White Paper

Where Security and IT Ops Come Together—5 Features to Secure Against Risks

IT Ops and the Security team must work together to reduce risks across infrastructure. This paper discusses how Data Center Automation (DCA) automates IT compliance and vulnerability risk management with five key features, combining security and operations in one tool for the single source of the truth.

opentext™

Table of Contents

page

"It's virtually impossible to show that IT Ops is remediating the exact requirements that Security hands down, and how our remediation ties back to the original requirements." If this statement resonates with you, then likely you are struggling to keep up with security requirements across decoupled content and toolsets.

IT Ops and the Security team must work together to reduce risks across multivendor server operating systems. When the Security team defines the requirements, it's up to IT Ops to remediate proactively and consistently. IT Ops must also prove risk status against the original requirements. Essentially, Security requirements must link directly to IT Ops processes.

"It's virtually impossible to show that IT Ops is remediating the exact requirements that Security hands down, and how our remediation ties back to the original requirements." If this statement by an IT Ops Engineer resonates with you, then likely you are struggling to keep up with security requirements across decoupled content and toolsets.

In this paper, we'll discuss how OpenText™ Data Center Automation (DCA) automates IT compliance and vulnerability risk management with five key features, combining security and operations in one tool for the single source of truth:

- Separation of duties—independent content and role-based security access
- Policy-based automation with built-in SLO and exception management
- Intelligent job scheduling
- Single-UI compliance and risk dashboards
- SLO-based closed-loop remediation

Separation of Duties—Independent Content with Role-Based Access Control

Are your IT ops engineers writing PCI scripts, running them, and producing audit reports for your Security team? When one team does everything, write compliance and patch scripts, run them, and generate audit reports, the results don't generate high confidence. If you're making your own checks for security, how do you ensure thoroughness and accuracy?

DCA provides a security framework with out-of-the-box compliance benchmarks and imported Common Vulnerability Exposure (CVE) and patch metadata. Role-based access control (RBAC) enforces process compliance and simplifies security administration.

Out-of-the-Box Regulatory and Security Compliance Benchmarks

DCA is preloaded with out-of-the-box regulatory and security compliance benchmarks and remediation actions for PCI DSS, HIPAA, FISMA, CIS, ISO 27001, and more. DCA provides detailed rules for benchmark requirements—the content is already written for you, so you don't have to create it yourself. You can also clone or customize benchmarks for internal IT compliance needs.

Imported CVE and Patch Metadata

DCA provides tools to download and import CVE data from the National Vulnerability Database (NVD) and patch metadata from authorized sources such as vendor repositories.

You can create a patch bundle, a baseline of what should be patched, using the imported CVE and patch metadata. The patches are categorized based on severity, Common Vulnerability Scoring System (CVSS), patch type, operating system, and patch release date. You can search for patches by specific CVE ID and create targeted patch bundles for particular threats. Or you can take a broader approach and scan target resources based on vendor recommendations.

Create a patch bundle using imported CVE data from the National Vulnerability Database (NVD) and patch metadata from vendor repositories. The patches are categorized based on severity, Common Vulnerability Scoring System (CVSS), patch type, operating system, and patch release date.

