IRONSHARE
CYBER SECURITY SIMPLIFIED

Ironshare Endpoint Security With Cisco Secure Endpoint

SERVICE DEFINITION

SERVICE OVERVIEW

Ironshare provides Cisco Secure Endpoint licensing and/or fully managed endpoint security services to help organisations protect laptops, desktops, and servers against malware, ransomware, and advanced cyber threats. As a Cisco MSP partner, we deliver simplified licensing alongside expert implementation, monitoring, and ongoing operational management.

Cisco Secure Endpoint (formerly Cisco AMP for Endpoints) delivers cloud-managed endpoint detection and response (EDR), combining behavioural analytics, machine learning, and Cisco Talos global threat intelligence. Ironshare enhances this capability by providing continuous oversight, tuning, and expert-led response support, enabling customers to improve protection while reducing internal operational burden.

This service is suitable for organisations operating in cloud, hybrid, and on-premises environments and supports Windows, macOS, Linux, and mobile platforms.

Product Overview – Cisco Secure Endpoint
Cisco Secure Endpoint provides advanced protection throughout the attack lifecycle, including prevention, detection, investigation, and response. The platform delivers deep visibility into endpoint activity and correlates telemetry with global threat intelligence from Cisco Talos.

Key capabilities include behavioural analysis, retrospective detection, endpoint isolation, threat hunting, and integration with the wider Cisco security ecosystem, including Cisco XDR. Secure Endpoint enables organisations to identify threats quickly, investigate incidents effectively, and reduce dwell time across endpoint environments.

Service Description
Ironshare supplies Cisco Secure Endpoint licences and delivers a fully managed service covering the complete lifecycle of endpoint protection. Our service includes onboarding, agent deployment, policy configuration, alert monitoring, investigation, tuning, and ongoing optimisation.

We work closely with customers to ensure Secure Endpoint is configured in line with organisational risk appetite, regulatory requirements, and industry best practice. Our engineers continuously review alerts and endpoint activity, providing triage, investigation, and actionable recommendations to improve security posture and reduce false positives.

The service is delivered remotely as standard, with optional onsite support available by agreement. Customers benefit from centralised management, expert operational support, and simplified licensing, without the need to maintain in-house specialist expertise.

IRONSHARE SERVICES

Our services provide flexible options to support your solution deployment and ongoing operations:

- **Cloud licensing and subscription support** – light touch assistance with renewals, licence optimisation, and ongoing adjustments. (No managed service).

- **Professional services** – expert guidance on deployment, configuration, and best-practice implementation.

- **Fully managed service** – end-to-end operational management of your Duo environment.

Our qualified engineers offer specialist advice and clearly define the activities required to design, implement, and support your cloud-managed service.

Ironshare can also deliver comprehensive remote managed services for your Security solution, including:

- Full or partial managed service options
- Deployment and configuration aligned to vendor and industry best practice
- Policy management and optimisation
- Alerting, triage, and reporting on security events
- Integration with wider security services

ABOUT CISCO SECURE ENDPOINT

Key Features and Benefits

Cisco Secure Endpoint provides the following features and customer benefits:

1. **Advanced Malware Protection**
   Detects known and unknown threats using behavioural analysis, machine learning, and reputation-based intelligence.
2. **Endpoint Detection & Response (EDR)**
   Provides deep visibility into endpoint activity to support rapid detection and investigation of suspicious behaviour.
3. **Ransomware Protection**
   Identifies and blocks malicious encryption and ransomware techniques before impact.
4. **Retrospective Security**
   Alerts when files previously considered safe are later identified as malicious.
5. **Threat Hunting Capabilities**
   Enables proactive identification of Indicators of Compromise (IOCs) across endpoints.
6. **Cloud-Delivered Intelligence**
   Lightweight agents continuously updated with real-time Cisco Talos threat intelligence.
7. **Centralised Management**
   Unified cloud console for managing policies, endpoints, and alerts across platforms.
8. **Cisco XDR Integration**
   Correlates endpoint data with other Cisco security tools to improve response and automation.
9. **Policy Configuration & Tuning**
   Optimised policies reduce false positives while maintaining strong protection.
10. **Improved Compliance & Risk Reduction**
    Strengthens endpoint security posture and supports regulatory and framework requirements.

