

CYRISMA DATA SHEET

Cyber risk reduction through data-centric security analysis. A simplified approach with complementary risk management functions under a single application framework. Cloud based SaaS (Software as a Service) provides easy implementation and universal secure accessibility.

RISK MANAGEMENT FUNCTIONS

- Sensitive Data Discovery
- Vulnerability Scanning & Patching
- External Web App Scanning
- Configuration Hardening
- Active Directory Review
- Dark Web Monitoring
- Mitigation and Remediation Action

OVERALL RISK MANAGEMENT

- Compare progress of current & past scans
- Visible risk trend analysis and Scorecards
- Host risk matrix assessment
- Cyber Risk Assessment report and presentation
- Track compliance (HIPAA, PCI DSS, SOC 2, NIST CSF, CIS Controls V8, ACSC Essential Eight, UK Cyber Essentials)
- Compare cybersecurity performance against others in the same industry

VULNERABILITY MANAGEMENT

- Agent/Agentless based host
- Windows/Linux/macOS/Network Devices
- Email alerts and notifications
- Detailed CVE results
- Root cause analysis
- Vulnerability lookup and research
- Progressive scan compare
- Remediation action plan assistance
- Patch Management - 3rd Party Apps
- Vulnerability First Seen

SENSITIVE DATA DISCOVERY

- Endpoint support (Agent and Agent-less options)
- Windows/Linux/macOS
- Network Attached Storage/File Shares
- Local Office 365 Sync Scanning
- Cloud Office 365 Scanning (Exchange, OneDrive, SharePoint, and Team shares)
- Google Workspace (Google Drive, Docs, Sheets, Gmail)

Native File Format Summary

- Open-source Office Suites
- Open document standards
- File databases
- Compressed archives
- ASCII text files of unknown types

Sensitive Data Categories

- All PCI DSS payment types
- Financial data, routing, swift, IBAN
- National IDs, SSN and many other countries
- Personal Info; names, address, phone, DOB
- Driver's license and passports
- Custom data patterns of unlimited variety

OS CONFIGURATION HARDENING

- Windows/Linux/macOS
- Email alerts and notifications
- Direct tie to CIS/DISA configuration protocols
- Baseline standards lookup and research
- Compare progress over time
- Remediation action plan assistance

ACTIVE DIRECTORY MONITORING

- Monitor type - Azure AD & On-prem AD
- Domain Information - DCs , Domain Mode
- User Information - Active vs Disabled
- Last log on
- Password last changed
- Group Information - Group Types , User Group Membership

MICROSOFT SECURE SCORE

- Track your progress to secure your Microsoft cloud environment
- View recommendations to enhance your security posture

RISK MITIGATION PLANS

- Automatically generate action plans from results
- Monitor plan progress
- Assign plans to departments with accountability
- Remediation actions Include:
 - Secure delete of sensitive data
 - Encrypt sensitive data
 - Move sensitive data
 - Mask specific data within a file
 - Remove specific access rights

MICROSOFT COPILOT READINESS ASSESSMENT

- Ensure your Microsoft Copilot deployments align with security standards
- Manage and secure the data accessed and generated by Copilot
- Generate Copilot Readiness Reports

RISK ASSESSMENT REPORTING

- Generate easy-to-understand overall and category-specific risk assessment and scan reports

DARK WEB MONITORING

- Monitoring of Domains, IPs and email IDs in Breach Data (Compromised Accounts) & Forums (Ransomware /Marketplaces etc.)

RESTful API (Provisioning/Reporting)

- Provision instances
- Assign users
- Installation keys
- Scan data
- Dashboard information

PSA Integrations

- ConnectWise PSA
- AutoTask PSA

