# Data Loss Prevention Managed Service

Quorum Cyber

**Our Data Loss Prevention (DLP) service provides the design and deployment of DLP policies. This stage defines the tuning, severity, and priority for the business with regards to the exfiltration and oversharing of sensitive information.**

Our Data Loss Prevention (DLP) service provides the design and deployment of DLP policies. This stage defines the tuning, severity, and priority for the business with regards to the exfiltration and oversharing of sensitive information.

Once this is in place, Quorum Cyber will onboard your tenant into the Security Operations Centre (SOC) for the set-up of DLP signals into Sentinel and provide oversight into Quorum Cyber's Clarity solution.

The aim of this service is to provide a comprehensive solution that will help prevent data loss and protect the customer's data to meet regulatory and compliance requirements such as GDPR and financial data regulations across Microsoft 365 Exchange/SharePoint services and endpoints such as Windows 10/11/macOS.

## Design/Deploy

Our team will work with your business to define DLP policies such as GDPR/financial regulations. However, the initial packaged offering will include:

- GDPR information—Personally Identifiable Information (PII)
- Financial information—data related to credit card or bank numbers
- Custom—identified by the customer. Examples include data types, classification, and boundaries.

These policies will help identify and prevent sensitive data from leaving the organisation.

Our team will take into consideration the different types of data, such as PII and financial data, and work with the business to define the severity and priority of each policy.

info@quorumcyber.com

0333 444 0041

quorumcyber.com

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner

Security

Specialist
Cloud Security
Threat Protection

Quorum Cyber

## Tuning

Quorum Cyber will tune the DLP policies to ensure that the number of alerts generated within a period of time is manageable. Our target is to keep the number of alerts to a maximum of 20 per month. This will help the business focus on the critical alerts that require immediate attention.

Alerts over this cadence will be at additional cost in reference to the current managed service taken with Quorum Cyber.

The signals for DLP can derive from the Microsoft 365 services, such as Email (Exchange Online) and sharing out of the platform (SharePoint Online, OneDrive for business). If the customers are set up with Quorum Cyber's Managed Extended Detection & Response (XDR) service, these signals can also come from the endpoint for common exfiltration activities.

## Severity

Our team will assist the customer in defining the severity of each DLP alert, although it will be the priority that is set by each individual customer. This enrichment of the alerts will help the SOC team triage the alerts, so they are dealt with accordingly and the correct prioritisation given to the response.

Critical alerts are dealt with promptly in accordance with the SOC team's SLAs, while less critical alerts can be addressed later through weekly digests.

## Ingesting DLP alerts into Sentinel

Our team will ensure that DLP alerts are ingested into Microsoft Sentinel (Microsoft's cloud-native Security Information and Event Management (SIEM) solution). These details are fed into Quorum Cyber's Clarity solution as a single pane of glass for our customers to consume incidents through dashboards, reports, and triaged alerts.

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

## Solutions:

### Solution 1: Minimum Viable Product (MVP)

We will provide a weekly digest that summarises the DLP alerts generated during the previous week. This will help the business stay informed of any potential data loss incidents and allow them to take necessary actions. The insights will provide further discussions on how DLP can be tuned for the mitigation of risk via Quorum Cyber's professional services.

### Solution 2: Full-service DLP

The full-service solution will provide extra signals to the SOC team, which will help identify any potential issues with the DLP policies and provide remediation and tuning. This will allow us to refine the policies and reduce the number of false positives generated.

The SOC team will provide detailed information on each DLP alert generated, including who triggered the alert, what action/activity was taken, and why it was blocked.

All evidence and event correlation will be collected, and a full report created. Quorum Cyber will notify the customer through pre-defined playbooks to discuss the findings and provide clear recommendations on the next escalation steps. Such steps could be defined as account lockout or notification to management escalation. All these triage and notification steps will be created and documented as part of the managed service and after reviews have taken place with agreed SLAs.

**The full service will provide two types of outcomes:**

- The first is automation back to the customer, which will allow the business to bypass the SOC for less critical alerts.
- The second will allow the SOC team to investigate critical alerts and take necessary actions to prevent data loss.

## Conclusion:

Our managed DLP service provides a comprehensive solution that will help prevent the loss and exfiltration of sensitive data. Quorum Cyber will work with the business to define DLP policies that are aligned to their business, while ensuring the policies work through testing and tuning, and help define the severity and priority of each policy.

As a minimum, we will also provide a weekly digest so our customers can clearly see what's happening with their data across their Microsoft solutions and be able to provide an advanced, full-service offering that enhances DLP alerts through a managed SOC process, direct feedback to the business, and DLP incident response services.

Our service relies on the automation and logic within the platform that's customised to each customer's business needs.

# In Summary:

## What will you get?

- A managed DLP service
- Professional services for the design and deployment of DLP policies
- On-boarding into the SOC
- Set-up of DLP signals into Sentinel
- Oversight into Quorum Cyber's Clarity solution
- Weekly digest summarising DLP alerts generated during the previous week
- Detailed information on each DLP alert generated, including who triggered the alert, what action/activity was taken, and why it was blocked
- Automation back to the customer for less critical alerts
- SOC team investigation for critical alerts
- Clear recommendations on the next escalation steps

## What technologies will you use?

- Microsoft 365 Exchange/SharePoint Online services
- Endpoints such as Windows 10/11/macOS
- Microsoft Sentinel (Microsoft's cloud-native Security Information and Event Management (SIEM) solution)
- Quorum Cyber's Clarity solution

## What will you get as part of the service?

- Initial professional services for the design and deployment of DLP policies
- Definition of GDPR/financial information policies, and custom policies identified by the customer
- Tuning of DLP policies to ensure a manageable number of alerts
- Assistance in defining the severity of each DLP alert
- Automation back to the customer for less critical alerts
- SOC team investigation for critical alerts
- Detailed information on each DLP alert generated, including who triggered the alert, what action/activity was taken, and why it was blocked
- Weekly digest summarising DLP alerts generated during the previous week
- Clear recommendations on the next escalation steps
- Review meetings with agreed SLAs

info@quorumcyber.com

0333 444 0041

quorumcyber.com

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner

Security

Specialist

Cloud Security

Threat Protection