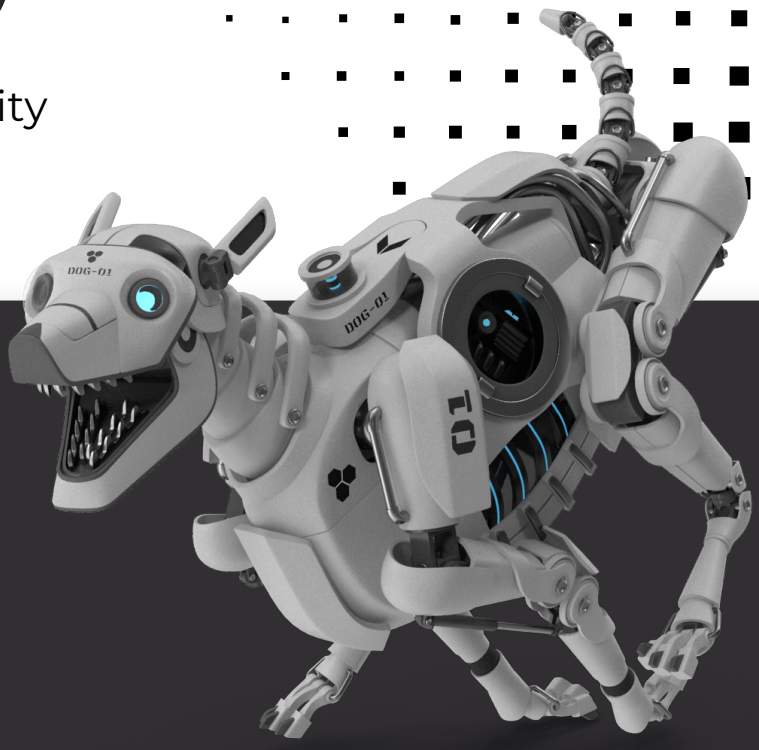
LANDALL

**Speak with an expert**
+44 (0) 330 043 2408

SECURITY

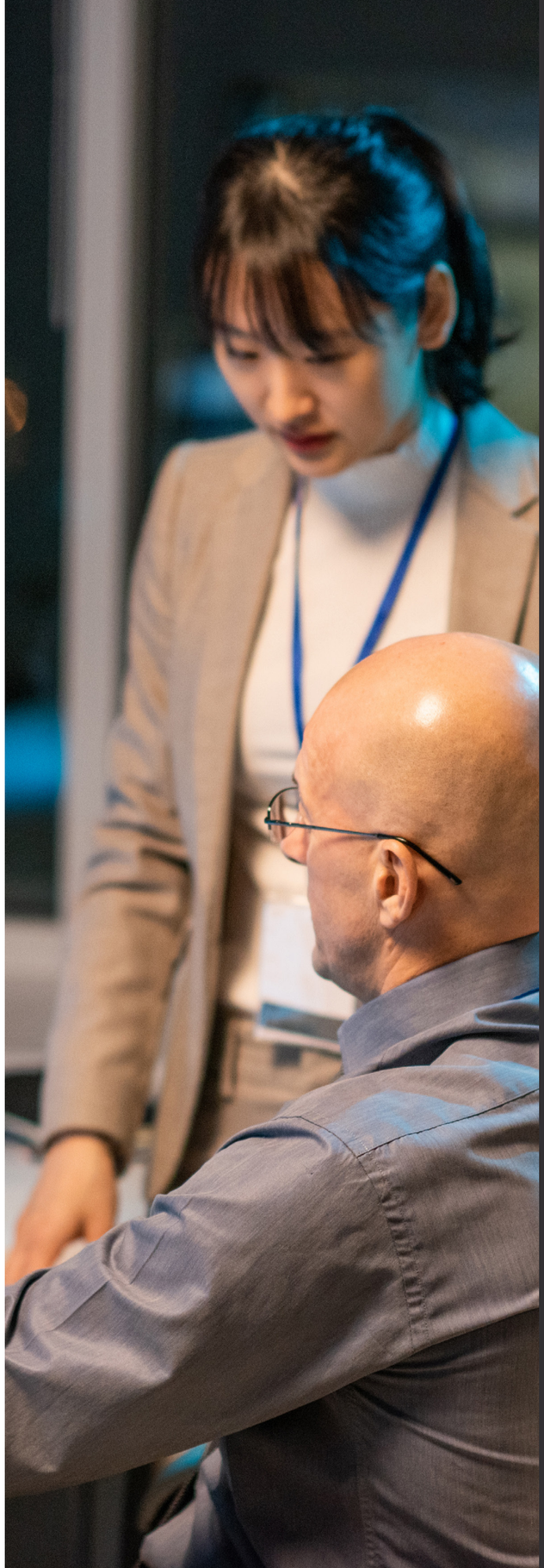
# Managed Cyber Security

Around the clock security monitoring




*Supported by AI-Powered 24/7 Guard Dog Protection*

# Suffering a data breach isn't a question of **if** - it's a question of **when**.



## Table of Contents


04. What is Cyber Security

05. Why Choose Landall Services

06. The Threat Landscape

08. Security Operations

10. Software-as-a-Service

12. Zero Trust Network

14. Security Professional Service

16. Cyber Security Training

18. Security Operations Centre

20. Dark Web Monitoring

22. Vulnerability Scanning

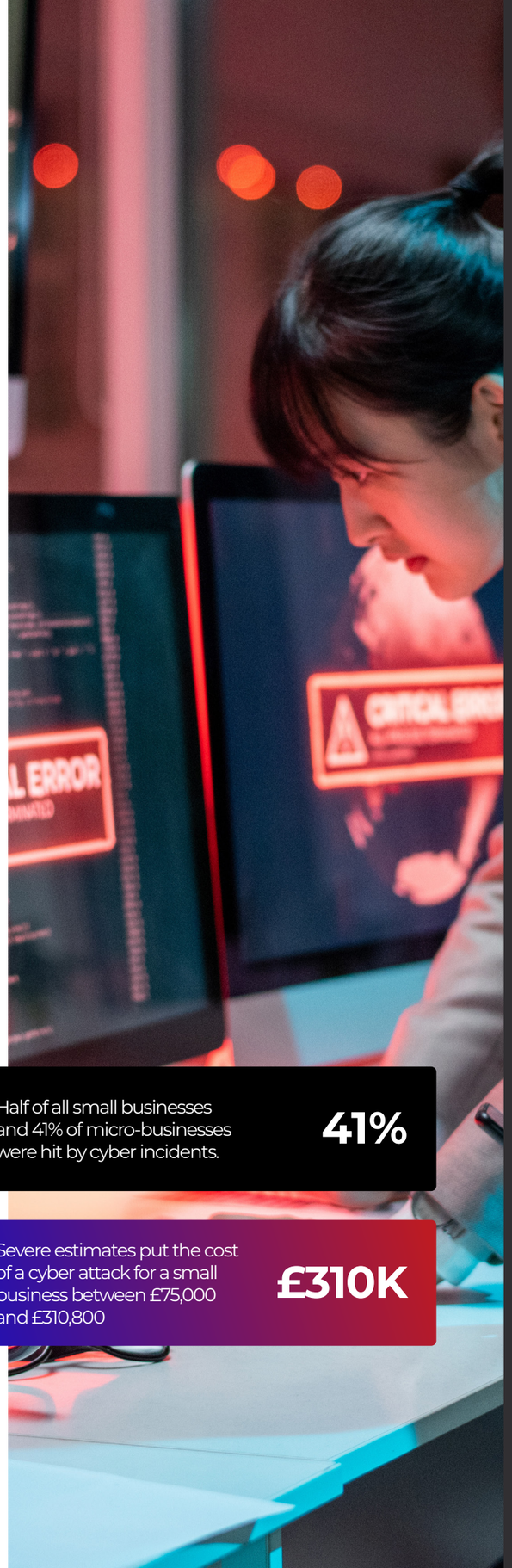
24. Cyber Security Assessment

26. Case Study

# What is Cyber Security?

**Without cyber security, your business is wide open to digital break-ins. Think of it like leaving your office doors unlocked, the windows open, the shutters rolled up, and a sign on the door saying, "come on in." Anyone could walk up, take what they want, or cause damage - and you might not realise until it's too late. That's exactly what happens when systems aren't protected.**

As businesses rely more on technology and expand their online presence, they **face ever-growing risks from cybercriminals** targeting weaknesses in their systems. A successful **cyber attack can cause serious harm**, including financial losses, reputational damage, loss of customer trust, and legal challenges. **Landall Services offers tailored solutions** and expert support for organisations of all sizes and industries, using trusted technologies from the world's leading cyber security providers.



