MICRO FOCUS

Data Sheet
IT Operations Management

Data Center Automation

Automate your service governance processes from end-to-end with smarter patching, continuous compliance management, advanced process orchestration, and enterprise-scale provisioning.

Product Highlights

Service Level Objective (SLO)-Based Patch Scan and Remediation for Multi-Vendor Server OS

Patch Policies. Perform automated infrastructure patch scan and remediation actions using patch policies. Policies contain measurement and remediation Service Level Objectives (SLOs) and patch bundles. SLOs define the frequency for automated scan and remediation actions while resource group maintenance windows define when the jobs can be run. Resource groups are subscribed to policies, while resource patch bundles contain information about the type of patches included (e.g., vendor recommended patches or an explicit list of individual patches) along with any corresponding Common Vulnerability Exposure (CVE) data from the National Vulnerability Database (NVD). Remediation SLOs ensure resources remain compliant with patch policies.

Static Patching. Patches can be applied using vendor specific patching infrastructure and local repositories. Create custom patch bundles of various types (e.g., recommended, critical, etc.) for multi-vendor operating systems, such as Windows, RHEL, SOLARIS, and more. When adding patches to a patch policy, patch filters allow sorting of patches based on patch release date, CVSS, and more.

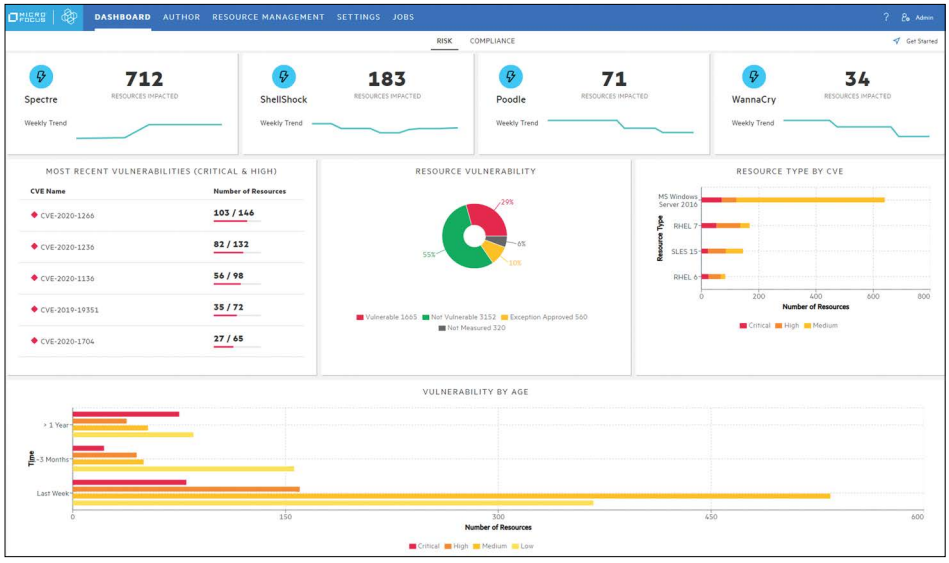

Figure 1. The risk dashboard shows patch vulnerabilities and CVE data across the datacenter.

Key Benefits

- Automate multi-platform patching, compliance, and provisioning to achieve high-quality, repeatable processes; eliminate manual errors and hand-offs between technology silos
- Detect and remediate vulnerability and compliance risks proactively across the data center; eliminate inconsistent patching, intermittent compliance, and meet Service Level Objectives
- Standardize provisioning across multi-vendor server OS and application infrastructure; eliminate error prone manual tasks
- Native integrations with other Micro Focus ITOM solutions provide a more holistic view of datacenter vulnerabilities
- Integrate with existing third-party toolsets via REST APIs to achieve quicker time to value
- Pre and post policy workflows allow for custom process integration

Dynamic Patching. DCA queries the vendor specific update utilities on the target resource to determine which patches should be applied based on vendor recommendations.

The risk dashboard uses CVE data imported from the NVD to identify patching vulnerabilities across IT infrastructure. Resources are evaluated for exposure to all known CVEs and results are displayed on the dashboard in various sections. The dashboard can be customized to show statistics including weekly impact trends and number of affected resources for vulnerabilities of particular interest. Other areas show key information such as most recent vulnerabilities and affected resources, overall resource count by vulnerability status, resource type and count by CVE severity (e.g., 55 critical CVEs on RHEL resources), and vulnerabilities by age (e.g., 14 resources have had an ongoing critical exposure for a period greater than one year).

Automated, Policy-Based Compliance Scan and Remediation for Multi-Vendor Server OS

Ongoing, Policy Based Compliance. Audit and Remediation SLOs are defined for each compliance policy. SLOs define the frequency for audit and/or remediation jobs (e.g., daily, weekly, or monthly). Maintenance schedules are created for resource groups to establish the time period in which these jobs will be run (e.g., Sunday between 12:00am and 6:00am).

