Quorum Cyber

Service Description
Clarity Protect
G Cloud 15

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

Table of Contents

Service Overview

Background

As the threat landscape continues to increase in complexity and sophistication, attackers continue to mature their playbooks and evolve their tactics, techniques, and procedures. The technology landscape has also drastically changed in recent years, with the move to Cloud, meaning you can no longer draw security perimeters using network lines.

This means we need a different approach to security. The traditional 'best of breed' approach, over time, has led to many organisations having a varied technology stack, with tools that do not fully integrate with each other, which has resulted in gaps in visibility and control and high costs.

At Quorum Cyber, we believe that a consolidated technology stack such as Microsoft Defender XDR combined with Microsoft Sentinel and other Azure capabilities such as Entra ID Protection, provides considerably advanced protection across your estate, whether they are on-premises, cloud, or hybrid.

To unleash the full power of the tooling and make it work for you, it requires constant maintenance and evolution of the configurations, from attack surface reduction rules, to tuning detections, to implementing enhanced security controls. Combining human intelligence, automations, analysis of trends in your environment and expert security engineering, we constantly evolve your Microsoft Defender XDR products to ensure you are protected.

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 Protect provides 24x7 detection and response and delivers a fully managed Microsoft Defender ecosystem (Microsoft Defender XDR), along with Microsoft Entra ID Protection, focused on continuous optimisation of your protections and controls, providing comprehensive security across your whole IT estate. Attacks are blocked earlier, attacker dwell time is reduced, and your security teams are freed up to concentrate on your core business rather than ongoing product management.

Our solution focuses on business results and outcomes, driving forward operational resilience, while reducing the total cost of ownership (TCO) to give you a clear return on investment (ROI), regardless of the size, complexity, and geographical footprint of your business.

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.

Microsoft Defender XDR

We deliver the service via regular daily, weekly, monthly and quarterly checks, and drawing input from our Threat Intelligence, Incident Response and SOC teams to inform ongoing security posture improvement:

- **Ongoing control optimisation:** As threats, technology and your estate changes, controls also need to change to provide the best protection possible. We review control efficacy in line with your risks, current alert trends, critical threats, industry guidance/benchmarks and compliance requirements on a continuous basis.
- **Attack Surface Reduction (ASR)**: Defender for Endpoint rules drastically reduce the risk of an attack being successful. Through a refined baseline set of controls, we maintain for all customers and custom rules focused on your threats and estate, we ensure these are giving you the best protection, regularly evolving these where needed.
- **Maintenance of custom rules:** We maintain IOCs and custom rules across the Defender products to ensure rapid and accurate blocks and detections, and alignment to business compliance (e.g., blocking of non-allowed

websites). We also maintain lists such as applications in Defender for Cloud Apps, protecting users from malicious applications.

- **Intelligent automations for immediate response:** Combining human intelligence and machine automation, we implement automated controls and response actions, such as Entra ID Protection to revoke suspicious user sessions, and automated investigations and blocks in Defender for Endpoint.
- **Enhanced protection and recovery support during incidents:** With Clarity Protect our teams can rapidly update Defender configurations to protect you during an incident (or urgent new vulnerability), on top of the containment and incident response support offered as part of the detection service.
- **Microsoft Secure Score:** Our service includes providing recommendations, and where related to Defender, implementing mitigations, relating to vulnerabilities on your endpoints covered by MDE, with the goal of reducing your exposure.
- **Streamlined tuning of detections:** Our XDR and SOC analyst teams work in parallel to constantly learn, refine and tune your detections across Microsoft Sentinel and the Defender XDR. This increases detection efficiency and reduces burden on your response teams – allowing them to focus where is needed.
- **Keep pace with the threats:** We are constantly reviewing your trends, new Defender features, and understanding your business and IT strategies to identify security improvements for your business.
- **Service health monitoring:** We ensure that all portals, devices, agents are working correctly and reporting in.

All changes and recommendations are captured in our Clarity portal, providing full visibility, change control and tracking in real-time, and allowing you to approve, reject, or ask questions about changes.

Service Benefits

The following **benefits** are recognised by managing the Microsoft Defender XDR product set for you – ensuring optimised controls and protections alongside detection:

- **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.**
- **Human-driven Structured Threat Hunting.**
- **Always Optimised Security Posture –** reducing the probability and impact of a security incident with an always optimised solution that keeps pace with the threats and your business needs.
- **Reduce the Total Cost of Security (TCO) –** unifying security controls under the Microsoft ecosystem, we reduce overall spend in licensing and management overheads – customers have seen a >30% TCO reduction.
- **Increase Effectiveness of Security Teams –** enable your teams to focus where it matters, rather than making products work. Strong controls and well-tuned alerts also mean your teams focus on only the important incidents, not false positives.
- **Operational Efficiency and Resilience –** visibility, orchestration and automation capabilities enable the organisation to thrive even when under attack; and rapidly recover from attacks.
- **Reduce Attacker Dwell Time** – by maintaining complete threat visibility and strong controls across all dimensions of your organisation, including identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.
- **Understand your Risk Profile and Where to Focus Improvements** – the Microsoft Defender XDR solution provides unique insights into your risks based on activity and alert trends, controls, and current security posture – enabling you to understand your risks and report to board.
- **Peace of Mind –** Rest easy and lean on our team of certified Microsoft and Security experts, combining the creative human talent of a team of security experts and threat hunters, with the power of Microsoft technology.