CyberRes

Product Map

Micro Focus products span the Continuous Diagnostics and Mitigation (CDM) spectrum more broadly and completely than any other single company in the world.

Micro Focus has delivered trusted and proven mission-critical software for the Federal government for more than 40 years, with more than 200 Federal agencies currently using our products.

See product details on reverse side.

		What is on the network? (Phase 1)	Who is on the network? (Phase 2)	What is happening on the network? (Phase 3)	How is data protected? (Phase 4)	
NetIQ Identity & Access Management	Data Access Governance				✓	↗
	eDirectory		✓			↗
	Identity Governance		✓			↗
	Identity Manager		✓			↗
	Access Manager		✓	✓		↗
	Advanced Authentication		✓		✓	↗
	Risk Service			✓		↗
	Privileged Account Manager		✓	✓		↗
	Directory & Resource Administrator		✓			↗
	Group Policy Administrator		✓			↗
	Sentinel			✓		↗
	Change Guardian			✓		↗
	AD Bridge	✓	✓			↗
	Universal Policy Administrator	✓	✓			↗
	Secure Configuration Manager	✓				↗
Voltage Data Protection	Voltage SmartCipher				✓	↗
	Voltage SecureData Enterprise				✓	↗
	File Analysis Suite (FAS)				✓	↗
	Content Manager				✓	↗
	Structured Data Manager (SDM)				✓	↗
	SecureMail					↗
Fortify Application Security	Fortify Static Code Analyzer			✓		↗
	Fortify Software Security Center			✓		↗
	Application Defender			✓		↗
	Fortify WebInspect			✓		↗
	Fortify on Demand			✓		↗
	Fortify Audit Assist			✓		
ArcSight Security Operations	ArcSight Enterprise Security Manager			✓		↗
	ArcSight Logger			✓		↗
	ArcSight Recon			✓		↗
	ArcSight SOAR			✓		↗
	ArcSight Intelligence			✓		↗

MFGS INC
Micro Focus Government Solutions Master Supplier

About Us

We are committed to serving your agency or organization leveraging Micro Focus' best in class portfolio of enterprise-grade scalable software solutions to solve mission-critical IT challenges.

www.mfgsinc.com/cyberres

CyberRes, a Micro Focus line of business

NetIQ

Identity & Access Management

Data Access Governance

- Controls access to data stored in the network file system according to identity and role
- Automates access assignments and remediation, prevents unauthorized access, mitigates risk
- Helps to meet attestation for unstructured data access compliance
- Governance, reporting, and analysis of access to file systems and unstructured data

eDirectory

- A full-service, secure LDAP directory providing incredible scalability and an agile platform.
- Provides a fast, reliable, secure, Open Standards based high-end identity store.
- Bundled with NetIQ Identity Manager and NetIQ Access Managers.

Identity Governance

- Real-time adaptive governance enables continuous risk reduction.
- Supports cloud, on-premises, and hybrid environments.
- Supports business-based role and attribute models.
- Define controls to detect and handle violations and exceptions.
- Supports access certifications.
- Integrations with ServiceNow, Remedy, and others.

Identity Manager

- Manages the complete identity lifecycle in a modular and integrated architecture across the enterprise.

Access Manager

- Out-of-the-box integration with Microsoft SharePoint and Office 365 Enterprise.
- Software development kit for iOS devices.
- Built-in, risk-based authentication engine that provides risk scoring and selective authentication based on score.
- Centralized policy engine for role-based access enforcement.
- Built-in mobile gateway for users on smartphones (iOS and Android) who need access to legacy applications.
- Access authorization, single sign-on, and personalization through a built-in access gateway.

Advanced Authentication

- Supports geo-fencing, 2-factor skipping, offline support, emergency password, non-domain clients, and all major application integration standards.

Risk Service

- Enables your organization to evolve from static authentication and access to an adaptive environment, using behavioral profiling and artificial intelligence.

