The purpose of the Continuous Diagnostics and Mitigation (CDM) Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities.

The Tools/CMaaS BPA Product Catalog lists the tools and sensors cross-referenced to a list of key attributes for CDM Phases 1 and 2 security products. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer’s websites.

Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.

The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement. All product categorizations, descriptions and web links have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.
Bit9 Parity Suite

**Overview:**

Bit9 Parity is the recognized leader in Whitelisting. Whitelisting is the ability to control file execution based upon a list of approved file names or file types. This approach is superior to traditional application control solutions because it is based on allowing only approved applications to run on your devices, rather than blocking everything else.

Bit9’s policy-driven approach to application control combines a powerful visibility and application discovery agent with trust and access control policies via Bit9’s proprietary User Interface System (UIS). This allows administrators to easily create, deploy, and manage policies across thousands of endpoints. At the core of Bit9 Parity Whitelisting are robust white lists that are continually updated and vetted by Bit9’s Threat Intelligence Cloud to help organizations greatly simplify and automate the set-up and ongoing management of their whitelisted environment.

**Key Features:**

- **Intelligent Application Whitelists:** Bit9 Parity Whitelists are used to control the execution of applications that run on endpoints.
- **Intelligent User Role Whitelists:** Bit9 Parity defines only a small number of roles that are used to control what applications can be run by standard users.
- **Intelligent System Whitelists:** By applying intelligent system whitelists, you can control the operation of the operating system itself, ensuring that only essential applications are installed and used.
- **Intelligent Application Whitelists with Advanced Security:** Bit9 Parity provides advanced security features such as file integrity monitoring, zero-day attack detection, and malware protection.

**Technical Details:**

- **White-listing:** Bit9 Parity uses a policy-based control approach to application control. By defining a list of approved applications and setting permissions for users, Bit9 Parity limits what applications can run on an endpoint.
- **Access Control:** Bit9 Parity defines user roles with specific permissions, ensuring that only authorized individuals can access sensitive information.
- **System Whitelists:** Bit9 Parity allows administrators to control the operation of the operating system itself, ensuring that only essential applications are installed and used.

**Benefits:**

- **Simplified Management:** Bit9 Parity simplifies the management of endpoints by allowing administrators to easily create, deploy, and manage policies across thousands of endpoints.
- **Improved Security:** By using whitelisting, Bit9 Parity reduces the risk of malware infections and ensures that only approved applications are run on endpoints.
- **Enhanced Productivity:** Bit9 Parity allows standard users to work efficiently with standard user accounts, while admin users are given full access to all system resources.

**Website:**

BMC Server Suite is a comprehensive solution that provides automated access control, privilege management, and audit capabilities for Windows, Linux, and UNIX systems. It is designed to improve business efficiency, security, and compliance by automating identity-related controls across physical, virtual, and cloud environments.

**Key Features**

- **Privilege Management**: Centrify Server Suite automates the management of user privileges, reducing the risk of unauthorized access and ensuring regulatory compliance.
- **Identity Consolidation**: Integrates with Active Directory and other directory services, consolidating user identities to reduce the attack surface.
- **Audit and Reporting**: Provides detailed reports and dashboards to help organizations comply with regulatory requirements.
- **Centralized Administration**: Enables administrators to manage user access and privileges from a single console.
- **Integration**: Seamless integration with existing IT infrastructure, including virtualization, cloud, and other security solutions.
- **Self-Service**: Supports self-service password reset and password management for users.

**Use Cases**

- **Identity Access Management**: Centrify Server Suite helps organizations manage user access and privileges, comply with regulatory requirements, and reduce security risks.
- **Privilege Management**: Automates the management of user privileges, reducing the risk of unauthorized access.
- **Audit and Compliance**: Centrify Server Suite provides detailed audit trails and reports to help organizations comply with regulatory requirements.

**Manufacturer's Link to More Information**

- [Centrify Server Suite](https://www.centrify.com/products/server-suite/)
- [CA Technologies Identity Management and Governance](http://www.ca.com/us/products/identity-management.aspx)
- [BMC Server Automation](http://www.bmc.com/it-solutions/bladelogic-server-automation.html)
- [BMC Atrium CMDB](http://www.bmc.com/it-solutions/atrium-cmdb.html)

*All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.*
Dell Core Insight is an enterprise-wide solution that consolidates and prioritizes vulnerabilities, identifies and eliminates attack vectors, and reduces the amount of time an organization needs to respond to a breach. It includes capabilities that help organizations to:

- Identify and prioritize vulnerabilities
- Detect and eliminate attack vectors
- Reduce the amount of time needed to respond to a breach

The Core Insight solution is delivered by Dell Security, and it is designed to work seamlessly with other security solutions to provide a comprehensive approach to security management. For more information, visit the Dell Security website at [http://software.dell.com/products/identity-manager/](http://software.dell.com/products/identity-manager/).

---

Dell Core Insight

**Product Family:** Dell Core Insight

**Manufacturer's Product Description:** A comprehensive, customizable platform providing real-time protection, including real-time protection for websites, web applications, and email. It includes capabilities that help organizations to:

- Detect and respond to suspicious activity in real-time
- Protect against a wide range of threats, including malware, viruses, and web-based attacks
- Reduce the amount of time needed to respond to a breach

The Core Insight solution is delivered by Dell Security, and it is designed to work seamlessly with other security solutions to provide a comprehensive approach to security management. For more information, visit the Dell Security website at [http://software.dell.com/products/identity-manager/](http://software.dell.com/products/identity-manager/).