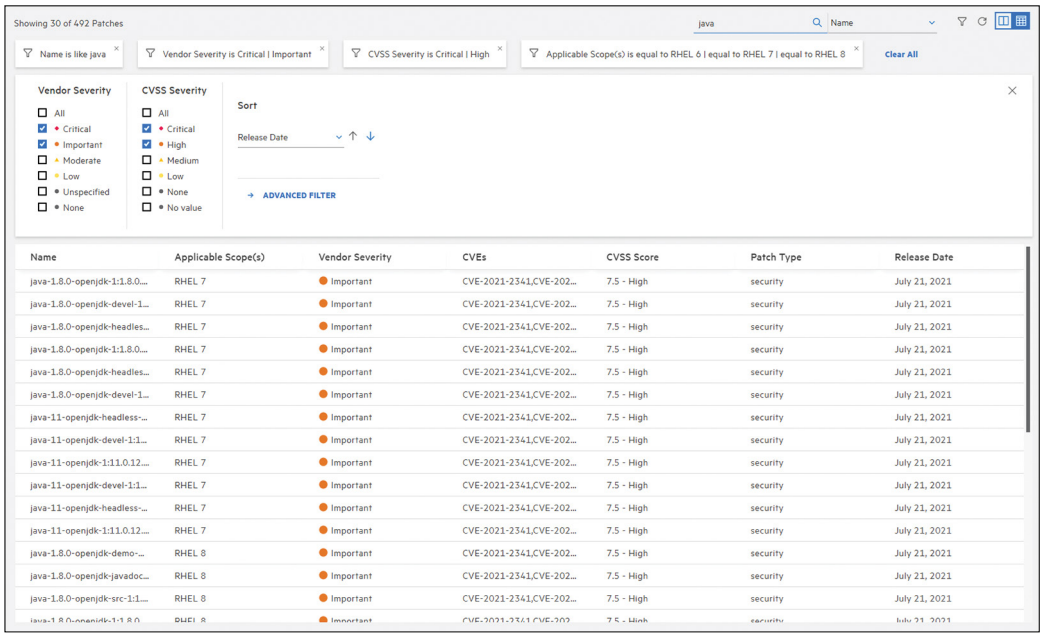

Figure 1. Patch list by severity, CVE IDs, CVSS score and release date

RBAC

RBAC helps to enforce process compliance and grants access to data center resources based on roles. Different roles help to ensure separation of duties between Authors, Operators, Resource Owners and Auditors. An Author role allows you to create policies using benchmarks and patch bundles. A Resource Owner role enables you to manage resources and resource groups, add policy subscriptions and maintenance windows, set exceptions and run scans and remediation. The Operator has privileges to run scans and remediation. A view-only Auditor role has access to the security policies and dashboards to evaluate the risk state of the data center.

DCA delivers a policy-based solution that bridges automation across teams. A policy can include a set of benchmarks, patch bundles, measurement SLO (scan frequency), remediation SLO (how soon to remediate after a scan), and the actions to be performed when non-compliance or risk is detected.

Policy-Based Automation with Built-in SLO and Exception Management

How do you fit IT compliance and vulnerability risk management into existing enterprise processes? There are maintenance windows to consider, Service Level Objectives (SLOs) to keep up with, and exceptions to manage.

DCA delivers a policy-based solution that bridges automation across teams. A policy can include a set of benchmarks, patch bundles, measurement SLO (scan frequency), remediation SLO (how soon to remediate after a scan), and the actions to be performed when non-compliance or risk is detected. A policy is then associated to a resource group (e.g., all RHEL servers).