Privileged Account Manager

- Enterprise Credential Vault for secured password vaulting.
- Database privileged account monitoring for users, tools, and applications.
- Risk-based session control to enable automatic session termination or access revocation.
- Remote session establishment and control for operating systems.
- Risk profiling that quickly identifies high-risk users.
- Smart risk ratings built on potential threat analysis.

Directory & Resource Administrator

- Multi-domain and forest management
- Less expensive Azure AD administration
- Microsoft AD bridging
- Multi-factor authentication
- ActiveView delegation model
- Privilege escalation prevention
- REST-based API support
- Non-repudiated auditing

Group Policy Administrator

- Granular delegation of least privilege separates duties among stakeholders.
- Compare and merge GPOs to maintain a clean and consistent GPO repository.
- Integrated Group Policy Change Monitoring.
- Live and offline Resultant Set of Policy (RSoP) analysis.
- Point-in-time analysis reports show changes with who/what/when detail.
- GPO version control with check-out, check-in.
- One-button rollback capability.
- WMI filter and GPO Link Order editing.

Sentinel

- Virtual software appliance packaging allows for fast and easy deployment.
- Unlike hardware-based options, virtual appliances can easily expand to handle growth and additional capacity.
- Identity enrichment provides rich context to security events, providing greater insight for detecting and preventing insider-based threats.
- Simplified administration with graphical rule building interfaces and capacity planning.
- Administrators can develop correlation rules quickly during implementation and easily maintain and update them as business needs change, providing a lower total cost of ownership.

Change Guardian

- Provides immediate visibility to unauthorized changes that could lead to a breach, enabling the fastest threat response.
- Identifies and reports on changes to critical files, platforms, and systems to help prevent breaches and ensure policy compliance.
- Real-time intelligent alerting provides immediate visibility to unauthorized changes that could lead to a breach, enabling the fastest threat response.

AD Bridge

- Extend Active Directory control to Linux.
- Take control of Linux-based VMs.
- Single IAM vendor coverage and visibility across your hybrid environment.
- Extend processes and policies to cloud-based Linux resources.
- Reduced risk of human error with native firewall services and settings in IPTables.
- Unrivaled privilege granularity with our ActiveView model.

Universal Policy Administrator

- Policy Consolidation: Improve ROI by centrally managing existing platform investments by extending your privilege, delegation, and policy management toolsets to all managed resources.
- Device Management: Increase efficiency by centrally managing resources within a single pane of glass and a single identity.
- Compliance Requirements: reduce risk by implementing consistent security controls and auditing capabilities across your entire environment.
- Allow policy administrators to manage their respective devices without having to hand over control to other administrators.
- Extensive out-of-the-box reports for RSOP analysis and conflict analysis to help alleviate the complexities of determining policy order.

Secure Configuration Manager

- Agent or agentless operating system, database, and application assessments.
- “Grade”-based risk scoring provides reliable metrics for tracking progress against known best practice configurations.
- Security Content Automation Protocol (SCAP) validation to ensure that your compliance assessment solution is in compliance with federal requirements.
- Integration with IT GRC solutions using the UCF interchange.

Voltage

Data Protection

Voltage SmartCipher

- Simplifies unstructured data management by embedding files with access and use controls that persist across the data lifecycle.
- Increases visibility and control over sensitive file access, use, and disposition with centralized policy control.
- Reduces risk of a data breach by encrypting and wrapping security policy that travels with files to protect them wherever they go.
- Improves compliance audit and inquiry response with real-time discovery, classification, monitoring, and reporting on files for sensitive data usage and creation.
- Accelerates hybrid IT adoption by enabling secure collaboration across platforms with no changes to applications or OS.
- Expands privacy and security with SecureMail integration by encrypting and inspecting email content and attachments with SmartCipher policies.
- Granular delegation of least privilege separates duties among stakeholders.
- Complete offline group policy lifecycle management and analysis.
- Cross-domain/cross-forest group policy management and reporting.
- Compare and merge GPOs to maintain a clean and consistent GPO repository.
- Integrated Group Policy Change Monitoring.
- One-button rollback capability.
- Point-in-time analysis reports show changes with who/what/when detail.
- Change Guardian for Group Policy integration.
- Built-in exception management capabilities to manage information security risks associated with known exceptions.
- Security Content Automation Protocol (SCAP) validation to ensure that your compliance assessment solution is in compliance with federal requirements.