43% of UK businesses faced a cyber attack or breach in the past year - that's over 600,000 companies. **43%**

Half of all small businesses and 41% of micro-businesses were hit by cyber incidents. **41%**

UK SMEs lose around £3.4 billion every year due to cyber attacks. **£3.4B**

Severe estimates put the cost of a cyber attack for a small business between £75,000 and £310,800 **£310K**



# Why Choose Landall Services

### Consultancy-led

Tailored advice and strategic planning from cyber security experts who align solutions with your specific risks and business goals.

### Proactive Threat Hunting

Experts actively searching for hidden risks and vulnerabilities before they can be exploited.

### Scalable Services

Flexible offerings that grow with your business, accommodating evolving threats and changing needs.

### Rapid Incident Response

Fast mobilisation of resources and expert teams to minimise the impact of any security incident.

### Dedicated Account Management

A single point of contact who understands your business, coordinates all security activities, and ensures seamless communication.

### Training & Awareness Programme

Ongoing education for your employees to build a security conscious culture and reduce human related risks.

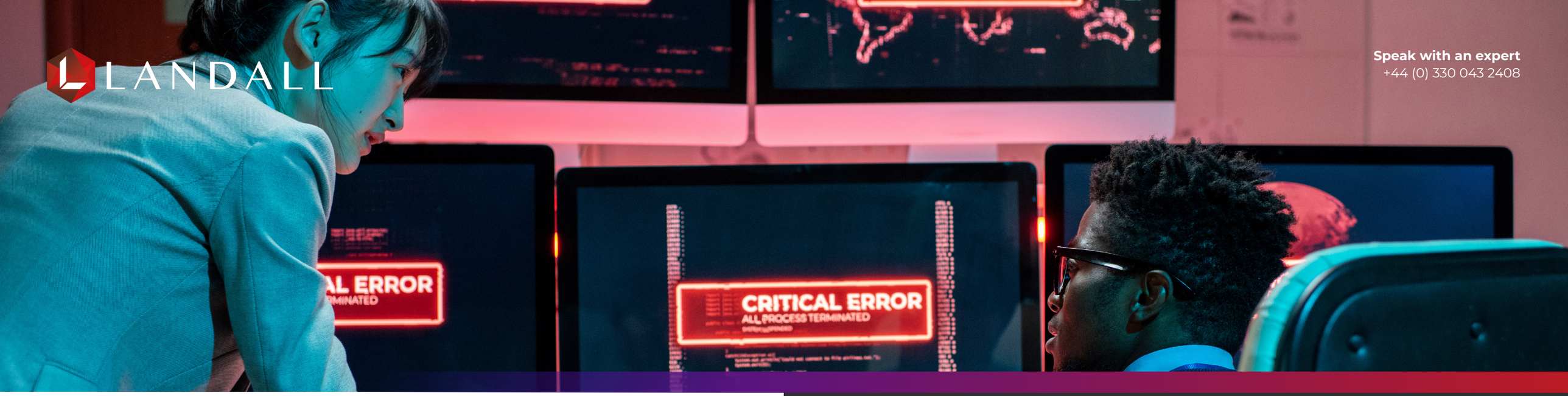
### Proactive Security Monitoring

Continuous surveillance and around-the-clock assistance to detect threats early and respond immediately.

### Continuous Improvement

Regular review and enhancement of security measures to stay ahead of emerging threats.