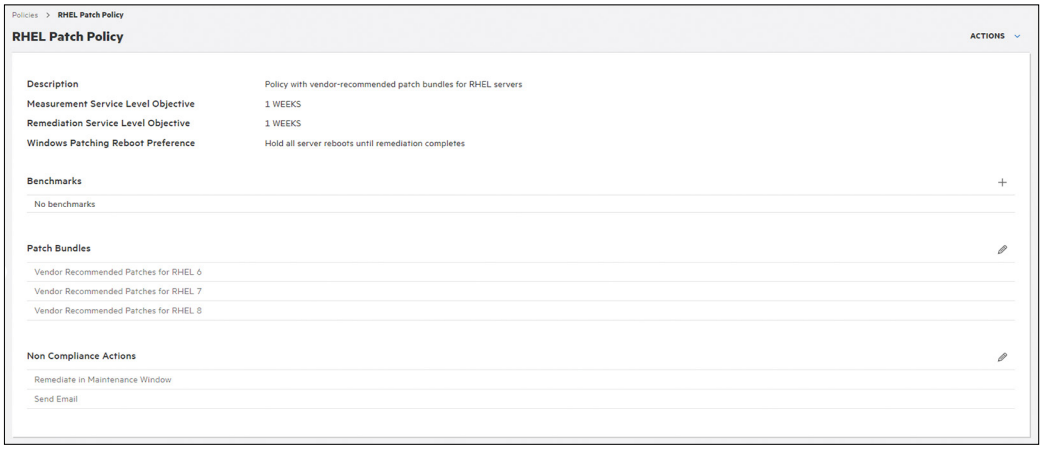

Figure 2. Policy-based compliance and patch management

A large organization will always have exceptions and there needs to be a consistent way to document and manage them. With DCA built-in exception management, you can document the exceptions and assign a designated approver to oversee them.

Intelligent Job Scheduling

Not all of the scheduling is in the automation system; they're also in Outlook emails. Manually scheduling jobs is a tedious error-prone task. Coordination with resource group owners to schedule jobs takes too long and leaves gaps.

In the absence of an intelligent job scheduler, there are many silos. You have to work with resource owners (e.g., server admins) to coordinate messy compliance and patch jobs, negotiating your way through limited maintenance windows. Oversight and errors are likely to crop up in this intensely-manual process. Unfortunately, this is an all-too-common situation.

DCA has a built-in, intelligent job scheduler. The job scheduler uses two already-known input parameters—the measurement and remediation SLOs and the maintenance windows—to automatically generate the job schedule.

DCA automatically creates the job schedule the moment SLOs and maintenance windows are defined. And if SLOs and maintenance windows change, DCA recreates the schedule.

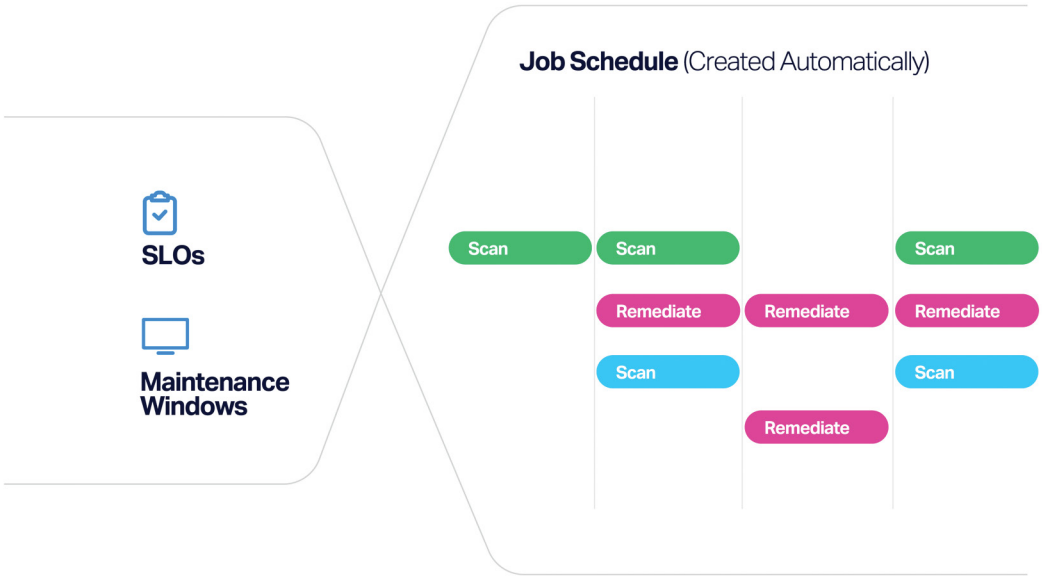

Figure 3. Intelligent job scheduler

Behind the scenes, DCA figures out the load and dependencies across the infrastructure. Without any manual intervention, it automatically schedules the jobs at appropriate time slots based on maintenance windows and the availability of resources. With the intelligent scheduler, you don't have to manually coordinate and create job schedules. Nobody pushes a "create schedule" button. DCA creates the schedule the moment SLOs and maintenance windows are defined. And if SLOs and maintenance windows change, DCA recreates the schedule.