Voltage SecureData Enterprise

- Data encryption at the application level, achieving encryption at rest, in transit, and in use using Format Preserving Encryption (FPE).
- FIPS 140-2 and Common Criteria validated solution; sensitive data is protected with NIST-Standard FF1 AES encryption, pioneered by Micro Focus.
- Flexible range of interface including REST, simple APIs, gateway, and native for easier integration with a broad range of databases, applications, and platforms.
- Hyper SST—Next generation high performance tokenization.

File Analysis Suite (FAS)

- Automatically scan, index, and optimize data—enabling data reduction, migration, minimization, application retirement, and ROT management.
- Identification of sensitive data, assessment of access rights privileges, and detection of risk-sensitive data and anomalies—providing deep content and metadata analysis, reporting, auto-classification, policy development, and controls.
- Detailed data analytics, providing analysis of all organizational data from a centralized dashboard interface view to address complex data privacy regulations. In addition, identify key data insights that protect the business and identify complex risk scenarios. With ability to connect to and monitor the most common sources of personal and sensitive data.
- Data governance and IT Modernization providing data mapping, discovery, tagging, trained machine-learning based classification, with active and passive remediation of data.
- Utilize policy-based scanning to identify data, manage data-in-place, preserve high-value data in a secure long-term repository and quickly respond to internal and external information requests

Content Manager

- Classifies content and records automatically, based on detailed categories. It uses a manage-in-place framework to apply holds to content in external repositories, eliminating the need to migrate it to a central repository.
- Automated rules, classification, and workflow capabilities facilitate the easy capture, management, and lifecycle management of your business content from creation to disposal—improving staff efficiency, security, and enterprise performance. Control the management and legal disposition of data to meet global, national, and state privacy regulations.
- Can be configured to automatically create containers or folders for newly added information as part of your governance-based enterprise content management process. This can be done based on pre-defined criteria, such as the creation date, specific metadata, or the person or group who created the information.
- Enables you to apply security, retention, and disposition policies automatically to enterprise content and records to help you mitigate risk and support compliance initiatives.

Structured Data Manager (SDM)

- Out-of-the-box discovery of sensitive data such as social security numbers, credit card data, client names, etc.
- End-to-end data privacy protection to sensitive data by leveraging hyper Format Preserving Encryption (FPE), protecting data over its entire lifecycle—from the point at which it is captured and throughout its movement across the extended enterprise, without gaps in protection.
- Lower TCO: Reduce your data footprint and storage costs, including hardware, maintenance, and administration.
- Comply with data privacy laws: Delete relevant data and protect or mask sensitive information to meet privacy regulations.
- Simultaneous access to production and archived data using combined reporting; a single query can run without changes, using standard application screens or reports.

SecureMail

- Ensure internal and external email encryption from the originator to the intended recipient with this complete email security solution.
- SecureMail enables decryption on desktop, web, and mobile for internal and external users via its scanning and filtering capabilities.
- SecureMail adds end-to-end email encryption to Office 365, flexible deployment options, and additional compliance and collaboration features.
- SecureMail secures sensitive data contained in internal emails, on company-issued equipment, and on mobile devices to ensure email security.
- Business users can initiate secure messages with the click of a button—no need for recipients to download software to read them.

Fortify

Application Security

Fortify Static Code Analyzer

- Integrated Development Environments (IDE): Eclipse, Visual Studio, JetBrains (including IntelliJ)
- CI/CD Tools: Jenkins, Bamboo, Visual Studio, Gradle, Make, Azure DevOps, GitHub, GitLab,
- Maven, MSBuild
- Issue Trackers: Bugzilla, Jira, ALM Octan
- Open Source Security Management: Sonatype, Snyk, WhiteSource, BlackDuck
- Code Repositories: GitHub, Bitbucket
- Swaggerized API for unlimited customization

Fortify Software Security Center

- Automate security in the CI/CD pipeline with Swagger-supported RESTful APIs, GitHub repo, and plugins for Bamboo, VSTS, and Jenkins.
- Leverage all major IDEs: Eclipse, Visual Studio, IntelliJ IDEA.
- Integrate with defect management tools and cover security issues caused by open source components with software component analysis tools integration.

