Hands On IT Services

Service Catalogue

Contents

Hands On IT Services

MDR / SOC with Behaviour Monitoring & Ransomware Detection

RocketCyber

24/7 Elite Protection: Hunting Threats, Stopping Ransomware.

In today's landscape, standard antivirus isn't enough. Cybercriminals use sophisticated tactics that bypass traditional "perimeter" defences. **Kaseya MDR (Managed Detection and Response)**, powered by **RocketCyber**, provides a dedicated team of elite security veterans watching over your business 24/7/365.

The Three Pillars of Defence

- **Continuous 24/7 Monitoring:** The Security Operations Centre (SOC) never sleeps. While you're away, their analysts are triaging alerts, hunting for anomalies, and isolating threats across your **Endpoints, Network, and Cloud (Microsoft 365).**
- **Behaviour-Based Detection:** They don't just look for "known bad" files. They monitor **behaviour**. If a legitimate tool suddenly starts behaving like a hacker's script, the system flags it instantly.
- **Active Threat Hunting:** They don't wait for an alarm to go off. The SOC pro-actively searches for hidden "Indicators of Compromise" (IoCs) to find adversaries before they can execute their plan.

Industry-Leading Ransomware Defence

Their proprietary **Ransomware Detection** is specifically designed to stop "crypto-locking" in its tracks:

- **Real-Time File Monitoring:** They watch for the specific mathematical patterns of encryption.
- **Automated Kill-Switch:** When ransomware is detected, the system **automatically kills the malicious process** and **isolates the infected device** from the network.
- **Preventing Lateral Movement:** By "quarantining" the device instantly, they ensure the infection can't jump from one PC to your entire server infrastructure.

Why Choose Kaseya MDR/SOC?

Feature	The Kaseya Advantage
Human Intelligence	Backed by a global SOC of expert analysts (not just automated bots).
"Siem-less" Logs	Full visibility into Windows/Mac, Firewalls, and M365 without expensive hardware.
Instant Response	Critical alerts are triaged in minutes, with remediation steps delivered directly.
Seamless Integration	Works alongside your existing tools like Microsoft Defender or DattoAV.

"It's not just software; it's a security team in your corner."

By combining AI-driven behaviour monitoring with human-led investigation, we provide the highest level of cyber-resilience available to modern businesses.

Cyber Confidence Starts Here

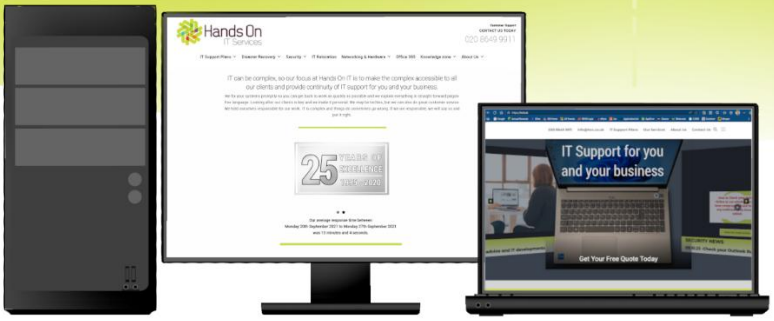
Kaseya MDR isn't just another tool - it's your frontline defence team. With 24/7 vigilance, behaviour-based analytics, and ransomware-specific countermeasures, your business gains more than protection - it gains peace of mind. Whether you are a small business or an enterprise with a complex infrastructure, Kaseya MDR scales with you, integrates seamlessly, and delivers human-led security that never sleeps.

Ready to upgrade from reactive to resilient?

Choose Kaseya MDR and let elite defenders guard your business around the clock.

Hands On IT Services

Dark Web Monitoring



Actionable Threat Intel for Your Organization

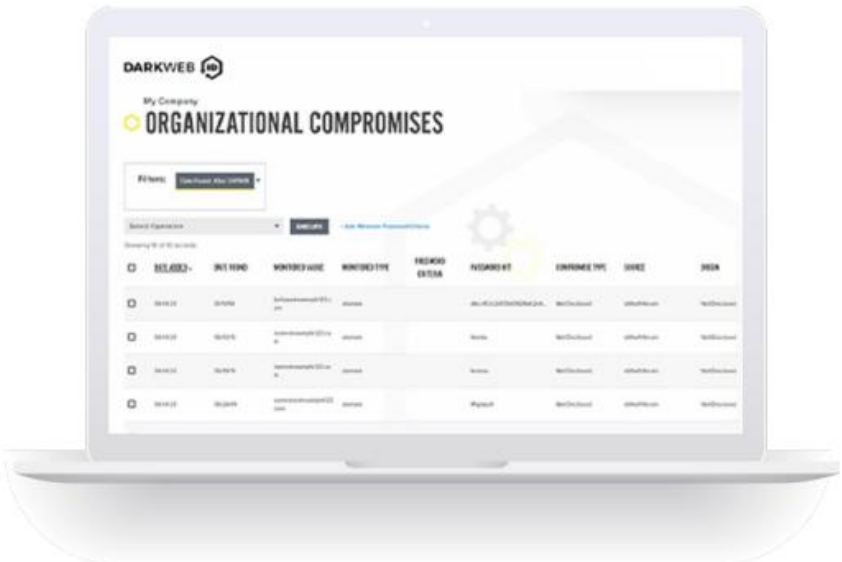
With cyberthreats increasing every day, Dark Web ID helps ensure you are proactively protecting your company's brand, employees and executives.

Gain deeper awareness into your security gaps - before cybercriminals get the chance to exploit them and steal from you.

