Quorum Cyber

Service Description
Clarity Extend
G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview

Background

Public sector organisations increasingly rely on native, Microsoft security products to protect sensitive data and maintain compliance. However, the evolving threat landscape (ransomware, phishing, and advanced persistent threats) combined with the rapid adoption of cloud services and remote work, has made 24/7 security monitoring and incident response critical.

Many organisations lack the in-house expertise and resources to provide continuous monitoring, proactive threat detection, and rapid incident response. This gap leaves them vulnerable to breaches, financial loss, reputational damage, and regulatory penalties.

Quorum Cyber's Solution

Clarity Extend is an annual managed detection service delivered by Quorum Cyber to its customers.

It is the core of our catalogue of fully managed threat detection and response subscription services, providing unlimited cybersecurity coverage and protection for our customers by utilising the following features:

- Near real-time, proactive security event analysis
- Response and containment of incidents
- Remediation guidance
- Identify anomalies and suspicious behaviour

Clarity Extend is delivered 24 hours a day, 7 days a week, 365 days a year, and integrates the current market leading technology, behavioural analytics, proprietary algorithms and rules, global threat intelligence, and a team of certified security analysts.

Powered by Microsoft Sentinel, Quorum Cyber has partnered with Microsoft to deliver an all-inclusive managed cyber security incident Detection and Response service that enables rapid time-to-value in a simple subscription model.

Our service is designed to address the critical mission of reducing cyber security risk, proactively detecting, and responding to cyber-attacks.

Differentiators

Our main differentiator is that you only pay for the number of users in your environment. Therefore, if you have 1000 users, 1000 endpoints and 50 servers, you pay for 1000 users. There are no additional costs, caps or charges for monitoring data sources other than user increases.

Unlike many providers, Quorum Cyber go beyond alerting: we Respond. Following NIST incident response guidelines, we take containment actions such as isolating compromised devices and disabling affected user accounts—ensuring threats are neutralized before they escalate.

Our in-house platform **Clarity** provides a single pane of glass for real-time visibility into alerts, investigations, and service performance. No more static reports. Clarity is your operational dashboard and service review in one, enabling secure collaboration, rapid incident tracking, and actionable insights from anywhere.

Our Security Operations Centre (SOC) and all service delivery teams are fully UK-based, operating from Edinburgh, Scotland. This ensures compliance with UK data sovereignty requirements and provides customers with confidence that their data remains within UK jurisdiction.

Being UK-based also means faster response times, alignment with UK public sector standards, and a deep understanding of local regulatory frameworks such as GDPR and NCSC guidelines. Our proximity and cultural alignment enable seamless communication and collaboration with UK organizations.

Service Features

Microsoft Sentinel

The technological foundation of the service is the use of Microsoft Sentinel, a scalable, cloud-native SecOps platform, delivering security information event management (SIEM), security orchestration automated response (SOAR), threat intelligence, behavioural analytics, and threat hunting capabilities.

Microsoft Sentinel delivers cloud-based security event ingestion, intelligent security analytics and threat intelligence across an enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Detection and Hunting

Powered by a comprehensive collection of processes and procedures, our technology platform enables our people to deliver advanced capabilities at scale across the globe, including:

- 24/7/365 Managed SOC. Theat detection and response
- Incident response included with all Managed Services (Up to & including containment of the incident)
- Rapid onboarding
- Full coverage from any source both Microsoft security tools and third-party technologies
- Quorum Cyber's full analytic library
- Quorum Cyber's in-house curated Threat Intelligence feeds
- Named service delivery team with Monthly service reviews
- Health and cost monitoring (Maximising Microsoft licensing and ingestion)
- Automated Threat hunting (Utilising our in-house, premium and Microsoft threat intel feeds)
- Delivered within your tenancy, so no data has to leave.

Our teams constantly improve the service based on the latest threat intelligence, ensuring the platform proactively detects new threats across all industries, enriching the ecosystem with every ticket and incident we respond to, delivering real and continued service improvements.

Service Benefits

Our threat-centric approach enables us to deliver a service that is tailored to your most critical risks, while our teams of professionals leverage cutting-edge Microsoft Security technologies to protect your business everywhere, regardless of your approach. The service will monitor security logs and alerts from Microsoft native cloud security tooling such as Entra ID, M365, Defender XDR and Defender for Cloud.

- Effectively and efficiently reduce cyber risk for a fraction of the cost of building internal teams and capabilities.
- Reduce burden on your teams, reduce noise, and respond to incidents faster than ever.
- Easily meet compliance and regulatory obligations, with a service delivered entirely in your Microsoft Azure tenancy.
- Simple subscription based on the number of people we protect, ensuring you only pay for what you use, and avoiding large up-front investments in licences and technology. We also advise on the most cost-effective use of Microsoft Sentinel – focusing on threat led ingestion of data to ensure you maximise detection but minimise cost.
- Enhanced security alert coverage allowing for a more thorough analysis of security events.
- Full cost management.
- Frequent service reviews.
- Human-driven Structured Threat Hunting.