---

CyberArk Privileged Account Security

**Product Family:** CyberArk Privileged Account Security

**Manufacturer's Product Description:** CyberArk Privileged Account Security is based on CyberArk Shared Technology Platform, which combines an isolated vault server, a unified policy engine, and a discovery engine to provide scalability, reliability and enhanced security for privileged accounts.

For more information, visit the CyberArk website at [http://www.cyberark.com/](http://www.cyberark.com/).

---

Damballa Failsafe

**Product Family:** Damballa Failsafe

**Manufacturer's Product Description:** Damballa Failsafe is a solution for detecting and terminating persistent threats and targeted attacks in enterprise networks. Damballa Failsafe tracks files in real-time, and identifies behaviors that indicate the presence of malicious content. For more information, visit the Damballa website at [https://www.damballa.com/products-solutions/damballa-failsafe/](https://www.damballa.com/products-solutions/damballa-failsafe/).

---

Cisco Systems Inc

**Product Family:** Cisco Prime Infrastructure

**Manufacturer's Product Description:** Cisco Prime Infrastructure provides a comprehensive solution for managing and maintaining access control policies in large-scale environments. It integrates with other Cisco security solutions to provide a complete security solution for your organization.


---

Dell Dell Asset Manager

**Product Family:** Dell Asset Manager

**Manufacturer's Product Description:** The Dell Asset Manager is a solution for managing software and hardware assets. Through a single console, it allows users to discover and track asset movements and access agreements, and provide detailed reporting on all key configuration, user and administrator changes for Active Directory, ADLDS, AD Queries, Exchange, and SQL Server. Change Auditor also tracks detailed user activity for web storage and services, logon and authentication activity on the desktop, and detailed user activity for external system activity. For more information, visit the Dell website at [http://software.dell.com/products/change-auditor/](http://software.dell.com/products/change-auditor/).

---

CyberArk CyberArk Shared Technology Platform

**Product Family:** CyberArk Shared Technology Platform

**Manufacturer's Product Description:** CyberArk CyberArk Shared Technology Platform is a powerful, modular technology platform that provides the industry's most comprehensive Privileged Account Security Solution. Each product can be managed independently or combined for a cohesive and complete solution for managing privileged access. For more information, visit the CyberArk website at [http://www.cyberark.com/](http://www.cyberark.com/).

---

Dell Dell One QuickConnect

**Product Family:** Dell One QuickConnect

**Manufacturer's Product Description:** Dell One QuickConnect is a solution that allows organizations to automate the process of identity data synchronization between different systems and to ensure that users have access to the right systems and data. It provides a unified solution for managing access control across different systems, including software, hardware, and cloud-based environments. For more information, visit the Dell website at [http://www.dell.com/products/quickconnect](http://www.dell.com/products/quickconnect).

---

CyberArk CyberArk Privileged Account Security Solution

**Product Family:** CyberArk Privileged Account Security Solution

**Manufacturer's Product Description:** CyberArk is the trusted expert in privileged account security. Designed from the ground up with a focus on security, CyberArk has developed a powerful, modular technology platform that provides the industry's most comprehensive Privileged Account Security Solution. Each product can be managed independently or combined for a cohesive and complete solution for managing privileged access. For more information, visit the CyberArk website at [http://www.cyberark.com/](http://www.cyberark.com/).

---

Dell Dell One Cloud Access Manager

**Product Family:** Dell One Cloud Access Manager

**Manufacturer's Product Description:** Dell One Cloud Access Manager is a solution that allows organizations to automate the process of identity data synchronization between different systems and to ensure that users have access to the right systems and data. It provides a unified solution for managing access control across different systems, including software, hardware, and cloud-based environments. For more information, visit the Dell website at [http://www.dell.com/products/quickconnect](http://www.dell.com/products/quickconnect).

---

Dell Dell One Identity Manager

**Product Family:** Dell One Identity Manager

**Manufacturer's Product Description:** Dell One Identity Manager is a solution that allows organizations to automate the process of identity data synchronization between different systems and to ensure that users have access to the right systems and data. It provides a unified solution for managing access control across different systems, including software, hardware, and cloud-based environments. For more information, visit the Dell website at [http://www.dell.com/products/quickconnect](http://www.dell.com/products/quickconnect).

---

Dell Dell One Identity Manager

**Product Family:** Dell One Identity Manager

**Manufacturer's Product Description:** Dell One Identity Manager is a solution that allows organizations to automate the process of identity data synchronization between different systems and to ensure that users have access to the right systems and data. It provides a unified solution for managing access control across different systems, including software, hardware, and cloud-based environments. For more information, visit the Dell website at [http://www.dell.com/products/quickconnect](http://www.dell.com/products/quickconnect).
<table>
<thead>
<tr>
<th>CDM PHASE 1</th>
<th>CDM PHASE 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manufacturer's Product Description</strong></td>
<td><strong>Manufacturer's link to more information</strong></td>
</tr>
<tr>
<td><strong>Firewall-Packet AcuityLight</strong></td>
<td><a href="http://software.dell.com/products/privileged-access-suite-for-unix/">http://software.dell.com/products/privileged-access-suite-for-unix/</a></td>
</tr>
</tbody>
</table>

**CDM Product Family**

<table>
<thead>
<tr>
<th>Hewlett-Packard</th>
<th>CSM</th>
<th>VUL</th>
<th>TRUST</th>
<th>DEBUG</th>
<th>CRED</th>
<th>PRIV</th>
</tr>
</thead>
</table>

**The HP Atalla X** is a solution that consolidates and validates data, license, license, and license 005:3. It provides enhanced reporting, allowing you to access your security management and data validation services under a certified seal. The HP Atalla X solution ensures visibility and access enabled operation of access rights and identities across your entire data ecosystem.

