MANAGED DETECTION & RESPONSE

Your Secure Defend

Detect.
Investigate.
Respond.

Most security tools generate alerts. Your Secure Defend investigates and responds to them.

Unified managed cyber defence, monitored 24x7, powered by the Heimdal Unified Cybersecurity Platform, from Your IT Department Ltd.

MONITORED 24x7

- **Endpoint** — Detect and contain
- **Email** — Phishing and fraud
- **Microsoft 365** — Identity and access

GET IN TOUCH

your-itdepartment.co.uk | info@your-itdepartment.co.uk | 0115 822 0200

Your IT Department Ltd
Unit 8, Farrington Way, Eastwood, Nottingham, NG16 3BF
info@your-itdepartment.co.uk your-itdepartment.co.uk

AWARD-WINNING IT SUPPORT
for business

Contents

ABOUT THIS BROCHURE

This brochure introduces Your Secure Defend, the managed detection and response service from Your IT Department. It explains who the service is for, what is included, and how it's delivered. For a tailored quote, please speak to your Your IT Department account contact.

Why Your Secure Defend

Prevention is no longer enough. The real question is whether you will know when something gets in. Your Secure Defend is Your IT Department's managed detection and response service. It is designed for organisations that need continuous cyber defence capability without building their own internal Security Operations Centre.

The service is based on the Heimdal security stack and combines predictive DNS security, endpoint protection, ransomware protection, email security, threat hunting, SIEM-style monitoring, 24x7 security operations oversight and incident response coordination into a single managed service.

> **Most security tools generate alerts. Your Secure Defend investigates and responds to them.**

A UNIFIED PLATFORM, NOT A PATCHWORK OF TOOLS

Rather than stitching together separate antivirus, DNS filtering, email security and monitoring tools, Your Secure Defend delivers layered protection across endpoint, email, network, identity and Microsoft 365 environments through one managed platform.

Is this you?

Your Secure Defend is designed for a specific type of organisation. If the descriptions below sound familiar, this service was built for you.

Security-conscious SMEs without a SOC

You need managed cyber defence capability but don't have, or want to build, an internal Security Operations Centre.

Material threat exposure

Ransomware, email compromise, account compromise or endpoint threats represent a material operational risk to your business.

Insurance & incident readiness

Your leadership team is looking for better cyber insurance readiness and improved incident response capability.

Co-managed clients

Your internal IT team needs additional threat monitoring, investigation and response capability, without replacing their function.

TYPICAL BUYERS

Managing Director, Finance Director, Operations Director, IT Manager or Compliance Lead, anyone accountable for reducing cyber risk and demonstrating incident readiness.

Outcomes for your business

Your Secure Defend is built around measurable business outcomes, not just technical delivery.

Outcome	What this means for your business
Earlier threat detection	Suspicious activity is identified and investigated before it becomes a wider business incident.
Reduced ransomware risk	Layered endpoint, DNS and ransomware protection helps reduce exposure to encryption-based attacks.
Stronger email defence	Phishing, spam, malicious attachments and business email compromise risks are reduced.
Improved Microsoft 365 threat visibility	Microsoft 365 threat activity and identity-related security signals are monitored and investigated.
Security operations capability	You gain access to monitoring, escalation and response coordination without building a SOC.
Better executive confidence	Monthly reporting and incident coordination provide clearer cyber risk visibility.
Simplified security stack	Multiple protection layers are managed through a unified platform and delivered as one service.

POWERED BY HEIMDAL

Endpoint protection & predictive DNS security

Stopping threats before they reach your business

Layered endpoint controls and DNS-level protection designed to block malicious destinations and command-and-control activity before they cause harm.

Endpoint protection & response

- Next-generation antivirus protection
- Endpoint detection and response capability
- Behavioural threat monitoring
- Malware prevention and remediation
- Threat intelligence-driven blocking
- Automated threat containment where supported by policy
- Rootkit and backdoor protection where supported

Predictive DNS security

- DNS security for endpoints
- DNS security for network-level protection where deployed
- Malicious domain blocking
- Threat intelligence-driven filtering
- Command-and-control protection
- Prevention of communication with known malicious infrastructure

POWERED BY HEIMDAL

Ransomware & email threat protection

Protecting your two highest-risk attack surfaces

Dedicated anti-ransomware controls, combined with layered protection against phishing, spam and business email compromise.