Out-Of-The-Box (OOTB) Compliance Scan and Remediation Content. Leverage prebuilt compliance content for a broad range of popular IT, regulatory, and security compliance benchmarks such as CIS, PCI, DSS, SOX, ISO 27001, FISMA, HIPAA, NERC, DISA, and more. The OOTB compliance content includes compliance deployment templates and remediation content. Along with its OOTB compliance content, DCA allows you to create custom compliance benchmarks and policies to meet any internal compliance needs. Policies can contain benchmarks for mixed resource types and can be applied to a resource group containing multiple resource types.

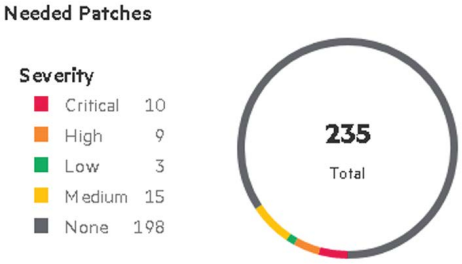

Figure 2. Drilldown from dashboard showing needed patches with CVSS severity.

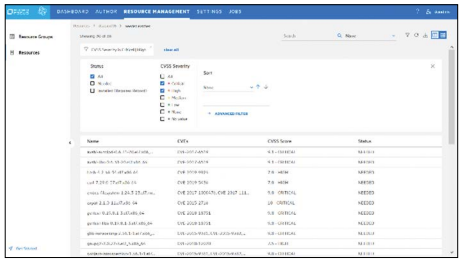

Figure 3. Resource management screen shows patch and compliance statistics for a given resource.

Compliance Dashboard. Obtain compliance reports via dashboards available for resource groups, individual resources, and policies. Observe key details on compliance such as compliance status (within or outside of SLOs), severity, and failed benchmarks. Overall infrastructure compliance statistics and metrics are available from the central dashboard. Drill into the dashboard for more detailed information including benchmark and resource identification. DCA's Collect-Once-Store-Once (COSO) reporting allows you to report on historical as well as transactional compliance data.

Provisioning and Configuration Features

Configurable Build Plans. Out-of-the-box with customizable build plans for multi-vendor OS including but not limited to: RHEL, Solaris, Windows, CentOS, and Ubuntu. Build plans can be customized to include advanced configurations such as RAID and BIOS settings. Configure custom scripts to be run at time of build to further customize deployments. All provisioning can be scheduled or run ad hoc.

Provision Bare Metal. Bare metal servers can be provisioned using a PXE boot process. Servers are PXE booted and brought under management using an agent. The customizable build plan is then deployed to install the desired OS.

Provision Virtual Servers. View an inventory of unmanaged VMware vCenter and Microsoft SCVMM VMs. OS build plans can be configured to create a VM from a template. When an OS build plan is deployed the selected servers are brought under management and then the desired OS is installed.

Process Orchestration

DCA uses out-of-the-box orchestration workflows to perform DCA operations on managed multivendor OS. Orchestration flows can be created as extensions to automate any processes related to the provisioning, patching, and compliance lifecycle of a resource. Leverage orchestration workflows to integrate with 3rd party tools and existing content, for example—create a workflow that updates a service management ticket when a compliance or provisioning operation is performed on a particular resource or resource type.

DCA Containerized Deployment Option

Built on top of the ITOM Container Deployment Foundation (CDF), containerized DCA presents new innovations for orchestrated infrastructure management. The ITOM CDF platform has a simple install process and once installed handles all provisioning, orchestration, and management of the underlying core Kubernetes/Docker cluster infrastructure. The CDF UI is a single portal used for DCA suite and CDF platform management tasks, making it easier to scale and offering in-place upgrades.