## Certified Service Delivery Professionals




EVOLVING RISK

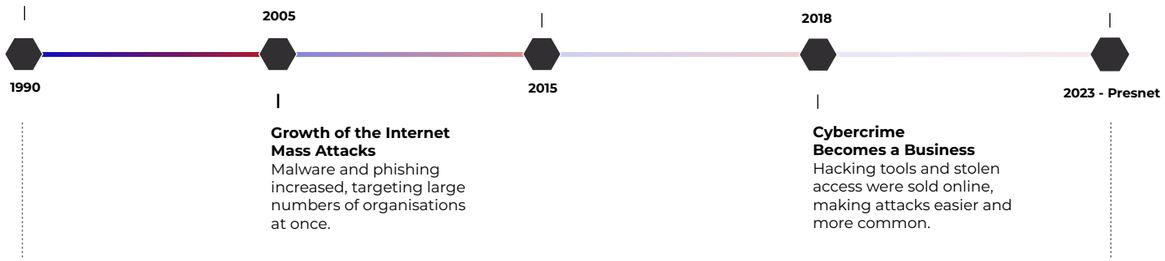
# The Threat Landscape Has Fundamentally Shifted

Attackers no longer target only large enterprises. Increasingly, they focus on SMEs, which may lack continuous security oversight and resilience. Staying secure means understanding the full range of threats lurking in today's digital world.

**Early Days**
Attacks were basic and easy to spot, often random and unsophisticated.

**Cloud & Remote Working**
Attacks became more targeted, stealing login details and moving quietly inside systems.

**AI-Driven Threats Today & Beyond**
Criminals use AI to launch faster, smarter, and harder to detect attacks.




**Growth of the Internet Mass Attacks**
Malware and phishing increased, targeting large numbers of organisations at once.

**Cybercrime Becomes a Business**
Hacking tools and stolen access were sold online, making attacks easier and more common.

**Ransomware**
First identified in 1989, ransomware is far from a new phenomenon. However, despite its decades-long history, it remains one of the most prevalent and financially damaging cyber threats facing organisations today. Modern ransomware attacks are significantly more sophisticated than their early predecessors, often involving data exfiltration, double extortion tactics, and highly targeted infiltration methods designed to disrupt operations and pressure businesses into payment.



**Cybercriminals are using smarter and faster tools than ever before. Instead of just breaking in, they now use artificial intelligence (AI) to hide their attacks, trick users, and get past standard security measures quickly.**

Because attackers use AI, protecting your business has become more difficult. Threats like fake emails that look real, automated hacking attempts, and fake audio or videos are becoming common - and much harder to spot.

## AI-Driven Threats

**Double Agents**
AI bots that quietly explore and hack company systems without being noticed

**Deepfake Scams**
Fake videos or audio of leaders used to fool staff into making bad decisions or payments.

**AI-Gen Fake Messages**
AI creates convincing emails, texts, and calls to trick employees into giving up info or access.

**Stealing Passwords**
AI tools that quickly guess or steal passwords and then gain higher access inside systems.

**Smart Malware**
Malware that adapts its behaviour to slip past security tools and stay hidden.

**Supply Chain Attacks**
Using AI to find and exploit vulnerabilities in suppliers or partners to get into your network.

**Prompt Injection**
Manipulating AI by feeding it bad data or commands to make it do harmful things.

**Risks from Uncontrolled AI Tools**
Security issues from AI apps used without proper control or oversight inside the company.

**Speak with an expert**
+44 (0) 330 043 2408

# Security Operations

## Highly trainined security professionals ready to take action

Security operations (SecOps) is the day-to-day protection of information, assets and infrastructure.  A dedicated Security Operations Team provides constant vigilance against cyber threats, detecting and responding to attacks before they disrupt your business. By combining expert knowledge with advanced technology, they reduce risk, minimise downtime and protect your valuable data, giving you peace of mind and the freedom to focus on growth.

**The benefits**

Security Operations give you visibility, control, and fast response - reducing risk, downtime, and business impact.

- Limits damage from cyber incidents
- Detects threats early
- Provides peace of mind
- Reduces disruption and downtime

## What this includes

### Managed Security Operations Centre (SOC)

Delivers expert, 24/7 threat monitoring and rapid response without the cost and complexity of an in-house team, helping you to stay protected around the clock.

### Extended Detection & Response (XDR)

Offers deeper, unified visibility across your entire digital environment, enabling faster and more accurate threat detection and automated responses to stop attacks before they escalate.