**The CESM** is a solution that delivers out-of-the-box, real-time federation with CESM Universal Configuration Management Database. This integration results in one of the few systems to automate the entire IT Service Management process without requiring a monolithic repository. Federation reduces data redundancy and improves transaction performance—so that relevant data resides within its respective business domain, yet is available across the business infrastructure. In addition, preserving business productivity.

**The FireMon Firemon ES Appliance** is purpose-built, ready-to-deploy Security Manager implementations tailored to fit directly into a specific customer environment. Whether you're monitoring 100 devices or 1,000, or conducting analysis in the same environment over time, the FireMon family of appliances has all the power and wrong analysis necessary to meet security manager's performance standards and the archival needs of your organization.

**eIQ SecureVue** is a platform that provides continuous security monitoring and mitigation for all IT environments. eIQ capabilities include:

- **Audit Log Management & SIEM**
- **Compliance Management & Reporting**
- **Risk Management Framework (RMF) Compliance**
- **Continuous STIG & USGCB Compliance Monitoring**
- **Audit Log Management & SIEM**

**ForeScout CounterACT** is a platform that provides continuous security monitoring and mitigation for all IT environments. ForeScout capabilities include:

- **Cyber Analytics**
- **STIG Assessments for IT Auditors**
- **Risk Management Framework (RMF) Compliance**
- **Continuous STIG & USGCB Compliance Monitoring**
- **Audit Log Management & SIEM**

**Firewall-Packet AcuityLight** is a platform that provides continuous security monitoring and mitigation for all IT environments. AcuityLight capabilities include:

- **Audit Log Management & SIEM**
- **Compliance Management & Reporting**
- **Risk Management Framework (RMF) Compliance**
- **Continuous STIG & USGCB Compliance Monitoring**
- **Audit Log Management & SIEM**

**Firewall-Packet Asset Manager Enterprise Suite** is a platform that provides continuous security monitoring and mitigation for all IT environments. Asset Manager capabilities include:

- **Risk Management Framework (RMF) Compliance**
- **Continuous STIG & USGCB Compliance Monitoring**
- **Audit Log Management & SIEM**

**Firewall-Packet Malia** is a platform that provides continuous security monitoring and mitigation for all IT environments. Malia capabilities include:

- **Risk Management Framework (RMF) Compliance**
- **Continuous STIG & USGCB Compliance Monitoring**
- **Audit Log Management & SIEM**

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.
IBM Security Access Manager provides automated and policy-based user lifecycle management and access control. It enables organizations to store, manage, and control access privileges and access rights throughout the user lifecycle. IBM Security Access Manager supports user registration, user authentication, and role-based access control. It allows organizations to easily configure and manage access policies and access rights. IBM Security Access Manager is available as a stand-alone solution or as a component of IBM Security Identity and Access Manager.<br>
<br>IBM Cognos Business Intelligence provides capabilities designed to provide: secure, automated and policy-based user lifecycle management and access control. It supports various access management models, such as role-based access control and attribute-based access control. It allows organizations to easily configure and manage access policies and access rights. IBM Cognos Business Intelligence is available as a stand-alone solution or as a component of IBM Cognos platform.<br>
<br>IBM Security Access Manager for DataPower provides flexible and policy-based access management for mobile and cloud environments. It supports various access management models, such as role-based access control and attribute-based access control. It allows organizations to easily configure and manage access policies and access rights. IBM Security Access Manager for DataPower is available as a stand-alone solution or as a component of IBM DataPower Gateway.<br>
<br>IBM Security Access Manager for Mobile provides flexible and policy-based access management for mobile environments. It supports various access management models, such as role-based access control and attribute-based access control. It allows organizations to easily configure and manage access policies and access rights. IBM Security Access Manager for Mobile is available as a stand-alone solution or as a component of IBM Security Identity and Access Manager.<br>
<br>IBM Security Access Manager for Web provides flexible and policy-based access management for web environments. It supports various access management models, such as role-based access control and attribute-based access control. It allows organizations to easily configure and manage access policies and access rights. IBM Security Access Manager for Web is available as a stand-alone solution or as a component of IBM Security Identity and Access Manager.<br>
<br>IBM Security Identity and Access Manager provides flexible and policy-based access management for web environments. It supports various access management models, such as role-based access control and attribute-based access control. It allows organizations to easily configure and manage access policies and access rights. IBM Security Identity and Access Manager is available as a stand-alone solution or as a component of IBM Security Identity and Access Manager.
IBM

Infor

- **Infosphere**
  - X
  - X
  - X
  - X
  - X
  - X
  - X
  - X
  - X

Manufacturer's Product Description

- The Infosphere Platform provides the foundational building blocks of trusted data, including data integration, data master, master data management, applications, and information governance. The platform provides an enterprise scale foundation for information integration projects, providing the performance, scalability, reliability and automation needed to simplify, standardize and deliver trusted information to your business future.

Manufacturer's link to more information

http://www-01.ibm.com/software/data/infosphere/

IBM

Qradar Incident Forensics

- X
- X
- X
- X
- X
- X
- X
- X
- X

The IBM Security Incident Forensics allows you to narrow down the time window to a specific area of a potential attack, and quickly and accurately view the image of the malicious activity. By analyzing the integrity and forensics of suspected malicious network security incidents, it reduces the time it takes security teams to determine if a threat is present and also reduces the time it takes to remove malware. In many cases from data loss to new malware reuse, scans often use inaccurate feeds.

