP policies across Email, Web, and Cloud Applications.

Support

Microsoft 365 includes various options for support depending on the Enterprise Agreement. Standard Support for Microsoft 365 Business tiers include telephone and online support (24x7 for Severity A cases, which must be business critical). Non-critical incidents have an 8hr SLA during business hours only. This can be upgraded for a fee to Unified Enterprise support which gives priority routing – pricing is variable based on product usage. For Azure cloud infrastructure and M365 there is a minimum contract price of $50,000 then 10% fee up to $1.8M with the rate reducing as annual spend increases in bands – for users (Modern Workplace, Business Apps etc.) the starting fee is 7.5%.[17]

At Censornet we are proud of our UK-based white-glove customer and technical support capabilities. Our support plans include business-hours and email support as standard with options to add live telephone and chat, and 24x7 availability. These are simply billed at flat rates of 15% or 20% of annual contract value, no minimum requirement and no sliding-scale to complicate billing.

We have never dropped below 100% First Response SLA, with over 50% of support tickets being resolved on 1st contact. This world-class service and focus on customer success is a significant contributing factor that helps deliver our class-leading Net Retention Rate (NRR) of >122%.

[16] *Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Gartner*
[17] *Microsoft Unified Enterprise details, Microsoft (correct as of April 2023)*

Censornet's Autonomous Integrated Security Platform

The Censornet platform integrates powerful security technology across the entire digital attack surface and cloud-borne threats.

The single pane-of-glass portal integrates:

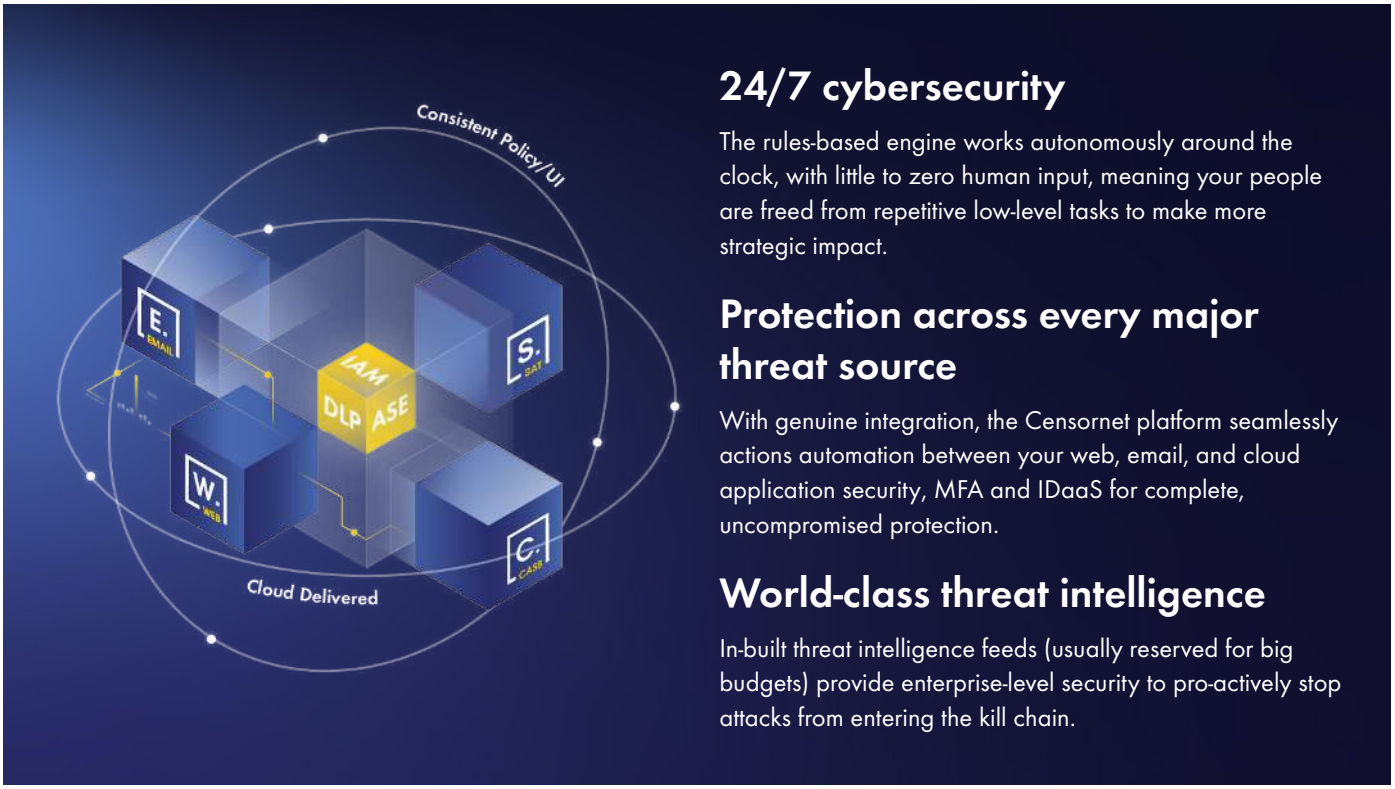
- Email Security (Inline/API)
- Web Security (http/https)
- Cloud Application Security (Inline/API)
- MFA
- Identity Services (SSO)
- Security Awareness Training
- ASE (Autonomous Security Engine)

All these are presented through a simple intuitive rule builder and policy engine.

The powerful analytics engine provides high-level dashboard views for at-a-glance insights that are fully interactive delivering forensic-level analysis and alerting if required.

By integrating the core modules from the ground up this enables our Autonomous Security Engine to orchestrate threat response without an admin – passing threat telemetry, state data and rich context information between the services, delivering seamless protection against multi-channel attacks and reducing the operational burden.

See Censornet in action



24/7 cybersecurity

The rules-based engine works autonomously around the clock, with little to zero human input, meaning your people are freed from repetitive low-level tasks to make more strategic impact.

Protection across every major threat source

With genuine integration, the Censornet platform seamlessly actions automation between your web, email, and cloud application security, MFA and IDaaS for complete, uncompromised protection.

World-class threat intelligence

In-built threat intelligence feeds (usually reserved for big budgets) provide enterprise-level security to pro-actively stop attacks from entering the kill chain.

ASE D. DLP C. CASB W. WEB E. EMAIL S. SAT ID. IDaaS M. MFA

About Censornet

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection.

Its Autonomous Integrated Cloud Security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed. For its millions of users globally, its AI-driven, autonomous solution is smarter, faster, and safer than is humanly possible.

Censornet was named Technology Provider of the Year at the British Business Awards 2022. Supported by an award-winning team of customer support specialists, it's leading the way with autonomous integrated security.

Censornet's clients include Macmillian Cancer Support, Fever Tree, Lotus Cars, Parnassia Group, Mizuno, Radius Payments, Newlife Disabled Children's Charity, National Portrait Gallery, Hallmark Hotels and Thatchers Cider.

For more information, please visit censornet.com.