→ Datasheet

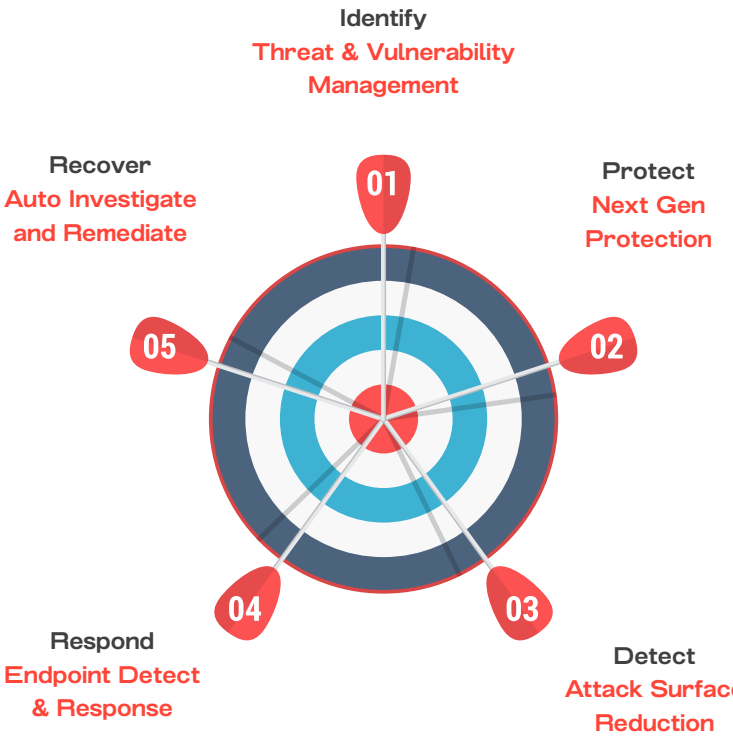
# EDR as a Service

Turn on the highest level of protection for your endpoints with 24x7 coverage

## Are you confident in your endpoint security?

From cybercriminals to ideologues and those involved in corporate espionage, the drivers often come down to money, power and publicity. Alongside desire to inflict operational and reputational damage. From the smallest SMB to the largest enterprise, organisations security strategies are being tested every single day and this can be stressful.

Ultima's Endpoint Detection and Response (EDR) service can significantly enhance visibility of attacks that are targeting endpoint devices, including up-to-the-minute threat intelligence to identify dangers that other controls can simply miss. With access to two different flavours, our service provides increasing levels of ownership and accountability, covering everything from monitoring, alerting and mitigation, comprehensive reporting, and advanced threat hunting.




**Find out more about EDR**

## Why Ultima for EDR?

Rapidly stop attacks, by delivering endpoint security across Windows, macOS, Linux, Android, iOS, and network devices.

**Threat & Vulnerability Management**
Uncover vulnerabilities & misconfigurations in near real time, and prioritize responses based on threat landscape and detections

**Attack Surface Reduction** - Rules target certain software behaviours, e.g. launching executable files and script, and running obfuscated or otherwise suspicious scripts

**Next Gen Protection** - Behaviour-based, heuristic and real-time AV and cloud-delivered protection, including near-instant detection and blocking of emerging threats

**Endpoint Detection & Response** - Analysts can effectively prioritize alerts, gain visibility into the full scope of a breach, and swiftly respond to threats to your organization

**Auto Investigations and Remediation**
Examine alerts and take immediate action to resolve breaches, significantly reducing alert volume, freeing up security teams

**Threat Experts** - Provides your Security Operation Centres with expert level monitoring and analysis to ensure that critical threats don't get missed

Ultima

# Service Plans

| Description | Advanced | Ultimate |
|---|---|---|
| Monitoring, Alerting & Mitigation - Anti Virus, Malware & Potentially Unwanted Apps | ✓ | ✓ |
| Inventory - Sensor health state and on-boarding status | ✓ | ✓ |
| Runbooks - Malware and Potentially Unwanted Apps (PUA) | ✓ | ✓ |
| Initial Review - EDR configuration | ✓ | ✓ |
| Reporting - Incident trends, secure score and vulnerabilities | Monthly | Monthly |
| Major Incident Management - P1 via Ultima's EDR | - | ✓ |
| Managed Vendor Support | ✓ | ✓ |
| Scheduled Scans - Setup and manage | Optional | Optional |
| Review - Software risk and weaknesses | Quarterly | Quarterly |
| Review - EDR configuration and recommendations | Yearly | Quarterly |
| Prevent EDR client traffic to known malicious content [1] | ✓ | ✓ |
| Review and Alert - Secure Score Reporting | - | Quarterly |
| EDR Health Check Reporting | - | Annual |
| Advanced Threat Hunting [2] | - | 1 day / Quarter |
| On demand device checking or user time line | - | ✓ |

[1] Can be turned on but additions, amendments or deletions to filtering rules, policies will need access to other Office 365 products

[2] This will be carried out when there is information of cyber incidents elsewhere or as a result of a separate advisory service



Ultima

Gainsborough House,
Manor Park, Basingstoke Road,
Reading, Berkshire,
RG2 0NA, UK

T: 0333 015 8000
E: enquiries@ultima.com
W: ultima.com