Quorum Cyber

Service Description Phishing Protection G Cloud 15

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

Table of Contents

Service Overview

Background

Our Phishing Protection Service is aimed at defending organisations against phishing attacks.

Phishing attacks are designed to exploit human trust and bypass defences. From mass scams to targeted spear-phishing, they're one of the biggest cyber risks, leading to email compromise, ransomware, data loss, and reputational damage. Training is valuable, but relying on employees to judge email safety isn't enough. That's where expert analysis and specialised tools come in, providing a layer of defence to spot and stop phishing far better than human judgement alone.

Phishing is the easiest way for attackers to steal credentials and breach networks. Once inside, they can quickly exfiltrate data, disrupt operations, and compromise systems. Stopping phishing at the outset is vital to securing your organisation.

Our Phishing Protection fills the critical gap left by traditional defences, quickly detecting and responding to sophisticated AI-driven attacks. Suspicious emails reported by users are analysed instantly through advanced AI

Your users get clear updates on whether their reported emails are safe, suspicious, or malicious. Meanwhile, your security team get expert insights and detailed findings, enabling smarter decisions to quickly remove threats and block attacks, keeping your organisation safe. Transparent Reporting and Rapid Response expert human review, powered by real-time threat intelligence and escalated directly to our SOC. This seamless blend of tech and human insight cuts through noise, eliminating guesswork enabling swift, accurate responses to stop phishing attacks at their source.

Quorum Cyber's Solution

Our service is designed to enable users to report suspicious emails as soon as they feel something is off, giving them a perfect solution that provides consistent quality, and a simple call to action to put their training into use.

The service provides additional coverage (beyond our Clarity MDR services) for potentially malicious emails received by end users, by giving them a quick and effective way to submit them to Quorum Cyber's Security Operations Centre (SOC) team for review. The service provides critical protection against one of the most common initial access tactics, phishing, allowing you to rapidly prevent and purge, block and respond to any activity following a phishing email.

Our phishing service will analyse emails reported by users. Users will receive an update (via email) once their email has been analysed, which will categorise it as benign, suspicious, or malicious. Your security teams can login to the Clarity portal and review comments added by our analyst which will detail investigation steps, findings, and reasoning for the classification. In combination with our Clarity Managed Detection & Response services, Quorum Cyber can also take containment actions such as purging emails and blocking senders.

The phishing service is also used to identify and escalate phishing campaigns directly to security teams, either via a Clarity Incident ticket and/or an email from their Service Delivery Manager.

Differentiators

We are passionate about cyber security, and we're obsessed with helping you achieve your goals. Everything we do is geared towards helping you win. We are Microsoft experts – we are a proud Microsoft Solutions Partner for Security and a member of the Microsoft Intelligent Security Association (MISA). We work with multiple security frameworks and standards and are constantly developing and evolving our knowledge across our teams.

Our main differentiator is that you only pay for the number of users in your environment. Therefore, if you have 1000 users and 1000 endpoints, 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

Our Phishing Protection Service provides UK Business Hours phishing email analysis delivered by a specialist team of cyber security professionals based in the United Kingdom. Notifications are sent to end users on the classification of the email; and deeper insights provided to your Security team on the phishing emails and campaigns. We provide recommendations for your Security and IT teams to rapidly respond to any threats, blocking malicious URLs and emails for example. Real-time service insights are delivered by our Clarity platform and provide a unique service experience that enable deep integration between your teams, and our people, ensuring great collaboration and knowledge transfer.

The service includes:

- Automatic and manual analysis of user reported emails
- Sandboxing of payloads
- Malware and exploit detection
- Operational Threat Intelligence integration
- Deep entity analysis (sender, receivers, links, attachments, language, sentiment, etc.).
- Containment and eradication actions
- User reports
- Trend reports

Service Benefits

- Reduced TCO and burden on security teams
- Reduce likelihood and impact of phishing attacks
- Increase employee satisfaction, enabling them to safely report concerns and offload the responsibility of ”getting it right every time”
- Increase organisational satisfaction with security, delivering a great customer experience that enables better response times and business outcomes
- Enrich context of other Quorum Cyber Clarity managed detection and response services
- Simple subscription model based upon number of users