IBM

Qradar SIEM

- X
- X
- X
- X
- X
- X
- X
- X

The IBM Security Qradar SIEM consolidates log event received from thousands of on-premise and cloud applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to discover and detect threat forms faster. As an option, this software enhances IBM Security QRadar Threat Intelligence by supplying a pool of potentially malicious IP addresses including inbounds, outbound and unknown. IBM Security QRadar can also correlate new system events with content, data and files, furthering the insider security monitoring.

IBM

Qradar Vulnerability Manager

- X
- X
- X
- X
- X
- X
- X
- X

The IBM Security Qradar Vulnerability Manager provides comprehensive network detection and appliance security by subcategory, with content and reports on the presence of vulnerabilities and threat activity. It is fully compliant with the IBM Security Qradar Threat Intelligence Platform and enhances the results of threat schedule and dynamic vulnerability scans with relevant asset information, security information. New data, log and most-malicious IP intelligence to manage vulnerabilities and ensure compliance. IBM Security Qradar Vulnerability Manager helps automate updated alerting for addressing security exposure. Utilizing advanced data correlation, the solution brings a vulnerability information to task security teams gain the visibility they need to act on more events. IBM Security Qradar Vulnerability Manager provides the performance, scalability, reliability and automation needed to simplify, standardize and deliver trusted information to your business future.

IBM

Security Identity Manager for Role Management

- X

- The IBM Security Identity Manager is a comprehensive, policy based identity and access management solution with the management capabilities that help automate the provision of managing and tailoring of user rights across the extended enterprise.

IBM

Security Key Lifecycle Manager

- X
- X
- X

- The IBM Security Key Lifecycle Manager is a comprehensive, policy based identity and access management solution with the management capabilities that help automate the provision of managing and tailoring of user rights across the extended enterprise.

IBM

Tivoli Federated Identity Manager

- X
- X
- X
- X

- The IBM Security Identity Manager is a comprehensive, policy based identity and access management solution with the management capabilities that help automate the provision of managing and tailoring of user rights across the extended enterprise.

IBM

Tivoli Security Policy Manager

- X
- X

- The IBM Security Identity Manager is a comprehensive, policy based identity and access management solution with the management capabilities that help automate the provision of managing and tailoring of user rights across the extended enterprise.

Itron

GroupID

- X
- X
- X
- X

- Itron's GroupID is a comprehensive solution that manages the entire identity lifecycle for enterprise environments. GroupID offers a simple approach for managing user access to corporate resources.

Infobase

Infor Approve

- X
- X
- X
- X
- X
- X
- X

- Infor Approve is an industry leading solution that enables you to manage, delegate and control access to your critical business applications, resources, and data. It simplifies the end user experience, delivering more efficient and effective processes with less risk.

Infobase

Infor HCM

- X
- X

- Infor HCM is a comprehensive solution that aligns talent management with corporate strategy. Integrated modules address hiring, on-boarding, training, talent and career development, performance management, and succession planning. This next generation talent management system helps organizations attract, retain, and develop talent by making it easy to align talent management with your company’s strategy.
All product categorizations, descriptions, and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

**Infor**
Infor Technology


**Informatica**
ActivEOS


**Informatica**
Informatica Master Data Management (MDM)


**Informatica**
Informatica PowerCenter


**Informatica**
Informatica PowerExchange


**Informatica**
Informatica VBE Data Novum


**Interra Billing (CGS Inovate)**
Intress Security Orchestrator (ISD)


**LogRhythm**
LogRhythm SIEM

All product categorizations, descriptions and web links have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

- **McAfee Vulnerability Manager Product Family**: Conducts deep scans of web applications to ensure security vulnerabilities are found.
- **McAfee SIEM Product Family**: Integrates with third-party solutions, providing actionable threat intelligence.
- **McAfee HIPS Product Family**: Monitors and controls system behavior, helping prevent malicious activity.
- **McAfee ePO Product Family**: Provides centralized management of security policies and data, including vulnerabilities.
- **McAfee Application Control Product Family**: Blocks unauthorized executables, protecting systems from threats.
- **Lumeta Corporation IPsonar Product**: Identifies and monitors network devices, enhancing security posture.
- **Lumeta Corporation ESI Product**: Offers real-time monitoring of network conditions.

For more information, please visit the following links:
- [McAfee Vulnerability Manager](http://www.mcafee.com/us/products/vulnerability-manager.aspx)
- [McAfee SIEM](http://www.mcafee.com/us/products/siem.aspx)
- [McAfee HIPS](http://www.mcafee.com/us/products/hips.aspx)
- [McAfee ePO](http://www.mcafee.com/us/products/epolicy-orchestrator.aspx)
- [McAfee Application Control](http://www.mcafee.com/us/products/application-control.aspx)
- [Lumeta IPsonar](http://www.lumeta.com/products/esi/)

---

**Microsoft System Center**: Integrates with Microsoft Cloud OS to provide unified security management.

- [Microsoft System Center](http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/)

---

**All product descriptions are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.**
Oracle

Access Management Suite

Oracle Identity and Access Management Suite is a comprehensive, fully integrated identity and access management solution. It provides a unified approach to managing identities, access, and entitlements, ensuring secure and efficient access to applications and data. Oracle Identity and Access Management Suite helps organizations:

- Manage identities for users, devices, and applications
- Provide single sign-on (SSO) for secure and seamless access
- Enforce strong password policies
- Manage access based on role, location, and time
- Protect data using encryption and tokenization
- Comply with privacy and regulatory requirements

Oracle Identity and Access Management Suite is available in a software-only option or as a hosted service. It can be deployed on-premises or in the cloud, allowing organizations to choose the deployment model that best fits their needs.