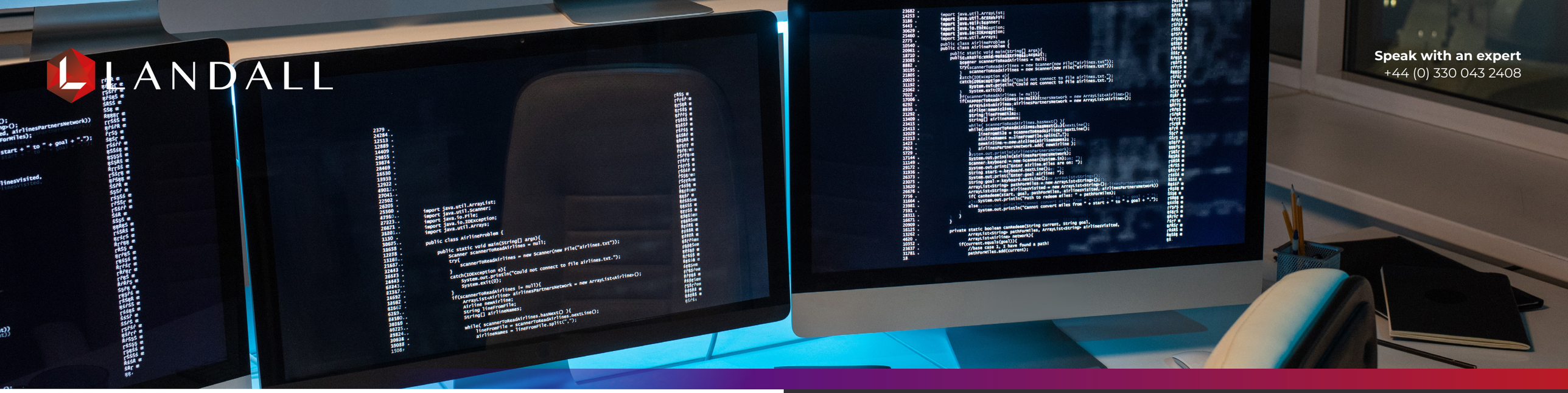
### Endpoint Protection

Protects all devices connected to your network by blocking threats at the source, preventing attacks from spreading and keeping your systems safe and reliable.

### Reduce the risk of a breach

Don't wait to become a victim: protect your business now.

Call an expert on:
**+44 (0) 0330 043 2408**







# Software-as-a-Service (SaaS)

## Complex to simple solutions that protect your data

Software-as-a-Service (SaaS) shields the essential online tools your team relies on every day - like email, web browsing, and cloud apps - from ever-evolving cyber threats.

With your staff potentially working from anywhere, these tools become a prime target for cybercriminals looking to exploit weaknesses and steal your valuable data. SaaS security blocks attacks before they reach your people or systems, keeping your business safe and your team confident.

**The benefits**

Protect your organisation with expert SaaS security designed for today's digital work environment.

- Reduced risk of data breaches
- Simplified compliance
- Better visibility and control
- Improved productivity
- Support for remote and hybrid work

## What this includes

### Email Security

Blocks phishing, malware, spam, and prevents sensitive data leaks. It stops threats before they reach your inbox, keeping communication safe and compliant.

### Web Security

Monitors and controls internet access, blocks harmful sites, enforcing safe browsing and protecting users from web-based threats while maintaining productivity.

### Cloud Access Security Broker

Gives visibility and control over all cloud apps in use. It detects risky behaviour, enforces policies, prevents data loss, and secures shadow IT.

### Reduce the risk of a breach

Before you become a victim, protect your business and your data with a team of cyber security professionals.

Call an expert on:
**+44 (0) 0330 043 2408**




# Zero Trust Network Access

## Take full control of your network access - never trust, always verify

Traditional security trusts anyone inside the network, but today's remote work and cloud use mean attackers can easily exploit stolen credentials and weak access controls. This allows them to move undetected, putting your sensitive data and systems at risk.

### The benefits

Secure your business today with technology that adapts and protects as fast as threats evolve.

