



# DATA SHEET

## CYRISMA DATA SHEET & SPECIFICATIONS

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

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

### OVERALL RISK MANAGEMENT

- Compare progress of current and past scans
- Visible risk trend analysis and Score Cards
- Host risk matrix assessment
- Cyber Risk Assessments report and presentation
- Track progress against compliance standards
  - HIPPA    PCI DSS
  - NIST CSF    CIS Controls v8

### DATA DISCOVERY

- End point 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

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

#### Discovery Types

- 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

### 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

### 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

- Domain Information
  - DC's                  Domain Mode
- User Information
  - Active                  Disabled
  - Last logon              Password last changed
- Group Information
  - Group Types          User Group Membership

### DARK WEB MONITORING

- Continuous Monitoring for Domain/IP Info in
  - Breach Data (Compromised Accounts)
  - Forums (Ransomware/Market Places etc.)

### 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