Oracle Advanced Security

Oracle Advanced Security is a comprehensive suite of security solutions designed to protect enterprise data and applications. It includes:

- Oracle Database Advanced Security
- Oracle WebLogic Advanced Security
- Oracle Application Security
- Oracle Web Services Security

Oracle Advanced Security provides a unified approach to securing data at rest and in transit, as well as securing applications and services. It includes features such as:

- Encryption: Encrypt data to protect it from unauthorized access.
- Tokenization: Mask sensitive data to protect it from exposure.
- Access Control: Control access to data and applications based on roles, attributes, and policies.
- Auditing: Monitor security events and ensure compliance with regulatory requirements.

Oracle Data Integrator Enterprise Edition

Oracle Data Integrator Enterprise Edition is a powerful data integration platform that enables organizations to connect data across disparate sources, ensuring that data is consistently available to business applications.

- Data Integration: Migrate, transform, and load data from various sources into your enterprise data warehouse.
- Data Quality: Ensure data quality by identifying and correcting data errors and inconsistencies.
- Data Governance: Manage data assets and ensure compliance with regulatory and corporate policies.

Oracle Identity Federation

Oracle Identity Federation is a complete, turnkey solution for federated single-sign-on (SSO) and identity management. It enables organizations to extend user identity and data to applications outside the firewall, providing secure and efficient access to these resources.

- Single Sign-On (SSO): Eliminate the need to remember multiple usernames and passwords.
- Identity Federation: Securely share identity information between applications.
- Authorization: Control access to resources based on user identity and attributes.

Oracle Identity Governance Suite

Oracle Identity Governance Suite provides a comprehensive solution for managing and governing identities, access, and entitlements. It includes:

- Identity Governance: Manage identities and attributes throughout the lifecycle.
- Access Governance: Enforce access policies and entitlements.
- Risk-based Access: Implement risk-based access control policies.

Oracle's award-winning identity management offerings are available as a comprehensive identity management suite. With Oracle Identity Governance Suite, organizations can:

- Streamline identity management processes
- Reduce security risks and compliance costs
- Enhance user experience and productivity

Oracle's identity management solutions are designed to be scalable and adaptable, ensuring that organizations can meet the changing needs of their businesses.
RadiantOne Cloud Federation Service is a solution that delegates the task of authenticating an organization's identity stores to

Oracle Identity Manager

Oracle Management Pack Plus for Identity Management

Oracle Mobile Security Suite

Oracle API Gateway

Oracle Audit Vault & Database Firewall

Oracle Business Intelligence Enterprise Edition

Oracle Database Enterprise Edition

Oracle Java Suite

Pentaho Pentaho Data Integration

Qlik Qlik Sense

KrollLogic Cloud Federation Service (CFS)
### Radiant Logic

**Identity Correlation & Synchronization Server (ICSS)**

Radiant Logic correlates and disambiguates correlates across access data silos, creating a single set of identities where duplicate user accounts are joined to create a global profile. The global profile provides a single representation for all users across multiple systems, instead of the underlying profiles.

With our powerful correlation technology, it’s easy to:

* Build application workflows for dealing with a heterogeneous environment. Identity information is often duplicated in multiple repositories. Source user profiles may also contain contradictory attribute scopes and values, or may be in a different format. It is essential that consuming applications get the same information, in the expected form.

With a flexible integration layer and a unique core, various source attributes need to be defined differently—now it’s easy to manage inter-tasking for the access control. They are not interconnected and not set for disambiguation within the system. Values with valid attributes. If multiple values for source attributes exist in different systems, ICSS can return a multi-valued attribute.

- Metadata is defined based on correlation source. Radiant Logic also returns attributes based on priority. This allows administrators to set procedures for attribute value sources, ensuring only required attribute data is available.


---

### Rapid7

**NEXPOSE**

RedSeal’s vulnerability management solution, Nexpose, helps you reduce your threat exposure by prioritizing risk across vulnerabilities, configurations, and controls with awareness of the real landscape across the modern network.

Data breaches are growing at an alarming rate. Your attack surface is constantly changing. The adversary is becoming more nimble than your security teams, and your board wants to know what you are doing about it. Nexpose gives you the confidence you need to understand your attack surface, focus on what matters, and reduce breach security events.


---

### Radiant Logic

**Virtual Directory Server (VDS)**

RadiantOne VDS is a sophisticated virtualization platform designed to address the complexity of today’s identity environments. It supports safe token forwarding options, each of which shares many of the advanced capabilities from its prior generation and is protected against users being directed out of context, or being locked into a context that is not aligned with the domain. RadiantOne VDS can federate attributes from multiple repositories. Same-user profiles may also contain contradictory attribute scopes and values, or may be in a different format. It is essential that consuming applications get the same information, in the expected form.

- Return attributes based on authoritative source: RadiantOne can also return attributes based on priority. This enables administrators to set procedures for attribute value sources, ensuring only required attribute data is available.

- Return multi-valued attributes: If multiple values for an attribute exist in different systems, VDS can return a multi-valued attribute.