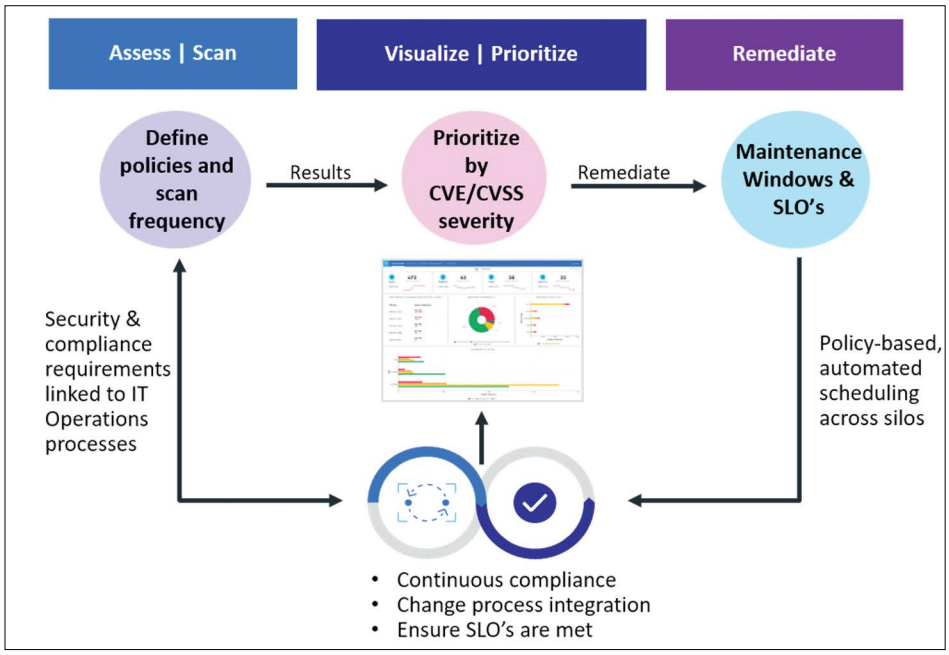

Figure 4. Micro Focus DCA process framework

DCA Suite Management. Monitor job queues and check the health and status of individual service pods from the analytics dashboard. Debug issues by viewing log files and configuration files from the UI. Create and manage suite namespaces and perform other suite configuration tasks including installs and upgrades.

Scale Horizontally. Easily scale DCA for greater resource capacity by adding new Kubernetes worker nodes. Worker nodes can be added from the CDF UI. Once credentials are provided for the new worker node, CDF installs Kubernetes/ Docker on the node. When CDF completes the provisioning of the new worker node it is added to the cluster and begins to accept workloads from the master.

Headless Operation. Because DCA is built on open APIs, any DCA on CDF feature is available using RESTful APIs. These APIs enable the full capacity of DCA to be leveraged from any technology capable of consuming an API.

Mixed Mode Operation. Containerized DCA manages mixed mode deployments on agentless and agent based resources in the datacenter. Agent based operations are performed using existing agent based infrastructure such as Server Automation. DCA can integrate with an external UCMDB to quickly onboard existing infrastructure resources. Agentless resources can also be imported directly into DCA using orchestration workflows.

Server Automation Integration. DCA can be integrated with Server Automation to discover existing resources and resource groups under SA management. Once resources are discovered, DCA discovers the OS deployed on the resources. From there, the full range of DCA capabilities and operations can be performed on these resources. Quickly identify SA managed resources on DCA dashboards and resource lists.

Robust Reporting and Integrations

Integration with Operations Bridge Manager. Out-of-the-box integration with Micro Focus Operations Bridge Manager (OBM) allows DCA to send compliance and vulnerability scan data into OBM to further assess the business service level impact of vulnerabilities on specific resources, giving a more holistic view of the datacenter.

DCA COSO Reporting. Powered by the ITOM reporting service. Leverage OOTB business value dashboards or bring your own BI tool to create reports that best fit your needs. Analyze both historical as well as operational data to gain a complete picture of the risk and compliance state of your datacenter.

REST APIs. Call DCA functionality from any external tool that can consume APIs. Modern REST APIs allow you to integrate DCA functionality into your workflows for a truly customized experience. Seamlessly integrate patch and compliance functionality for secure, compliant deployments.

Key Features

- Static and dynamic patch polices with SLO-based scan and remediation actions and exception management features
- Comprehensive out-of-the-box compliance content for the most popular IT, regulatory, and security compliance benchmarks
- Risk and compliance dashboards for quick assessment of the current state of the datacenter
- Integration with Micro Focus Operations Bridge Manager to further assess the business service-level impact of vulnerabilities
- DCA COSO Reporting powered by the ITOM Reporting service provides business value dashboards or the ability to bring your own BI tool
- Containerized deployment option for easier, in-place upgrades
- Policy extension workflows allow for customized, end-to-end patch, compliance, and provisioning processes
- REST APIs allow DCA functionality to be called from third-party tools that can consume APIs

Contact us at:
www.microfocus.com

Like what you read? Share it.

DCA Suite Features and Capabilities	DCA Express Patch	DCA Premium + Compliance
Security Patching		
Patch scan, discovery, and remediation	X	X
Vulnerability scoring and risk dashboard	X	X
SLO-based patching to prevent breaches	X	X
IT Compliance		
Compliance scan, discovery, and remediation		X
Compliance dashboard		X
SLO-based compliance management to always meet SLAs		X
Provisioning, Configuration Drift, Global Shell		X
Other Features		
Streamline infrastructure operations through orchestration	Patching Orchestration	Infrastructure Orchestration
Real-time & historical reporting (COSO based)	X	X
Puppet integration—manage patch & compliance centrally	X	X
Host connectivity via agent	X	X
Host connectivity—agentless	X	X

For a complete list of supported devices, systems, and applications please visit:
Data Center Automation Documentation

Learn more at
www.microfocus.com/DCA