Stolen user credentials (email addresses and passwords) found on the dark web can indicate that your company or a third-party application or website used by your employees has been compromised—so you can take immediate action.

60% of the information available on the dark web could potentially harm enterprises

Cybercriminals traffic and buy stolen credentials so they can infiltrate your networks to steal your data. By monitoring the dark web for threat intelligence about stolen user data associated with your company's domains, you can be alerted when a compromise is detected and then respond to stop a potentially costly and devastating data breach.



MONITOR 24/7/365

- Hidden chat rooms
- Unindexed sites
- Private websites
- Peer-to-peer (P2P) networks
- IRC (internet relay chat) channels
- Social media platforms
- Black market sites
- 640,000+ botnets

MONITOR, IDENTIFY AND MITIGATE THREATS

Your business security strategy extends far beyond your network, and Dark Web ID can help strengthen it. Easily monitor for exposure and leverage rich threat intelligence to take the appropriate actions that will protect your company's assets and reputation and lower the risk of breach.

SAAS BUSINESS APPLICATIONS INCREASE RISK

Although web-based applications allow employees to do their jobs from most anywhere, they also open your organization to risk. Payroll and HR platforms, CRM and marketing automation tools, travel sites, banking sites and social media accounts are accessed by your employees many times throughout a day. A recent survey shows that 65% of people reuse the same password for multiple or all accounts - potentially the same one they use to log in to your network.

EMAIL MONITORING FOR HIGHLY TARGETED EXECS AND PRIVILEGED USERS

Your executives and administrative users often have greater access to systems, information and sensitive data. If their personal email credentials are compromised and they happen to reuse the same credentials at work, the attackers may use them to gain access to corporate systems. The attackers may also use social engineering to impersonate your executives to trick other employees to give up access, divert funds, or for other schemes. Therefore, it's important to monitor the personal mail addresses of your executive and administrative users along with their corporate email accounts.

EXTEND SECURITY TO THE SUPPLY CHAIN

Some cyberattacks could happen due to exposure to third-party vendors from your supply chain. The interwoven systems of vendors and partners present security risks since data is shared across networks. The growing need for cyber supply chain risk management has prompted forward-thinking organizations to add dark web monitoring to vendor due diligence.

HOLISTIC VISIBILITY

By adding Dark Web ID monitoring to your security strategy, you will get a more complete picture of your company's security posture. Not only does it serve as an early warning mechanism that alerts you before breaches occur, it also provides invaluable data analytics to evaluate where employees need security awareness training or where multi-factor authentication and single sign-on are warranted.

Hands On IT Services

Agent Protection and Housekeeping

Our **Datto RMM (Remote Monitoring and Management) Agent** is the "brain" installed on every PC that allows our IT team to manage security and performance without ever needing to touch the physical machine.

Here are the main tasks that we use it for

1. Managed Antivirus (AV)

The agent acts as a 24/7 guard for your antivirus software, ensuring it is never disabled or out of date.

- **Health Monitoring:** The agent constantly checks "Is the AV service running?" and "Are the virus definitions current?" If a user accidentally disables their AV, the agent detects it within 60 seconds and can automatically turn it back on.

- **Centralized Alerts:** If a virus is detected on a PC, the agent sends an instant alert to the IT dashboard. We don't have to wait for the user to call us; we often know about the threat before they do.
- **Automated Scans:** We use the agent to schedule deep system scans during lunch breaks or after hours so that the PC remains fast while the user is working.

---

2. Microsoft & 3rd Party Patching

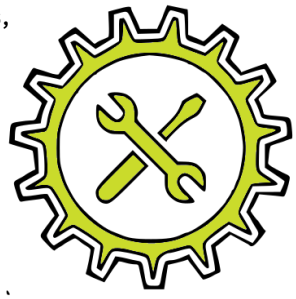
This is the most critical defence against hackers. The agent automates the "boring" updates that users typically "Snooze" or ignore.

- **Microsoft Updates:** The agent bypasses the standard Windows Update screen. It downloads and installs security patches silently in the background, ensuring the PC is never left vulnerable to known exploits. In 2026, hackers used AI to find vulnerabilities hours after they are announced. If you don't patch, you are leaving a window open after the alarm has already gone off.

- **3rd Party Patching:** Most people remember to update Windows, but ignore Third-Party apps (like Chrome, Adobe, or Zoom). Hackers know this and often target these "neglected" apps as a side-door into your PC.
- **Proactive vs. Reactive:** Patching is **proactive**. It removes the threat before a hacker even tries to use it. Without it, you are constantly playing "catch-up" after an infection has already started.
- **Failure Reporting:** If an update fails to install (a common Windows issue), the agent flags it immediately so we can fix the underlying problem before a hacker finds that "open window."

3. Weekly Housekeeping & Preventative Maintenance

Think of the agent as a "Digital Janitor" that cleans the PC every week to keep it running like new.

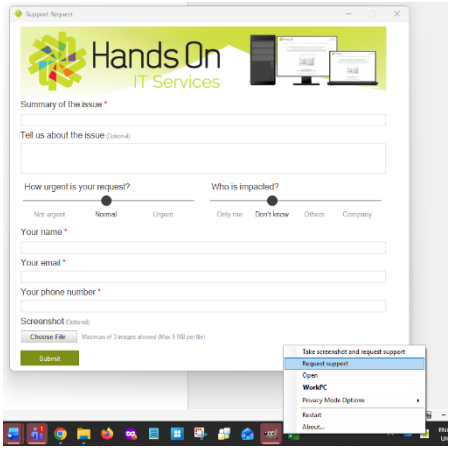


- **Disk Cleanup:** The agent automatically clears out temporary files, system logs, and "cache" data that slows down the computer over time.
- **Automated Reboots:** We can schedule a "forced" reboot once a week (usually at 2:00 AM) to clear out "stuck" processes and refresh the system memory.
- **Self-Healing Scripts:** The agent runs "preventative" scripts that check for common errors, such as low disk space or high CPU usage. If it finds an issue, it can often run a "fix" script automatically before the user even notices a slowdown.