- Disambiguate attributes and map to unique names: Often, same-named attributes need to be defined differently—now it’s easy to handle overlapping attributes. When dealing with a heterogeneous environment, identity information is often duplicated in multiple repositories. Source user profiles may also contain contradictory attribute scopes and values, or may be in a different format. It is essential that consuming applications get the same information, in the expected form.

- Handle overlapping attributes: When dealing with a heterogeneous environment, identity information is often duplicated in multiple repositories. Source user profiles may also contain contradictory attribute scopes and values, or may be in a different format. It is essential that consuming applications get the same information, in the expected form.

- Attribute-driven authorization and personalization, and real-time cache refresh.


---

### Rapid7

**METAPOSTUT**

Metadata, backed by a community of 1000+ users and contributors, gives you that insight. It is the kernel of RedSeal’s technology platform. You can access over 1000 security events and 175 distinct security events per host. RedSeal’s intelligent scanning examines device configurations, scanner data, vulnerability databases, and host information. It includes the virtual (Cloud-Native) SDN-based, SDN) parts of your network as well as the physical.

RedSeal then centralizes and integrates all of this information, first verifying that your network complies with industry best practices, then testing it to identify security risks. Most importantly, RedSeal prioritizes needed security actions—in the context of your network context of your network--and gives you the critical information you need to quickly remediate issues. And it does this context of your network--and gives you the critical information you need to quickly remediate issues. And it does this.

[https://redseal.co/content/product](https://redseal.co/content/product)

---
RES

RES Suite 2014

X X X

**CDM PHASE 1**

**CDM PHASE 2**

**Manufacturer's Product Description**

**Manufacturer's link to more information**

RES Archer Assessment and Authorization

X X X X X X X X

The RES Archer Assessment & Authorization (A&A) solution is a key foundation for a comprehensive RES Archer-based I Management suite. It ensures that all systems—both new and legacy—are brought into compliance. It is an organizational tool for the development of a comprehensive risk management and control framework that assists in the management of the entire lifecycle of an asset. The RES Archer Assessment and Authorization (A&A) solution empowers enterprises to make informed IT security and operations decisions.

**RES Archer Federal Continuous Monitoring**

X X X X X X

The RES Archer Continuous Monitoring (CM) solution provides excellent visibility into IT infrastructure and applications. It leverages existing threat intelligence to produce real-time and predictive insights into risks. It integrates with RES Archer Security Operations Management to provide a framework for customers building a security operations center (SOC). It leverages industry best practices to automate the monitoring of all IT assets and technology, while deploying appropriate security controls to help organizations prepare for and respond to cyber threats.

**RES Archer GRC Suite**

X X X

The RES Archer Governance, Risk, and Compliance (GRC) solution simplifies and streamlines the management of enterprise governance, risk, and compliance programs. The solution is designed to address the challenges of today’s enterprises, including increased regulatory scrutiny, the need to control complexity, the importance of collaboration across departments, and the need for agility in response to business and regulatory changes. The RES Archer GRC Platform integrates the best practices of GRC, including risk, compliance, asset management, and audit capabilities, to provide a comprehensive solution.

**RES Security Operations Management**

X X X X X X X X

RES Security Operations Management is a software solution that enables organizations to control the critical aspects of security and compliance. It helps organizations to streamline their risk management processes, automate tasks, and enforce policies. The platform provides comprehensive visibility into the security posture of the organization, enabling organizations to make informed decisions about their security posture and responding to security incidents.

**RES ONE**

X X X X X X

RES ONE provides organizations with a single, comprehensive platform for managing and monitoring their security posture. It allows for the integration of various security tools and systems into a single, unified environment. The solution provides organizations with comprehensive visibility into their security infrastructure, ensuring that they are fully aware of potential threats and vulnerabilities.

**RES Suite 2014**

X X X

RES Suite 2014 is a comprehensive platform designed for organizations to manage and monitor their security posture. It provides comprehensive visibility into the security infrastructure of the organization, allowing for the integration of various security tools and systems into a single, unified environment. The solution provides organizations with comprehensive visibility into their security posture, ensuring that they are fully aware of potential threats and vulnerabilities.

**RSA Archer**

**RSA Archer Assessment and Authorization**

X X X X X X

The RSA Archer Assessment & Authorization (A&A) solution is a key foundation for a comprehensive RSA Archer-based I Management suite. It ensures that all systems—both new and legacy—are brought into compliance. It is an organizational tool for the development of a comprehensive risk management and control framework that assists in the management of the entire lifecycle of an asset. The RSA Archer Assessment and Authorization (A&A) solution empowers enterprises to make informed IT security and operations decisions.

**RSA Archer Security Operations Management**

X X X X X X

RSA Archer Security Operations Management is a software solution that enables organizations to control the critical aspects of security and compliance. It helps organizations to streamline their risk management processes, automate tasks, and enforce policies. The platform provides comprehensive visibility into the security posture of the organization, enabling organizations to make informed decisions about their security posture and responding to security incidents.

**RSA Archer Vulnerability Risk Management**

X X X X X X

RSA Archer Vulnerability Risk Management provides a single application to help secure your infrastructure’s identity and data. The solution is designed to integrate with existing vulnerability management tools and processes, providing comprehensive visibility into the organization’s security posture. It helps organizations to identify and prioritize vulnerabilities, and take appropriate action to mitigate them.

**RSA IMG**

X X X X X X

The RSA IMG platform helps security organizations of any size or industry streamline various security and compliance activities. Its interface-driven, metadata-centric approach allows organizations to easily create and modify policies, workflows, and rules. The solution provides organizations with comprehensive visibility into their security posture, ensuring that they are fully aware of potential threats and vulnerabilities.

