Product Flyer
IT Operations Management

Automate IT Compliance and Vulnerability Risk Management

Micro Focus® Data Center Automation (DCA) automates IT compliance and vulnerability risk management across multivendor server OS, databases, and middleware for the hybrid enterprise.

DCA at a Glance:

- **End-to-End IT Compliance and Vulnerability Risk Management:**
  Assess, prioritize, and remediate risks in a single UI
- **Closed-Loop Remediation:**
  Remediate according to policies, Service Level Objectives (SLOs), and maintenance windows
- **Multivendor Support and Integration:**
  Run IT compliance, patching, and remediation across a heterogeneous data center, with support and content available for the broadest range of multivendor infrastructure

The Challenge

Faced with relentless threats and breaches, enterprise IT struggles to manage IT compliance and vulnerability risks. With a proliferation of tools and manual, error-prone processes, there is limited visibility of the state of risk in the data center. The growing scale and nature of self-service hybrid infrastructure add further complexity.

The Solution: DCA

DCA provides a powerful solution, automating IT compliance and vulnerability risk management for the hybrid enterprise.

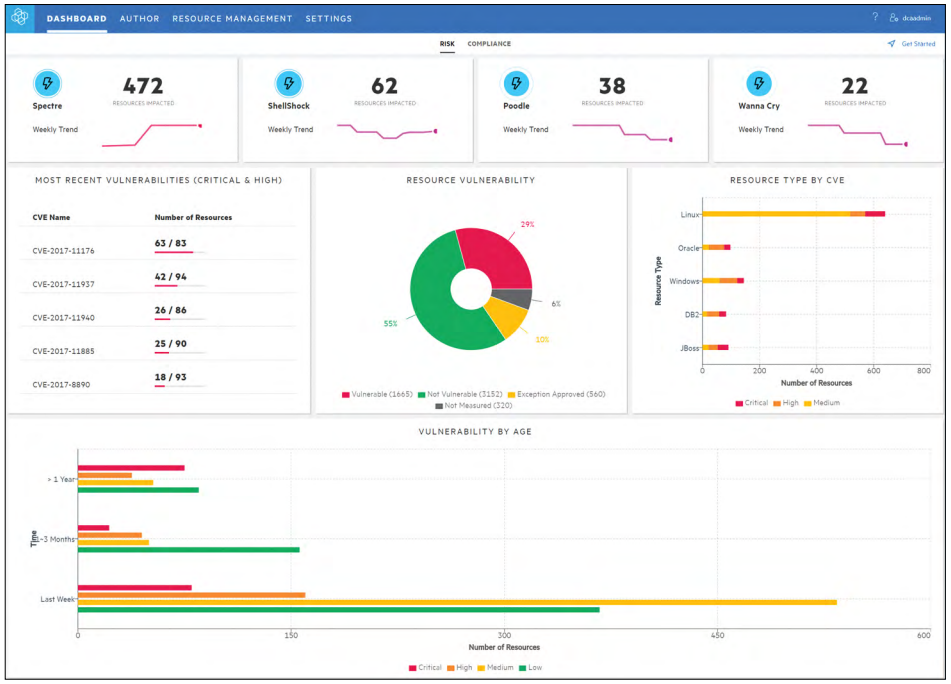

Figure 1. Risk dashboard

> **"Using a single version of the truth can significantly improve decision-making. A compliance and risk dashboard … [presents] the information in an easy-to-digest way, and tools such as DCA provide visibility into compliance and patch status across the infrastructure stack."**
>
> **ROY ILLSLEY**
> Principal Analyst, Infrastructure Solutions
> Ovum

Contact us at:
www.microfocus.com

Like what you read? Share it.

DCA offers a three step approach to risk management: **assess**, **prioritize**, and **remediate**.

The first stage is assessment. Scan the risk state of the data center against policies using the compliance and vulnerability content provided by DCA.

Prioritization follows. DCA makes it easy to determine what compliance variances should be fixed and what patches should be applied first. The **actionable, drill-down dashboard** shows risks by severity, key events, age of vulnerabilities, resources affected, and benchmarks.

Once the risks are prioritized, remediate them according to SLOs and maintenance windows.

The Details

SLO-based Policy and Closed-Loop Remediation

- Manage IT compliance and vulnerability risk using a Service Level Objective (SLO)-based policy and closed-loop remediation model.
- Customize policies to define the frequency of scans and remediation in accordance with SLOs and maintenance windows.
- Close the compliance and patch gap with orchestrated remediation. Built-in flows automate pre- and post-processes for remediation.

Regulatory, Security, and Internal IT Compliance

- DCA automates compliance audits and remediation across server OS, databases, and middleware, referencing market-leading out-of-the-box compliance benchmarks and remediation actions for PCI DSS, HIPAA, FISMA, CIS, ISO 27001, and more.

Vulnerability Risk Management

- DCA imports the Common Vulnerability Exposure (CVE) list from the National Vulnerability Database, and patch metadata from authorized sources, such as vendor repositories. The risk dashboard combines this, with the latest patch scans, to give the most up-to-date risk view.

Multivendor Support and Integration

- Tap into the broadest range of support for multivendor platforms; these include Windows, RHEL, SUSE, Ubuntu, Oracle, SQL Server, Db2, Microsoft IIS, and JBoss.
- Centralize risk management by using DCA to discover and run operations on resources deployed by open-source configuration management tools.

Container Deployment

- DCA deploys on open-source container architecture for easy installation and upgrades.

The Business Value

With DCA, manage compliance and vulnerability risks proactively and consistently across the hybrid enterprise.

Learn more at
www.microfocus.com/dca