Cisco Secure Endpoint Licensing Breakdown

Cisco Secure Endpoint is available in three primary licence tiers. Ironshare can advise on the most appropriate tier based on organisational size, risk profile, and security maturity.

Secure Endpoint Essentials

Entry-level endpoint protection focused on core threat prevention.

Key Capabilities:

- Malware detection and prevention
- Behavioural analysis
- Cisco Talos threat intelligence
- Cloud-based management console
- Basic alerting and reporting

Good for organisations requiring strong baseline endpoint protection without advanced investigation or response features.

Secure Endpoint Advantage

Enhanced endpoint security with investigation and response capabilities.

Includes all Essentials features, plus:

- Endpoint Detection & Response (EDR) visibility
- Device trajectory and file trajectory analysis
- Threat hunting capabilities
- Endpoint isolation
- Enhanced reporting and investigation tools

Suited to organisations seeking deeper visibility into endpoint activity and improved incident response capabilities.

Secure Endpoint Premier

Advanced endpoint security with extended analytics and threat intelligence.

Includes all Advantage features, plus:

- Advanced malware analytics
- Extended threat intelligence and enrichment
- Cisco XDR orchestration and automation
- Advanced investigation workflows
- Greater reporting depth and retention

Best for security-mature organisations requiring advanced detection, response, and integration with a broader security operations platform.

Ironshare Managed Service Components

Ironshare's managed service for Cisco Secure Endpoint typically includes:

- Licence procurement and renewal management
- Agent deployment and onboarding support (with assistance from local IT teams)
- Policy creation, tuning, and optimisation
- Continuous monitoring of endpoint alerts
- Alert triage and investigation
- Incident escalation and response guidance
- Monthly or periodic reporting
- Cisco XDR and security tool integration support
- Ongoing best-practice recommendations

Managed services may be delivered as fully managed or co-managed, depending on customer preference.

Service Constraints

- Service availability is dependent on Cisco Secure Endpoint cloud services.
- Feature availability varies by licence tier.
- Customer environments using unsupported or end-of-life operating systems may have limited functionality.
- Intrusive remediation actions require customer approval.
- Onsite services or complex integrations may incur additional charges.

ABOUT IRONSHARE

We are an IT Security Consultancy based in the Midlands. Our expertise in this area allows us to deliver proven, tried and tested results to our customers, and as a flexible business, we can be agile to our customer needs, while remaining commercially attractive in the market.

In addition to the board of directors, our team consists of analysts, administrative staff, and regional consultants from around the UK. These consultants can be called upon at any time during our customer engagements, to scale up or down our available resources, as and when required.

Our main business is in the provision of Security Consulting services to customer organisations for security health checks and assessments, project design and delivery of secure solutions, investigations, incident response, or training. We also cover Managed Security services, security policy documentation, risk analysis, secure build hardening and technical standards, and offer a retainer service which means companies get specialist knowledge without having to have expensive experts on the payroll.

CISCO PARTNERS

Ironshare are a registered Cisco Select partner, that have been certified in the Security Specialisation. We do however have experience across the technology sector and will assess every situation on its own merits. This means that we make recommendations to your business based on what is best for you and may offer third-party solutions from other recognised leaders in the industry.

COMPANY DETAILS

Ironshare Ltd
22 The Tything
Worcester
WR1 1HD
Company number: 10107127
VAT registration number: 238 7520 90

WEBSITE

www.ironshare.co.uk

CONTACT DETAILS FOR ENQUIRIES ABOUT THIS AGREEMENT

Email: information@ironshare.co.uk
Phone: 0121 769 0475

+44 (0) 121 769 0475
www.ironshare.co.uk
information@ironshare.co.uk

Reg Comp No: 10107127
Reg Comp Address: The Colmore Building, 20 Colmore Circus, Birmingham, B4 6AT, UK