**RSA Security Operations Management**

X X X X X X

RSA Security Operations Management is a software solution that enables organizations to control the critical aspects of security and compliance. It helps organizations to streamline their risk management processes, automate tasks, and enforce policies. The platform provides comprehensive visibility into the security posture of the organization, enabling organizations to make informed decisions about their security posture and responding to security incidents.

**RSA Suite 2014**

X X X

RSA Suite 2014 is a comprehensive platform designed for organizations to manage and monitor their security posture. It provides comprehensive visibility into the security infrastructure of the organization, allowing for the integration of various security tools and systems into a single, unified environment. The solution provides organizations with comprehensive visibility into their security posture, ensuring that they are fully aware of potential threats and vulnerabilities.

**RSA Archer**

**RSA Archer Assessment and Authorization**

X X X X X X

The RSA Archer Assessment & Authorization (A&A) solution is a key foundation for a comprehensive RSA Archer-based I Management suite. It ensures that all systems—both new and legacy—are brought into compliance. It is an organizational tool for the development of a comprehensive risk management and control framework that assists in the management of the entire lifecycle of an asset. The RSA Archer Assessment and Authorization (A&A) solution empowers enterprises to make informed IT security and operations decisions.

**RSA Archer Security Operations Management**

X X X X X X

RSA Archer Security Operations Management is a software solution that enables organizations to control the critical aspects of security and compliance. It helps organizations to streamline their risk management processes, automate tasks, and enforce policies. The platform provides comprehensive visibility into the security posture of the organization, enabling organizations to make informed decisions about their security posture and responding to security incidents.

**RSA Archer Vulnerability Risk Management**

X X X X X X

RSA Archer Vulnerability Risk Management provides a single application to help secure your infrastructure’s identity and data. The solution is designed to integrate with existing vulnerability management tools and processes, providing comprehensive visibility into the organization’s security posture. It helps organizations to identify and prioritize vulnerabilities, and take appropriate action to mitigate them.

**RSA IMG**

X X X X X X

The RSA IMG platform helps security organizations of any size or industry streamline various security and compliance activities. Its interface-driven, metadata-centric approach allows organizations to easily create and modify policies, workflows, and rules. The solution provides organizations with comprehensive visibility into their security posture, ensuring that they are fully aware of potential threats and vulnerabilities.

**RSA Security Operations Management**

X X X X X X

RSA Security Operations Management is a software solution that enables organizations to control the critical aspects of security and compliance. It helps organizations to streamline their risk management processes, automate tasks, and enforce policies. The platform provides comprehensive visibility into the security posture of the organization, enabling organizations to make informed decisions about their security posture and responding to security incidents.

**RSA Suite 2014**

X X X

RSA Suite 2014 is a comprehensive platform designed for organizations to manage and monitor their security posture. It provides comprehensive visibility into the security infrastructure of the organization, allowing for the integration of various security tools and systems into a single, unified environment. The solution provides organizations with comprehensive visibility into their security posture, ensuring that they are fully aware of potential threats and vulnerabilities.
ServiceNow Implementation Services

ServiceNow CDM Product Family

<table>
<thead>
<tr>
<th>PHASE 1</th>
<th>PHASE 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

ServiceNow Implementation Services provide an implementation andConfiguration Services package that can assist with the implementation of CDM and CSM. This package includes a comprehensive ServiceNow Implementation Services package that provides configuration services for ServiceNow products and services. This package includes a comprehensive Implementation Services package that provides configuration services for ServiceNow products and services.

ServiceNow CDM PHASE 1 CDM PHASE 2

ServiceNow ServiceNow Orchestration Core

ServiceNow ServiceNow Orchestration Core provides a comprehensive solution for the orchestration and coordination of serviceNow's suite of applications. It enables efficient and effective management of serviceNow's suite of applications, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow Orchestration Cloud

ServiceNow ServiceNow Orchestration Cloud is a comprehensive solution for the orchestration and coordination of serviceNow's suite of applications. It enables efficient and effective management of serviceNow's suite of applications, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow Orchestration Development Suite

ServiceNow ServiceNow Orchestration Development Suite provides a comprehensive solution for the development and deployment of serviceNow's suite of applications. It enables efficient and effective development and deployment of serviceNow's suite of applications, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestration services, ServiceNow Business Operations, and ServiceNow Security.

ServiceNow ServiceNow ServiceWatch provides comprehensive reporting, analytics, and monitoring capabilities to help organizations monitor and manage their IT environments. It enables efficient and effective monitoring of IT environments, including ServiceNow orchestratio
Symantec

Symantec DeepSight Intelligence

Symantec Identity: Access Manager (SAM)

Symantec SYMC Control Compliance Suite

Symantec SYMC Data Center Security Server

Symantec SYMC Encryption Management Server

Symantec SYMC Endpoint Protection

Symantec SYMC Endpoint Protection

Tenable

Tenable Tenable Series Appliance

Tenable Security Center Continuous View

Tanium

Tanium Tanium Platform

TANP

CipherForge Casdoor

Tactable Security Center Continuous View

Tactable Tactable Series Appliance

Validation and Identity Protection Service (VIP)

Symantec DeepSight Intelligence collects, analyzes and delivers cyber-threat information through a customizable portal and actionable threat intelligence feeds. It is designed to provide a comprehensive view of the threat landscape and enable organizations to make informed decisions.

https://www.symantec.com/deepsight-products/

Symantec Identity: Access Manager (SAM) is a cloud-based identity and access management platform that provides secure authentication, authorization, and access control to applications, devices, and services.