4. Communication and communicating

Alerting our customers and also allowing them to contact our engineers is crucial in the way we support you.

- **Notifications:** The agent allows us to alert our customers, to restart, tell them that maintenance is happening, or to start a “Chat”
- **Remote Assist:** Having direct access to a device is critical when trying to support you. Rather than using another tool to try and help, keeping the remote access locked within our security suite, protects us and you.



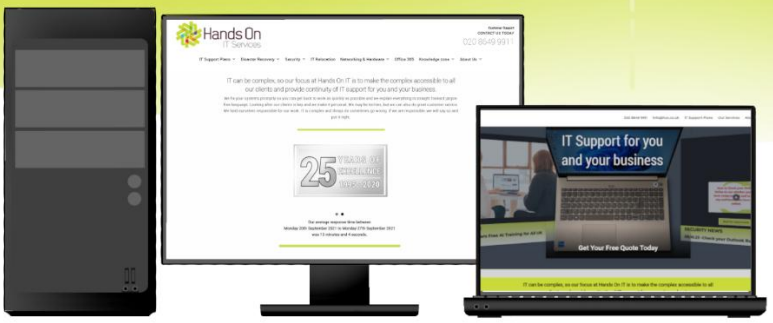
• **Ticket Raising:** Our agent allows the end user to create tickets directly into our system. This means that the ticket is in our queue straight away and the SLAs start. It is a faster way to guarantee our service and reduces any time delay from the human element of a phone call or emails.

The Datto RMM Agent allows us to turn a reactive IT setup ("Call us when it breaks") into a proactive one ("We fixed it before it broke"). It ensures the PC is always patched, always protected, and always clean!

Hands On IT Services

Datto AV

Next-Generation Antivirus Software For Your Business



Revolutionize Your Cybersecurity Posture

Protect your business from sophisticated cyber threats with Datto AV, an AI-driven, next-generation antivirus solution. Miercom, a global leader in cybersecurity testing, reports that Datto AV, when combined with Datto EDR, detects and stops 99.62% of all malwares, creating an easy-to-use and powerful threat detection combination.

Advanced Threat Prevention

Utilize AI, machine learning, and the latest in threat intelligence to proactively identify and block zero-day and polymorphic threats, ensuring your business stays ahead of attackers.

Seamless Performance

Enjoy top-tier security without sacrificing performance. Datto AV is designed for efficiency, maintaining system speed and user productivity without compromise.

Comprehensive Real-time Protection

Benefit from real-time scanning and automatic threat blocking with advanced unpacking capabilities, ensuring immediate response to any cyberthreat.

Global Threat Intelligence

Leverage cloud-based global threat intelligence for up-to-date protection. Datto AV's cloud infrastructure continuously updates with the latest threat data, offering superior defence mechanisms.

Advanced Features of Our Next-Generation Antivirus Software

Next-Generation Antivirus Engine

Beyond signature-based security, incorporating AI and machine learning for dynamic threat response.

Efficiency Meets Performance

Optimal security without compromising system performance, using minimal system resources.

Threat Detection and Remediation

Automatic, real-time identification, quarantine and cleansing of malware infected systems.

Cloud Security Intelligence

Access to global threat intelligence through cloud-based infrastructure for enhanced security insights.

Seamless Integration with AMSI

Protection against script-based malware and non-traditional cyberattacks.

DNS Filtering and Access Controls

Proactive security against domain-based cyberthreats and enforcement of web access policies.

Endpoint Protection Redefined

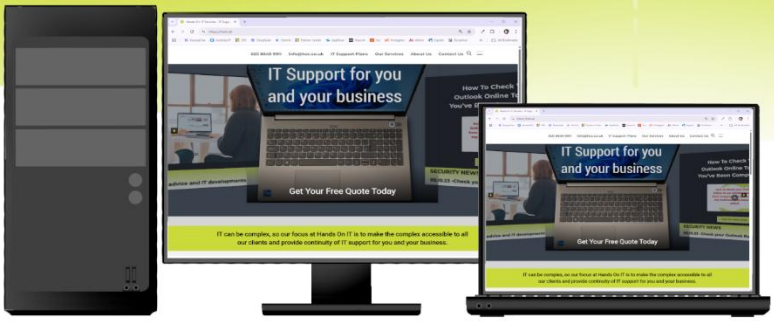
Datto AV follows the same core principles as Datto EDR: to be easy to use, not generate unnecessary noise, and stop the threats that plague businesses. Seamless integration between Datto AV and EDR creates a powerful combination to easily protect, detect, and respond to cyber threats, all from the same interface.

Don't just react to threats - stop them before they start with a security solution that works as hard as you do.

Hands On IT Services

Intelligent Defense Powered by GenAI

INKY®



Your Personal Email Security Coach

Making your inbox safer, one email at a time.

In today's world, phishing emails are designed to look exactly like messages from your bank, your boss, or popular brands. INKY is a smart security layer that sits inside your email to help you spot these fakes before they cause trouble.