- Strict control over who accesses what
- Enhanced protection for remote workers
- Continuous checks to block threats early
- Secure user experience without traditional VPN

## What this includes

### Multi-Factor Authentication (MFA)

Don't settle for just a password: MFA demands multiple types of proof of identity - like a code sent to a phone or a biometric scan - making it exponentially harder for attackers to break in. This simple step blocks 99.9% of account hacks, protecting your business instantly.

### Unified Identity Protection

Manage all user access from a single, secure platform. This means you set strict rules that govern who can reach what, when, and how - across every app and device. By simplifying control, you reduce human error and close gaps attackers exploit.

### Secure Access Service Edge (SASE)

Combine network and security functions in one cloud-delivered service that gives your teams fast, secure access from anywhere. SASE removes complexity, cuts delays, and blocks threats at the edge before they reach your network, keeping your data safe without slowing your people down.

### Reduce the risk of a breach

Before you become a victim, protect your business and your data with a team of cyber security professionals.

Call an expert on: **+44 (0) 0330 043 2408**

**Speak with an expert**
+44 (0) 330 043 2408

# Cyber Security Professional Services

## Expert guidance to strengthen your security posture

Cyber threats evolve constantly, and keeping up with the latest risks, regulations, and technologies can overwhelm even experienced teams. Without specialised expertise, critical vulnerabilities may go unnoticed, exposing your business to costly breaches and compliance failures.

A single security oversight can lead to data loss, operational downtime, and severe reputational damage. Compliance breaches bring fines and legal consequences. Many organisations struggle with limited resources and expertise, making reactive security measures the norm - leaving them one step behind attackers.

**The benefits**

Secure your business today with technology that adapts and protects as fast as threats evolve.

- Expert insight
- Tailored strategies
- Empowered workforce
- Proactive defence
- Regulatory confidence
- Ongoing support



## What this includes

### Security Assessments & Penetration Testing

Identify weaknesses before attackers do with thorough, simulated attacks.

### Risk Management & Compliance Support

Navigate complex regulations and align your security with industry standards.

### Policy & Procedure Development

Create clear, practical security policies that your staff can follow.

### Incident Response Planning & Simulation

Equipping your team to react swiftly and effectively if a breach occurs.

### Security Awareness Training

Provide users with the skills and awareness they need.

### Cybersecurity Incident Reporting

Document events for best practice and to meet compliance requirements.



# Cyber Security Training & Awareness

## Turn your people into your strongest line of defence

Most cyber incidents don't start with **complex hacking - they start with a simple human mistake**. Clicking a phishing email, using a weak password, or sharing information with the wrong person can instantly bypass even the best security technology.

Cybercriminals deliberately target employees because it's easier to trick a person than break through a firewall. One moment of distraction can lead to data loss, ransomware, downtime, and reputational damage. Without regular training, staff remain unaware of the risks - and attackers take advantage.

**The benefits**

Reduce risk by educating, testing, and protecting your people.

- Reduced human error
- Stronger first line of defence
- Improved security culture
- Support for compliance
- Ongoing risk reduction

## What this includes

### GDPR Awareness & Training

Ensure staff understand how to handle personal data correctly to reduce the risk of compliance breaches.

### Security Awareness Training & Testing

Regular, easy-to-understand training supported by testing to reinforce safe behaviour.

### Phishing Prevention

Simulated phishing attacks train staff to spot and report suspicious emails before real threats cause harm.

### Dark Web Monitoring

Detect stolen credentials early by monitoring criminal marketplaces and acting before accounts are abused.

### On-site Training

Identify and fix weaknesses in systems and applications before attackers exploit them.

### Reduce the risk of a breach

Before you become a victim, protect your business and your data with a team of cyber security professionals.

Call an expert on: **+44 (0) 0330 043 2408**

# 24/7 Security Operations Centre (SOC)

## Expert, 24/7 threat detection and response without the cost or complexity of building your own security team

A Managed Security Operations Centre provides continuous protection by combining advanced monitoring technology with dedicated security analysts who watch over your systems day and night. This service identifies threats in real time, investigates suspicious activity, and responds rapidly to contain incidents before they escalate.



**Speak with an expert**
+44 (0) 330 043 2408

# The Benefits

**Stronger Compliance Posture**
Comprehensive logging, reporting, and audit-ready documentation to support regulatory requirements.