SYMC Data Center Security Server provides comprehensive security posture management for data centers, including software-defined perimeter (SDP) and continuous systems management.

https://www.tenable.com/products/securitycenter/securitycenter-continuous-view

SYMC Encryption Management Server is a cloud-based solution for managing and automating security policies across Symantec's encryption portfolio.

https://www.symantec.com/deepsight-products/

Symantec SYMC Endpoint Protection provides real-time protection against malware, phishing, and other threats, ensuring a secure environment.

https://www.tanium.com/products/

Tanium Tanium Platform distributes management intelligence and data directly to the computing devices, enabling companies to manage and protect their IT assets in real-time.

https://www.tenable.com/products

Tenable Tenable Series Appliance replaces the Nessus VM Appliance and provides a preinstalled image of all Tenable applications available on the appliance with the Log Correlation Engine and Passive Vulnerability Scanner to be released soon.

https://www.tenable.com/products

Tenable Security Center Continuous View provides broad coverage of the user environment, detection of vulnerabilities, misconfigurations, malware and real-time threats, and continuous systems management.

https://www.tenable.com/products

Tactable Tactable Series Appliance provides real-time protection against threats and offers a customizable solution for enterprises looking to enhance their security posture.

https://www.tenable.com/products
All product categorizations, descriptions and web links have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Trend Micro

- **Deep Security - Compliance Pack**
  - **Functionality**: Tripwire Configuration Compliance Manager automates auditing, change monitoring, compliance processes, monitoring alerts.
  - **Discovery and Audit**: Tripwire Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. You receive highly detailed information on the configurations of your systems, applications, firewalls, routers and switches.
  - **Compliance Automation**: Tripwire CCM automates continuous configuration and compliance assessment, making it easy for your policy engine to tune and modify custom policies. Maximize your resources with a process that supports your goals.
  - **Agentless Architecture**: Tripwire CCM utilizes an agentless architecture, requiring no software to install on the monitored endpoints. You enjoy ease of management across the largest networks and highly cost-effective deployments. Simple and powerful.
  - **Discovery and Audit**: Tripwire® Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. You receive highly detailed information on the configurations of your systems, applications, firewalls, routers and switches.
  - **Compliance Automation**: Tripwire CCM automates continuous configuration and compliance assessment, making it easy for your policy engine to tune and modify custom policies. Maximize your resources with a process that supports your goals.
  - **Agentless Architecture**: Tripwire CCM utilizes an agentless architecture, requiring no software to install on the monitored endpoints. You enjoy ease of management across the largest networks and highly cost-effective deployments. Simple and powerful.
  - **Discovery and Audit**: Tripwire® Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. You receive highly detailed information on the configurations of your systems, applications, firewalls, routers and switches.
  - **Compliance Automation**: Tripwire CCM automates continuous configuration and compliance assessment, making it easy for your policy engine to tune and modify custom policies. Maximize your resources with a process that supports your goals.
**Tripakro**

**Suite360 Intelligence Hub**

- DynamicMP rapidly baselines your application risk by performing a broad, unauthenticated scan of all public-facing web applications, typically starting with a prioritized list identified by our Discovery technology.
- The Tripakro Suite360 Intelligence Hub improves accountability and effectiveness with automated risk reporting for all audiences.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**
  - **BOSS**
  - **CSM**
  - **VUL**
  - **TRUST**

**Tripakro Enterprise**

- Tripakro Enterprise provides real-time threat detection; security automation and business continuity.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**

**Trustwave**

**AppDetectivePro**

- Applications should be a database or Big Data concern that includes immediately assess configuration vulnerabilities, identifiable and recoverable from multi-user/role-based access, distributed architecture, and enterprise-level analytics.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**

**DbProtect**

- DbProtect is a data security platform that unscrambles database configuration information, identifies and access control issues, missing patches, or any toxic combination of settings that could lead to exploitation of vulnerabilities, data leakage, denial-of-service (DoS), or unauthorized modification of data stored within data stores.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**

**Varonis**

**DataProtect (DP)**

- DataProtection is data protection tool that unscrambles database configuration information, identifies and access control issues, missing patches, or any toxic combination of settings that could lead to exploitation of vulnerabilities, data leakage, denial-of-service (DoS), or unauthorized modification of data stored within data stores.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**

**DataPrivilege (DP)**

- DataPrivilege automates data governance by providing a framework for users and data owners to be directly involved in access entitlement review and authorization workflows.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**

**DatAdvantage (DA)**

- DatAdvantage software solution that aggregates user, permissions, data and access information from directories and files serves. Analytics applied to the collected information can show detailed data use and determine rightful access based on business need.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**

**Vendays, Inc.**

**Digital Guardian**

- Digital Guardian is a digital guardian delivers automated and guided security workflows, using automation and guidance for rapid repair of broken or security misconfigurations, and integrates with SIEMs, IT-GRC, compliance and regulatory systems.
- **Vendor Product Family:** CDM Product Family
  - **VUL**
  - **TRUST**
<table>
<thead>
<tr>
<th>CDM PHASE 1</th>
<th>CDM PHASE 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CDM Product Manufacturer</strong></td>
<td><strong>CDM Product Family</strong></td>
</tr>
<tr>
<td>VirtuStream</td>
<td>ViewTrust Software</td>
</tr>
<tr>
<td>VMware</td>
<td>AirWatch</td>
</tr>
<tr>
<td>Kandji</td>
<td>Route</td>
</tr>
</tbody>
</table>