How INKY Protects You

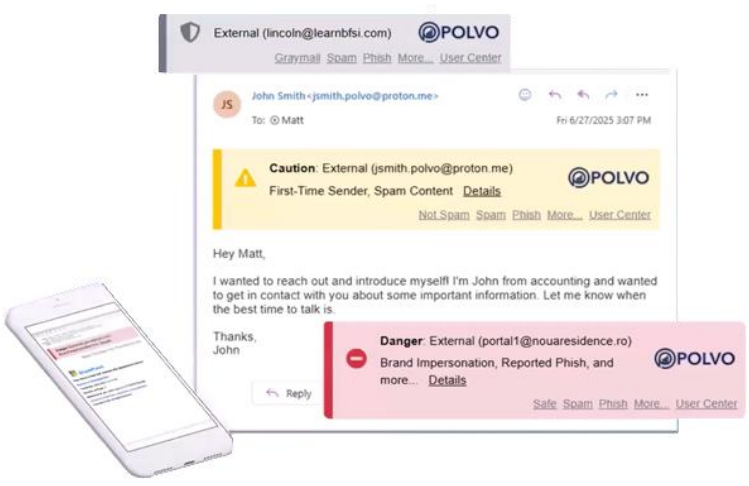
Instead of just blocking emails in the background, INKY "reads" every message just like you do. It uses artificial intelligence to look for signs of forgery, malicious links, and even dangerous QR codes and acts as a "security coach".

When INKY finds something suspicious, it places a clear, color-coded banner at the top of the email to guide you:

Grey (Neutral): This email is safe and hasn't shown any signs of danger. It will also confirm if the email came from an External sender, so you aren't surprised.

Yellow (Caution): Something is unusual. It might be a first-time sender or a request for sensitive information. Proceed with care.

Red (Danger): This email is likely a scam or contains a threat. It may be impersonating a brand or a colleague. In most cases, it's best to delete it immediately.



Key Benefits for You

Real-Time Coaching: INKY doesn't just say "Danger" - it explains *why*. Clicking "Details" on a banner shows you exactly what INKY saw, helping you become more security-savvy every day.

Works Everywhere: Whether you are using Outlook, Gmail, or your phone, the banners look and work exactly the same.

Safe Links & Attachments: If you click a link that turns out to be malicious, INKY can block the page in real-time and show you a screenshot of the threat instead. INKY scans every attachment for malicious code with a reported 99.7% accuracy. Also, INKY scans and decodes QR codes to ensure the destination URL is safe before a user clicks.

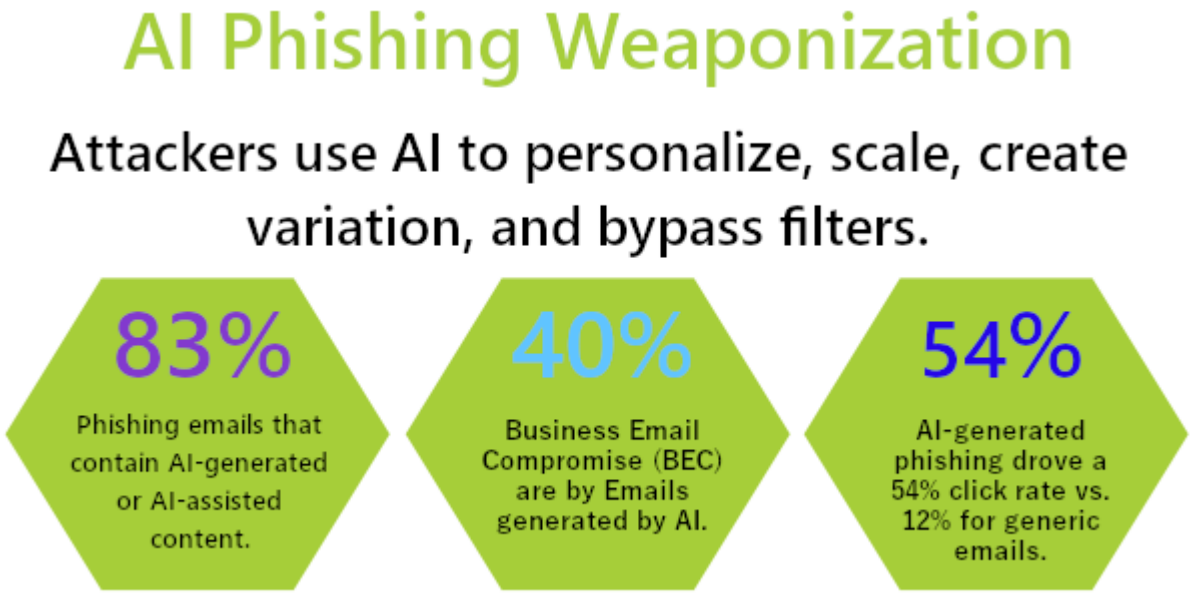
Take Control: You have the power to help. Use the "Report This Email" link on any banner to let the security team know if an email is safe, spam, or a phish. This actually helps INKY get even smarter for the whole company.

Stress-Free Sending: With the Pro version, if you accidentally try to send sensitive info (like a credit card number) to the wrong person, INKY can catch it and ask for a quick confirmation before the email leaves your outbox.

Simple Email Encryption: Need to send something confidential? With the Pro version, just add [encrypt] to your subject line, and INKY will automatically wrap your message in 256-bit security, ensuring only the right person can read it.

Seamless Integration

INKY integrates directly with Microsoft 365, Google Workspace, and Microsoft Exchange with zero downtime and no complex MX record changes required.