Application Defender

- Consistent and systematic logging of application activity without editing code or recompiling.
- Real-time protection from known and unknown vulnerabilities with the click of a button.
- Flexible event output in industry-standard formats for visualization, analysis, and alerting in any SIEM or log management solution.
- Event details with fully reconstructed attack strings and line-of-code details for efficient triage and remediation.
- Configurable alerting and reporting for risk prioritization and communication across the organization.
- Mature, proven runtime application self-protection (RASP) technology.
- When you perform security testing with Fortify on Demand, many of the vulnerabilities can be protected seamlessly with the click of a button without leaving FoD.

Fortify WebInspect

- Manage enterprise application security risk.
- Monitor trends and take action on vulnerabilities within an application.
- Save time with automation and integrations.
- Integrates with the Software Development Life Cycle (SDLC) without additional overhead.
- Pre-configured policies and reports for all major compliance regulations related to web application security, including PCI DSS, DISA STIG, NIST 800-53, ISO 27K, OWASP, and HIPPAA.
- Optimize Scan Results with Agent Technology.
- Get additional visibility and stack trace insight from scanned web applications; optimize the scanning process for both speed and accuracy.
- Start quickly and scale as needed on premises, as a service, or as a hybrid; OpenSSL preview.
- Solution to SCHANNEL lockdown issues.
- OpenSSL Preview provides a simple solution for environments where SSL is being restricted either by registry or group policy.

Fortify on Demand

- Supports 27+ languages: ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic ASP (with VBScript), COBOL, ColdFusion CFML, GoLang, HTML, Java (including Android), JavaScript/ AJAX/Node.js, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic, and XML
- Microservice licensing model for modern application development
- Real-time vulnerability identification with Security Assistant
- Actionable results in <1 hour for most applications with DevOps automation

Fortify Audit Assist

- Predict the exploitability of raw findings with 97% average accuracy. Audit Assistant amplifies the SAST return on investment by reducing the number of issues needing deep manual examination, identifying relevant issues and removing false positives sooner, and scaling application security with existing resources.

ArcSight

Security Operations

ArcSight Enterprise Security Manager

- Real-time correlation, real-time threat detection
- Scenario and playbook automation can be customized to efficiently address your SOC’s unique needs
- Collaborative incident response for faster reaction and increased efficiency
- Customizable case management of incident fields, severity, classification, and UI
- 110+ integration plugins from 70+ vendors for centralized investigation and response, without needing to move between tools

ArcSight Logger

- Comprehensive data collection
- Flexible deployment architecture
- Secure and reliable
- Ultra-fast search and investigation
- Non-stop compliance
- Easy to deploy and manage
- Machine-learning data science content

ArcSight Recon

- Comprehensive data collection
- Flexible deployment architecture
- Secure and reliable
- Search and investigation tools
- Efficient threat hunting
- Machine-learning data science content

ArcSight SOAR

- Robotic Process Automation for Cyber: Eliminate repetitive activities to focus on what matters most.
- Collaborative Defense: Investigate and respond collaboratively, engage and involve everyone in the organization.
- Central Command and Control for SecOps: Single pane of glass for security operations.
- Measure and Govern Security Operations: Collect and measure all SecOps activities.

ArcSight Intelligence

- Unsupervised machine learning models
- Baseline behavior for each entity
- Detection of anomalous behavior
- View threats in context of peers and history
- Behavioral analytics for coding environments
- Distill billions of events into a prioritized threat list

Learn more about CyberRes products and solutions at **cyberres.com**

Learn more about MFGS, Inc. and our full line of solutions at **www.mfgsinc.com**

CyberRes

MFGS INC
Micro Focus Government Solutions Master Supplier