Single-UI Compliance and Risk Dashboards

Do you have a single tool that your Chief Information Security Officer (CISO) can log in to and see the latest security exposures? Can you go to one place to see what hasn't been patched yet? With DCA, you get one window into the risk state, with actionable, drill-down dashboards.

In the compliance dashboard, you can see a complete view of infrastructure compliance by benchmarks (e.g., PCI compliance), by severity, by resources (e.g., RHEL servers, Oracle Linux servers), and by how long it took to remediate out-of-compliance resources.

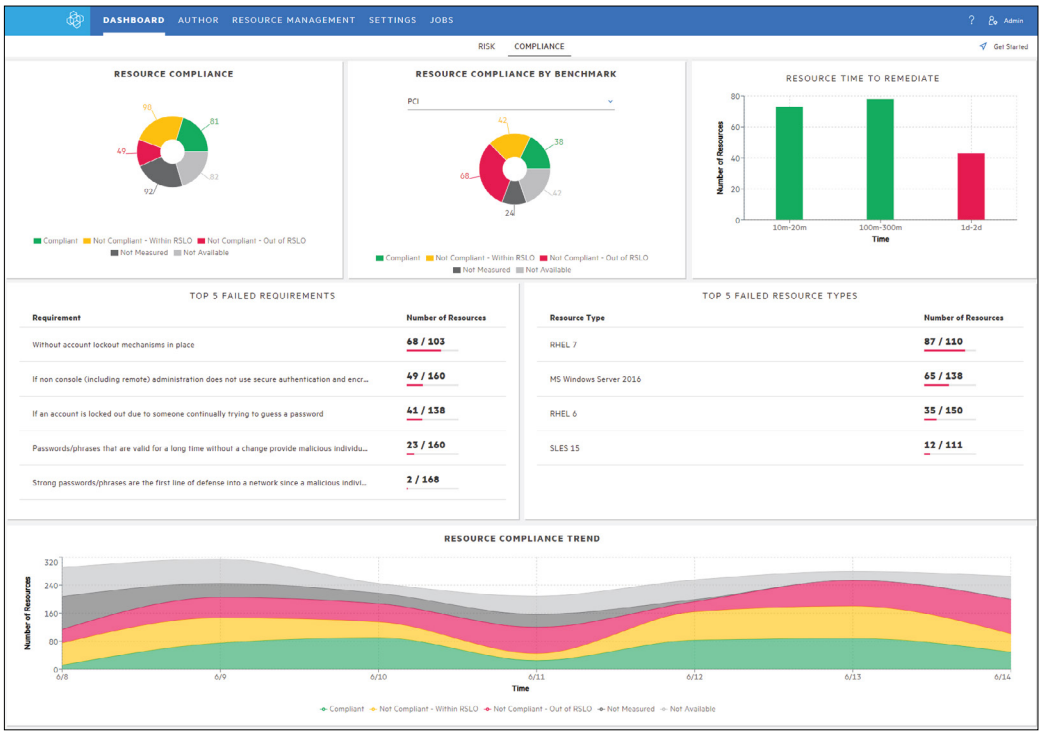

Figure 4. Compliance dashboard

The risk dashboard shows recent critical vulnerabilities, number of resources impacted, vulnerabilities by severity, and old vulnerabilities that have not yet been remediated. Combining the latest patch scan results with the most recent vulnerabilities, the dashboard helps you proactively assess risk state and prioritize remediation actions. Then, you can assess the progress made towards remediating risks and continuously monitor the trend of exposures.

Combining the latest patch scan results with key risk events (such as the most recent critical and high vulnerabilities), the dashboard helps you proactively assess risk state and prioritize remediation actions.