Hands On IT Services

Detect and Remediate Security Breaches

SaaS Alerts

Automatically Detect and Remediate Security Breaches in SaaS Applications

Imagine having a watchful protector that never sleeps, constantly guarding your clients' SaaS applications. Our platform does just that, detecting unauthorized access, and shutting it down without breaking a sweat.

The Most Comprehensive SaaS Security Platform Available

- MONITORING & ALERTING
- 24/7 DETECTION & RESPONSE
- SECURITY CONFIGURATIONS
- MONITOR MORE APPLICATIONS
- RMM & IT DOCUMENTATION TOOL MONITORING
- CUSTOMER & PROSPECT REPORTS

How Does SaaS Alerts differ from MDR providers?

MDR providers rely on human "threat hunters" which are tasked with aggregating data from multiple sources and responding as quickly as possible, usually measuring response time in hours. SaaS Alerts provides alerting and remediation steps with actions taken within seconds of malicious activity with no human interaction required. This difference significantly minimizes the risk of data egress or malicious activity within your clients' most vulnerable environments

A Deeper Look into SaaS Alerts

MONITORING AND ALERTING

We use machine learning to aggregate and analyse user behaviour in SaaS platforms. When unusual behaviour is detected, you get an instant notification so you can act fast.

24/7 DETECTION AND RESPONSE

SaaS Alerts automatically responds to detected threats and account compromises, temporarily disabling the account and blocking new login attempts. Automated threat mitigation occurs within minutes of detection and provides detailed forensic logs of compromised data and remediation steps.

SECURITY CONFIGURATIONS

Microsoft security recommendations are complex and require a lot of time to implement. With SaaS Alerts, you can apply security recommendations across all your tenants in minutes and receive alerts if a security score regresses.

BEYOND MICROSOFT 365

With our App Wizard, we can quickly integrate with any SaaS application with a viable API to pull mission-critical data into SaaS Alerts, so you can quickly detect and respond to SaaS security threats across almost all your clients' SaaS applications.

USER IDENTITY VALIDATION

Reconcile device data with SaaS data to ensure only authorized users on authorized devices can gain access to critical company SaaS applications.

INTUITIVE REPORTING

Powerful reporting of user behaviour and SaaS application events provides a comprehensive and timely view of the current state of SaaS security.

CORE APPLICATIONS WE PROTECT

Hands On IT Services

SaaS Backup Protection

SaaS Backup You Can Depend On

Right now, your business data (emails, files, and chats) lives in Microsoft/Google. While they keep you running, they aren't responsible if someone **inside** your organisation accidentally deletes a folder or if a hacker encrypts your files.

What is SaaS backup?

SaaS backup software is designed to store and protect data created by SaaS products. SaaS backup software is provided by a third-party vendor that creates an independent copy of that data. If a cloud application fails, you need a way to recover that data. Datto SaaS Protection is a SaaS backup solution that can be used to restore data to a functional state.

Datto SaaS Protection provides comprehensive recovery and backup for Microsoft 365. This includes protection for Exchange, Calendar, OneDrive, SharePoint, and Teams data with 3x daily backups and flexible restore options.

How does Datto help with SaaS Protection?

THE AUTOMATIC "MIRROR"

Three times every day, Datto take a snapshot of your entire digital office. You don't have to click anything; it happens quietly in the background. If a file exists at 9:00 AM, it’s backed up by lunch.

PROTECTION FROM THE "BIG THREE"

We use this to protect you against the three most common ways data is lost:

1. Accidental Deletion: A staff member deletes a folder by mistake.
2. Malicious Actors: An employee leaves on bad terms and wipes their inbox.
3. Ransomware: A hacker locks your files. With Datto, we don't pay the ransom; we just 'wind back the clock' to the hour before the attack happened.

INFINITE MEMORY

Microsoft only keeps deleted items for about 30 days. If you realise a file is missing on day 31, it's gone forever. With Datto, we keep that data for as long as you have the service. You can choose the 1-year retention period as default or extend it to infinite!

FAST RECOVERY

If you lose a single email, we can find it and "flick" it back into your inbox in seconds. If you lose your entire OneDrive, we can restore the whole thing exactly as it was. Restore lost data quickly with flexible restore options such as point-in-time, granular, and non-destructive restore.

PROTECT MICROSOFT 365 AND GOOGLE WORKSPACE DATA

Protect against permanent data loss and quickly recover from ransomware attacks or user-error with one-click restore functionality.

AUTOMATED, CONTINUOUS SAAS BACKUPS

Protect Microsoft 365 and Google Workspace applications against accidental or malicious deletion, ransomware attacks, and other cloud data loss with 3x daily, automated backups.

COMPLETE CONTROL

Automated point-in-time SaaS backups capture relevant changes across both Microsoft 365 and Google Workspace in their entirety. Our solution also provides an independent backup copy of data outside of SaaS provider servers.

So, if you are thinking of SaaS backup, Datto SaaS Protection is the only way to ensure your Microsoft 365 or Google Workspace data is truly independent, instantly recoverable, and backed up forever.