**Lower Operational Costs**
A cost effective alternative to building, staffing, and maintaining an in-house SOC.

**Always On Protection**
Always on monitoring to catch threats before they disrupt operations.

**Faster Threat Response**
Automated and specialist led actions that contain threats quickly and minimise business impact.

**Access to Specialist Expertise**
Round-the-clock support from experienced analysts, incident responders, and threat intelligence specialists.

## Key Service Highlights

- 24/7 monitoring and alert management by certified security specialists
- Advanced Security Information and Event Management (SIEM) and XDR technologies for deeper visibility and accurate detection
- Real-time incident triage, investigation, and containment
- Integrated threat intelligence to stay ahead of emerging risks
- Clear, actionable reporting and governance insights
- Log retention, compliance alignment, and forensic analysis support

Cyber attacks often go unnoticed until serious damage has been done, but organisations with continuous monitoring dramatically reduce their exposure. Acting now puts you ahead of threats rather than reacting after the fact. Make the decision that protects your future.

**Schedule your security assessment today: because postponing protection only increases the risk.**

**Book Assessment Now**

# Dark Web Monitoring

## Find stolen data before criminals use it against you

Cybercriminals trade stolen business data on hidden online marketplaces via the dark web. Email addresses, passwords, and company information are often sold quietly - long before a breach is discovered. Without visibility, businesses remain exposed and unaware until real damage begins.

Dark web scanning continuously monitors criminal marketplaces for stolen credentials and sensitive business data linked to your organisation. When a match is found, you are alerted immediately so action can be taken - before attackers gain access or cause disruption.



**Speak with an expert**
+44 (0) 330 043 2408

## The Benefits

- **Early Threat Detection**
  Identify exposed credentials before they are used in an attack.
- **Reduced Breach Risk**
  Act quickly to secure accounts and prevent unauthorised access.
- **Stronger Compliance Support**
  Demonstrate proactive protection of personal and business data.
- **Improved Security Awareness**
  Understand where risks originate and strengthen weak points.
- **Peace of Mind**
  Know that hidden threats are being monitored around the clock.

## Key Service Highlights

- Continuous monitoring of dark web marketplaces
- Detection of stolen usernames, passwords, and company data
- Rapid alerts with clear guidance on next steps
- Integration with wider security and response services
- Simple, non-technical reporting for business leaders

Once data appears on the dark web, the clock starts ticking. The longer it goes unnoticed, the greater the risk. Businesses that act early reduce damage, downtime, and cost.

### Protect What You Can't See

Don't wait for stolen data to become a security incident.

**Schedule your dark web scan today - because early warning changes the outcome.**

**Book a Dark Web Scan Now**

# On-request Vulnerability Scanning

## Spot security weaknesses anytime to fix before they are misused

Every network, system, and application has potential weaknesses - outdated software, misconfigurations, or missing patches. Cybercriminals constantly search for these gaps to exploit. Without regular, up-to-date checks, you're operating blind to serious risks.

Our on-demand service runs comprehensive scans on your entire environment - systems, networks, and applications - whenever you want. Identify risks immediately, prioritise the most critical weaknesses, and act fast to remediate before attackers strike.



**Speak with an expert**
+44 (0) 330 043 2408

# The Benefits

**Instant Risk Visibility**
Scan your environment anytime to reveal new vulnerabilities as they arise.

**Faster Remediation**
Fix vulnerabilities quickly, reducing your attack surface and limiting exposure.

**Flexible and Scalable**
Use scans as often as needed and scale with your business growth: no long term commitments.

**Focused Risk Prioritisation**
Receive clear reports highlighting the most urgent issues that could impact your business.

**Compliance Made Easier**
Show regulators you're actively managing security risks with regular scanning and reporting.

## Key Service Highlights

- Immediate, on-demand scanning with no wait times
- Broad coverage across networks, servers, and applications
- Clear, non-technical reports prioritising critical risks
- Expert guidance on fixing vulnerabilities fast
- Integration with your wider security strategy

Every day without a scan is another day a vulnerability can be exploited. Don't wait for a breach to reveal your risks. Take control and protect your business with instant insight and rapid action.