Ransomware encryption protection

- Ransomware Encryption Protection
- Signature-free ransomware behaviour monitoring
- Automated containment of suspected ransomware activity
- Protection aimed at reducing business disruption from encryption attacks

Email security & fraud prevention

- Advanced email threat protection
- Spam filtering and phishing protection
- Malicious attachment and link detection
- Email Fraud Prevention
- Business Email Compromise protection
- Impersonation and social engineering risk reduction

IDENTITY & THREAT VISIBILITY

Microsoft 365 threat monitoring

Watching for compromise, not just configuration

Active monitoring of Microsoft 365-related threat activity. This is focused on threat visibility and investigation, the broader Microsoft 365 governance work sits with Your Secure 365.

Microsoft 365 threat monitoring

- Microsoft 365 security alert monitoring
- Identity threat monitoring
- Account compromise detection
- Suspicious sign-in investigation
- Privileged account monitoring
- Security event investigation and escalation

INVESTIGATION & RESPONSE

Threat hunting, SIEM & 24x7 security operations

Security operations capability, without building a SOC

Investigation and response workflow capability, unified security event visibility, and continuous monitoring across your managed security estate.

Threat hunting & action centre

- Centralised threat investigation
- Alert triage
- Threat hunting workflows
- Security escalation
- Incident identification
- Response coordination activities

SIEM & unified monitoring

- Security event collection and correlation
- Threat visibility and prioritisation
- Investigation workflows
- Unified monitoring and reporting
- Security analytics and incident evidence gathering

24x7 security operations

- 24x7 security monitoring and alert validation
- Threat investigation and security escalation
- Incident coordination
- Security reporting and recommendations

What you receive every month

Beyond the underlying technology, Your Secure Defend delivers a consistent set of operational activities and reporting every month.

Deliverable	Description
Managed security tooling	Configuration and management of the included Heimdal security components.
Threat monitoring	Continuous monitoring of alerts and security events from managed components.
Alert triage	Review and prioritisation of security alerts.
Threat investigation	Investigation of suspicious activity across endpoint, email, identity and Microsoft 365 signals.
Incident response coordination	Escalation, containment guidance and coordination of response activity where a security incident is identified.
Monthly security reporting	Summary of security posture, events, actions and recommendations.
Security improvement recommendations	Practical recommendations identified through monitoring and operational review.

Where Your Secure Defend fits

Your Secure Defend is the active detection and response layer within the Your IT 360 Framework. It is intentionally separated from Microsoft 365 security governance, compliance assurance and infrastructure management.

Requirement	Delivered by
Microsoft 365 security governance	Your Secure 365
Secure Score management	Your Secure 365
Conditional Access design and governance	Your Secure 365
Cyber Essentials certification	YourFortify
Vulnerability management and compliance assurance	YourFortify
Infrastructure management	Your Infrastructure
User support and device support	Your Workplace
Automation and AI workflow services	Your Automation
Major incident remediation or recovery project work	Separate statement of work where required

Investment

Your Secure Defend is provided using fixed monthly user bands. User counts are rounded up to the next available tier, for example, a business with 28 users is quoted as "up to 30 users".

UP TO USERS	MONTHLY FEE
20	£300
30	£450
40	£600
60	£840
80	£1,080
100	£1,300
125	£1,600
150	£1,875
151+	Custom quotation

Prices shown are standard published starting rates, exclusive of VAT. Opportunities above 150 users are commercially scoped and priced individually. Your account contact can prepare a tailored quotation for your business.

Ready for 24x7 managed cyber defence?

A fixed-fee managed detection and response service for endpoint, email, identity and Microsoft 365 threat monitoring. Talk to us about bringing Your Secure Defend into your business.

- Endpoint protection, predictive DNS security and ransomware protection
- Email security and business email compromise defence
- Microsoft 365 threat monitoring and identity threat detection
- Threat hunting, SIEM-style monitoring and 24x7 security operations
- Monthly reporting and incident response coordination

Get in touch

Your IT Department Ltd

Unit 8, Farrington Way, Eastwood,
Nottingham, NG16 3BF

T: 0115 822 0200

E: info@your-itdepartment.co.uk

W: your-itdepartment.co.uk