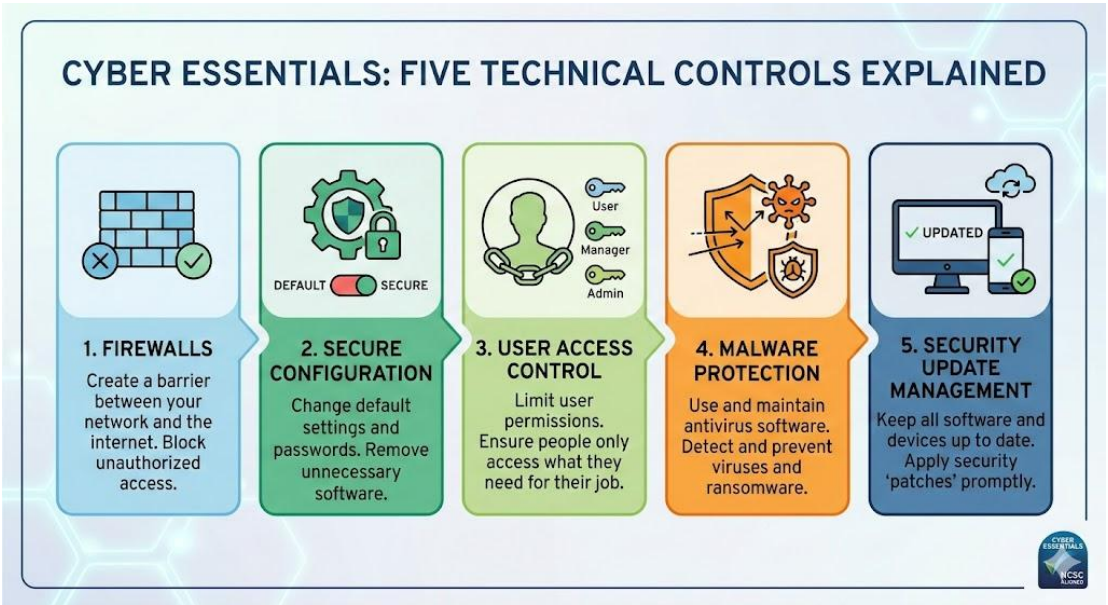
Hands On IT Services

Cyber Essentials CertificationService

What is Cyber Essentials?

Designed by the National Cyber Security Centre, the Cyber Essentials framework helps businesses to check or prove they are taking their IT security seriously by having the necessary measures in place to help protect their organisation. Cyber Essentials is the minimum standard of cyber security recommended by the Government for organisations of all sizes.

Developed by the experts at the NCSC, the certification scheme is aligned to five technical controls designed to prevent the most common internet based cyber security threats.

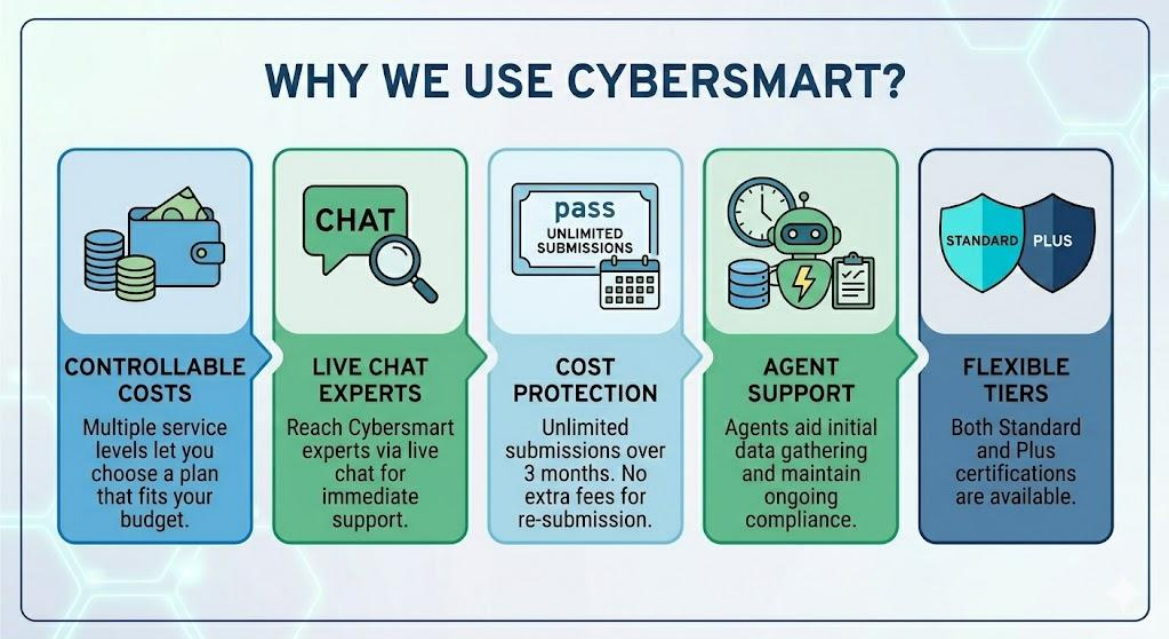


"Most successful breaches don't use high-tech "Mission Impossible" tactics; they simply exploit one of these five areas being left unmanaged."

We have partnered with CyberSmart to help us help our customers to achieve this certification. With their platform, we can be as "Hands On" with our assistance as you like.

Who Are CyberSmart?