**Contact us now to schedule your first on-request vulnerability scan.**

**Book Assessment Now**

# Free Cyber Security Assessment

## Discover your vulnerabilities before attackers do - at no cost

Cyber threats are growing more sophisticated every day. Without a clear understanding of your current security risks, your business could be vulnerable, exposing you to data breaches, costly downtime, and compliance penalties.

**Why Take Advantage Now?**

Reduce risk by discovering vulnerabilities before they are exploited.

- No cost, no obligation
- Early detection saves money
- Peace of mind



**Speak with an expert**
+44 (0) 330 043 2408

# What's included

- **Comprehensive Security Review**
  We assess your current cyber security posture to give you a clear overview of your organisation's risk exposure and readiness.
- **Identify Hidden Vulnerabilities**
  Spot weaknesses attackers could exploit before they cause damage.
- **Clear, Actionable Report**
  Receive an easy-to-understand summary of risks, their potential impact, and practical next steps.
- **Tailored Recommendations**
  Get expert advice on how to strengthen your security, prioritised to fit your business needs and budget.

# How It Works

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **Schedule Your Assessment** | **We Conduct a Thorough Review** | **Receive Your Report & Recommendations** | **Decide Your Next Steps** |

# Take Control of Your Cyber Security Today

Don't wait for a costly breach to reveal your risks. This free assessment gives you the clarity and confidence to protect your business - starting now.

**Contact us to book your Free Cyber Security Assessment. Your security can't wait.**

**Book Assessment Now**

**Speak with an expert**
+44 (0) 330 043 2408

ALBION STONE
Portland Stone - Naturally

# High-End Mining Company

## How an infrastructure overhaul resulted in improved cyber security

### Introduction

A family-owned mining business needed an IT and cyber security solution that could scale alongside its continued growth. With multiple sites and increasing operational demands, the Company required reliable communication, secure connectivity, and a modern infrastructure capable of supporting a dispersed workforce. To achieve this, improvements were made to strengthen performance, enhance security, and support long-term scalability.

> *The team quickly understood our challenges and delivered a solution that improved security, supported flexible working, and modernised our infrastructure with minimal disruption. Their consultative approach and technical expertise made the entire process smooth and highly effective.*
>
> **Jordan**

### When Legacy Systems Meet Modern Demands

The company faced a growing challenge as cyber threats increased and legacy systems struggled to meet modern demands. What had once been reliable infrastructure had become a potential source of risk, with ageing technology unable to provide the security, flexibility, or scalability required in a rapidly changing business environment.

At the same time, the shift towards hybrid and remote working fundamentally changed how employees accessed systems and information. Solutions designed for office-based working proved inadequate, forcing the organisation to rely on workarounds that introduced further complexity and vulnerability.



# How we successfully solved this challenge

We replaced on-premise servers and ageing hardware with a centralised, cloud-based virtual server environment. All physical data was migrated to SharePoint, providing a secure and accessible document management platform. The accounts system was moved to a virtual server hosted in Azure, enabling a consistent and secure way for staff to access business-critical applications.

The result was a fully cloud-based solution that allowed employees to work efficiently and securely from any location with an internet connection.

## The outcome following implementation

### Improved Security

Modern, fully managed cloud systems significantly reduce the risk of cyber attack. With enhanced monitoring, proactive maintenance, and robust disaster recovery options, the Company now benefits from a far more resilient security posture.

### Better Communication

Staff can now collaborate seamlessly from any location, with the reassurance that their data and devices are protected. Remote working is supported securely and efficiently, improving productivity across all sites.

### Flexible Scalability

Cloud infrastructure allows the business to scale up or down with ease. New users, storage, and services can be added quickly and cost-effectively, ensuring the IT environment can grow without disruption.

### Additional Benefits

By retiring physical servers, the Company has reduced energy consumption, cooling requirements, maintenance overheads, and the noise and space previously dedicated to on-site hardware. This not only lowers costs but supports more sustainable IT operations.

LANDALL

**Speak with an expert**
+44 (0) 330 043 2408


*Supported by AI-Powered 24/7*
*Guard Dog Protection*

www.landall.co.uk