CyberSmart is a UK-based cybersecurity company that specializes in providing comprehensive security solutions for businesses. They offer a range of services designed to protect organizations from cyber threats and ensure their digital assets are secure. CyberSmart's solutions can include vulnerability assessments, penetration testing, security monitoring, and compliance management



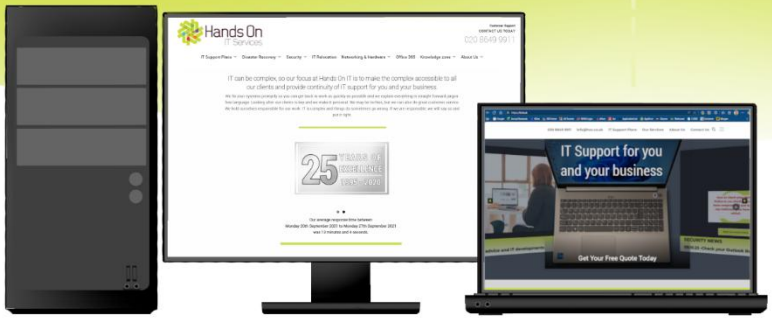
Here Are The Key Additional Considerations For Cyber Essentials (CE) And Cybersmart:

The "Plus" Factor (Cyber Essentials Plus)
While "Standard" is a self-assessment, Cyber Essentials Plus involves an independent technical audit. An assessor will actually test your systems to prove the five controls are working as you claimed.
BYOD (Bring Your Own Device)
If employees use personal phones for work email, those devices are technically "in scope" and must meet the security standards.
Automatic "Cyber Insurance"
A unique benefit of achieving Cyber Essentials (if your turnover is under £20m) is that you often qualify for automatic basic cyber liability insurance through IASME. This is a great safety net, but you should check if the coverage limits are high enough for your specific risk level.
The "Human Firewall"
The five technical controls protect your hardware, but they don't stop a human from clicking a bad link. Technical controls work best when paired with Security Awareness Training for your staff.
Annual Renewal
Cyber Essentials is not a "one and done" task; it expires every 12 months. This is where CyberSmart's "Active Protect" agent shines - it monitors your status year-round so that when renewal time comes, you aren't scrambling to fix 12 months of bad habits.
Legacy Systems
If you are running old software (like Windows 10 or older versions of MacOS) that no longer receives security updates, you will automatically fail Cyber Essentials. You may need to budget for hardware or software upgrades before you even begin the application process.

Hands On IT Services

Client Security Awareness Training

BULLPHISH ID



Effortless Security Awareness Training

The importance of conducting regular security awareness training that keeps up with the latest threats cannot be overstated. Having savvy, vigilant employees who recognize and avoid potential security threats and practice safe online behaviours drastically reduces the likelihood of a devastating cyber incident and fulfils compliance and cyber insurance requirements

CYBERATTACKS KEEP INTENSIFYING

Since employees form the core of any business, they will always be the main target of cyberattacks. The tactics used by cybercriminals are constantly evolving and so should your approach to defence. Making sure your end users pay careful attention and stay up to date with cybersecurity best practices is imperative.

90% of security breaches are caused by human error

LOWER YOUR CYBER RISK LEVELS

Security awareness training and phishing simulations go hand in hand to reduce the likelihood of security breaches. Phishing simulations test employees on how they would respond to a real-life phishing attack. You can track which employees have clicked on links in the phishing email, opened an attachment or given away their password. Once risky behaviours are identified, our platform delivers engaging educational videos to the users. Each video is accompanied by a quiz to test the training content retention. Automated reporting lets you monitor ongoing progress and analyse and share metrics with clients to demonstrate the value of security training.

MEET CLIENTS' CYBER INSURANCE AND COMPLIANCE NEEDS

Security awareness training is now a requirement for obtaining cyber insurance coverage. With the frequency and cost of cyberattacks escalating, it has become increasingly difficult to obtain a cyber insurance policy, leaving you vulnerable to devastating recovery costs if an attack takes place. Our service helps implement a user security awareness training program required to qualify for or to renew a policy. Ongoing security awareness training is required for compliance, especially if operating in healthcare, retail, government contracting and other sectors subject to regulatory oversight and implementing a security awareness training program to comply with industry regulations, like HIPAA, GDPR, CMMC, PCI-DSS, NIST 800-171 and others, and avoid incurring high fees for non-compliance.

Reduce your risk of experiencing a cyberattack by up to 70% with security awareness training.

PHISHING SIMULATION & SECURITY AWARENESS TRAINING

Ongoing, up-to-date employee cybersecurity training is a necessity in today's increasingly dangerous online threat environment. BullPhish ID educates and empowers your clients' employees, making them the best defence against cybercrime.

CUSTOMIZABLE SIMULATIONS

Using the email templates to quickly launch phishing exercises or customize emails and sending domains to align with your needs and specific threats you may encounter.

BRANDING FRONT AND CENTER

We can white label the user training portal with our logo and/or your company's.

EASY CAMPAIGN MANAGEMENT

We can automate directory sync which makes managing user groups for training and phishing campaigns easy and fast, and we can set up training weeks and months in advance to run automatically at designated times.

VIDEO-BASED TRAINING

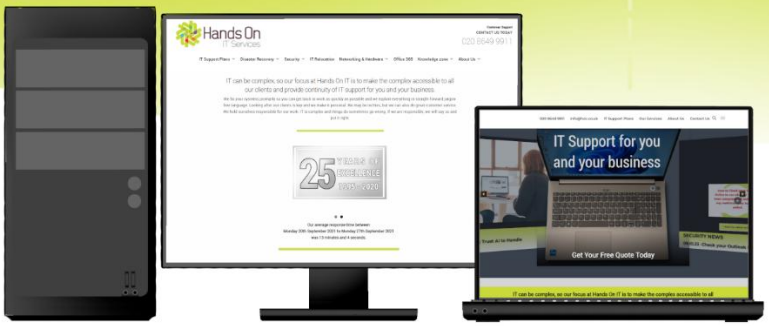
We offer brief, engaging security and compliance training videos in eight languages. We can test users' knowledge retention with online quizzes. A **FREE EXTRA FEATURE:** Upload your own training content.

INSIGHTFUL REPORTING

We can get automated reports showing your phishing exercise and training campaign results. It helps us assess your security posture and show the progress and value of training.

Hands On IT Services

Information Archiving

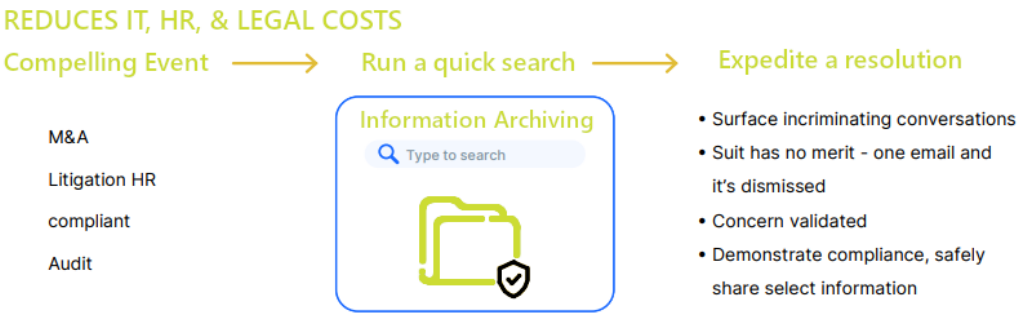


Managing daily electronic communications can be overwhelming and costly. Our modern archiving solution provides a proactive approach to compliance, simplifying the management of your historical data.

Why Choose Information Archiving?

- Universal Capture: Indexes and stores inbound, outbound, and internal communications from over 50 sources, including Email and Microsoft Teams.
- Compliance Ready: Easily adapt to regulations such as GDPR, HIPAA, SEC, and PCI DSS.
- Cost Efficiency: Reduces IT, HR, and legal costs by consolidating data into one searchable location.
- No Expertise Needed: Designed to be user-friendly with no technical expertise required.

How It Works



- Capture: Data is reformatted into electronic mail (EML) format.
- Journal: Information is stored in a searchable database with advanced indexing.
- Protect: Data is stored in an immutable "Write Once, Read Many" (WORM) state to prevent alteration.
- Retrieve: Seamlessly search and share datasets with internal or external stakeholders using SimplyShare technology.

Key Features & Benefits

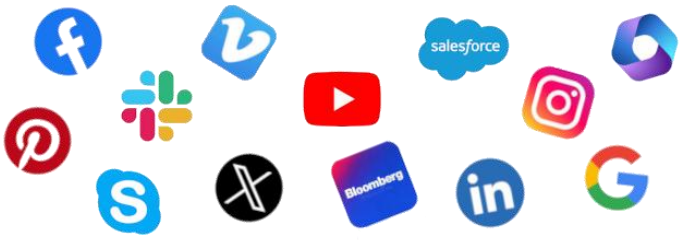
- Quickly and securely share eDiscovery findings with outside parties during litigations – without SFTP sites or external hard drives
- Intuitively search data across email, social media and collaboration tools
- Save time and money by using a solution that consolidates 50+ sources of communication data into one search
- Increase security with delegated access control
- Investigate complaints and violations faster by examining all communications in one place.
- Set policies from one month to indefinite (default is 6 years) with Custom Retention.

Protecting your organization against compliance violations and unplanned litigations.

Also Available: Comprehensive Teams Archiving

- We capture more than just text. Our service archives:
- Individual and Group chat messages.
- Channel posts and file uploads.
- Meeting recordings and scheduled events.
- System events and even Emojis.

Examples of other services that can be archived are: - Facebook, Instagram, LinkedIn, Pinterest, Salesforce, Skype, Slack, Twitter/X, Vimeo, Yammer, YouTube and Bloomberg Terminal and more.



Hands On IT Services

.co.uk .info .net .com

eNom Domain Registrar

Domain Registrar Service

Who is eNom?

eNom is a leading domain name registrar and web hosting company. They offer a variety of services including domain name registration, web hosting, email services, SSL certificates, and website building tools.

Why we use them?

We primarily use them as a domain registrar to manage the reservation of internet domain names. Here are some key functions of eNom:

1. **Domain Name Registration**: They allow individuals and organizations to register a domain name, which is the address people use to access websites (e.g., www.example.com).
2. **DNS Management**: They provide tools to manage the Domain Name System (DNS) settings, which control how domain names are translated into IP addresses.
3. **Renewals and Transfers**: They handle the renewal of domain registrations and the transfer of domains between registrars.

What is the current pricing when registering a domain name with Hands On IT Services?

These are the top domain extension.

1. **.co.uk** - The most popular country-specific domain for the UK.
2. **.uk** - Another widely used UK-specific domain extension.
3. **.com** - A globally popular domain extension, also extensively used in the UK.
4. **.org.uk** - Often used by non-profit organizations in the UK.
5. .**org** - Used by various organizations, including non-profits.
6. **.net** - Commonly used by network services and internet providers.
7. **.me.uk** - Typically used for personal websites in the UK.
8. **.info** - A generic top-level domain used for informational websites

Transferring a domain typically takes between **24 hours to 7 business days**

The key process involves several steps, including:

1. **Unlocking the domain** with the current registrar.
2. **Obtaining an authorization code** (also known as an EPP code or transfer code).
3. **Initiating the transfer** request with the new registrar.
4. **Confirming the transfer** via email or other verification methods.

These steps are dependent on the Top-Level Domain extension and so, during this period, there might be brief downtime for your website or email services

It's a good idea to plan and inform any users or clients about the potential temporary unavailability.