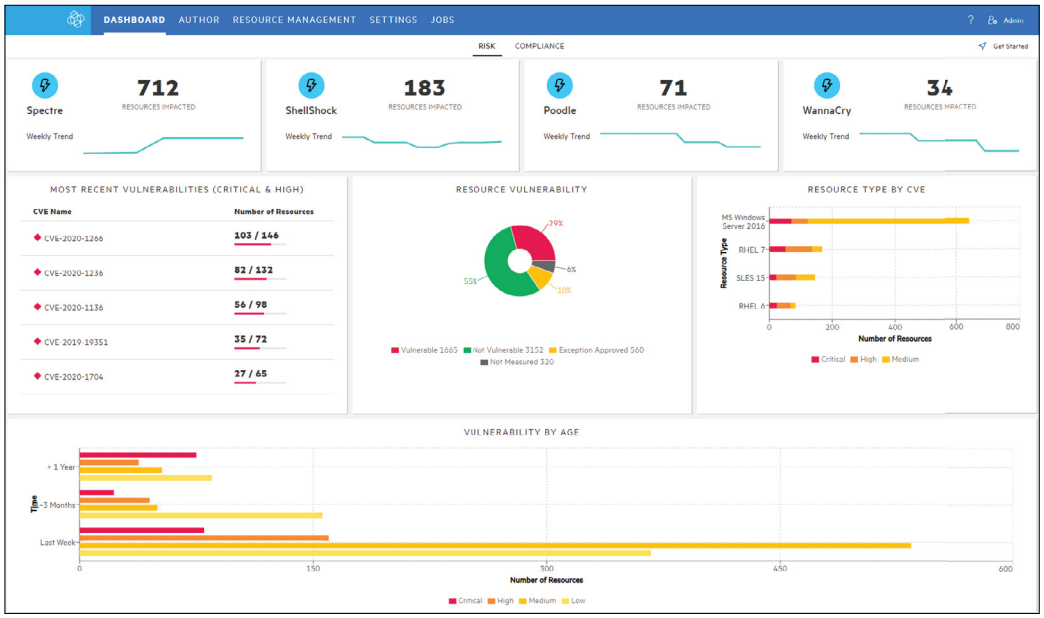

Figure 5. Risk dashboard

SLO-based automated remediation is where DCA shines. Remediate right after a scan or according to maintenance windows and SLOs.

SLO-Based Closed-Loop Remediation

Manual remediation—when the scan is decoupled from the remediation process—is a huge business risk. Without closed-loop remediation, it's difficult to follow up on gaps on time and protect the data center. SLO-based automated remediation is where DCA truly stands out. You can remediate immediately after a compliance and patch scan, or according to maintenance windows and SLOs. During remediation, DCA orchestrates the processes for IT compliance configuration and patching, with the ability to trigger orchestration flows to run pre- and post-process dependencies.

Putting It All Together, in Five Easy Steps

Now that we've discussed the five key features for automated IT compliance and vulnerability risk management, let's turn to how you can implement the process in DCA:

1. Create a policy using out-of-the-box compliance benchmarks and/or patch bundles with desired measurement and remediation SLOs.
2. Attach the policy to a data center resource group and set up maintenance windows for the policy to run on the resources.
3. Scan according to the measurement SLO and assess exposure in the compliance and risk dashboards.
4. Remediate risks on-demand or according to the remediation SLO.
5. After remediation, reassess risk state in the compliance and risk dashboards.

Connecting Security and Operations

This paper has shown how DCA creates a complete chain for your risk management lifecycle with five key features. These features include: out-of-the-box compliance content and imported patch metadata, SLO-based policy automation, intelligent job scheduling, single-UI dashboards, and closed-loop remediation. With these capabilities, IT Ops can prove exactly how and when all security requirements are met, mapping to specific benchmarks, CVEs, and remediation objectives.

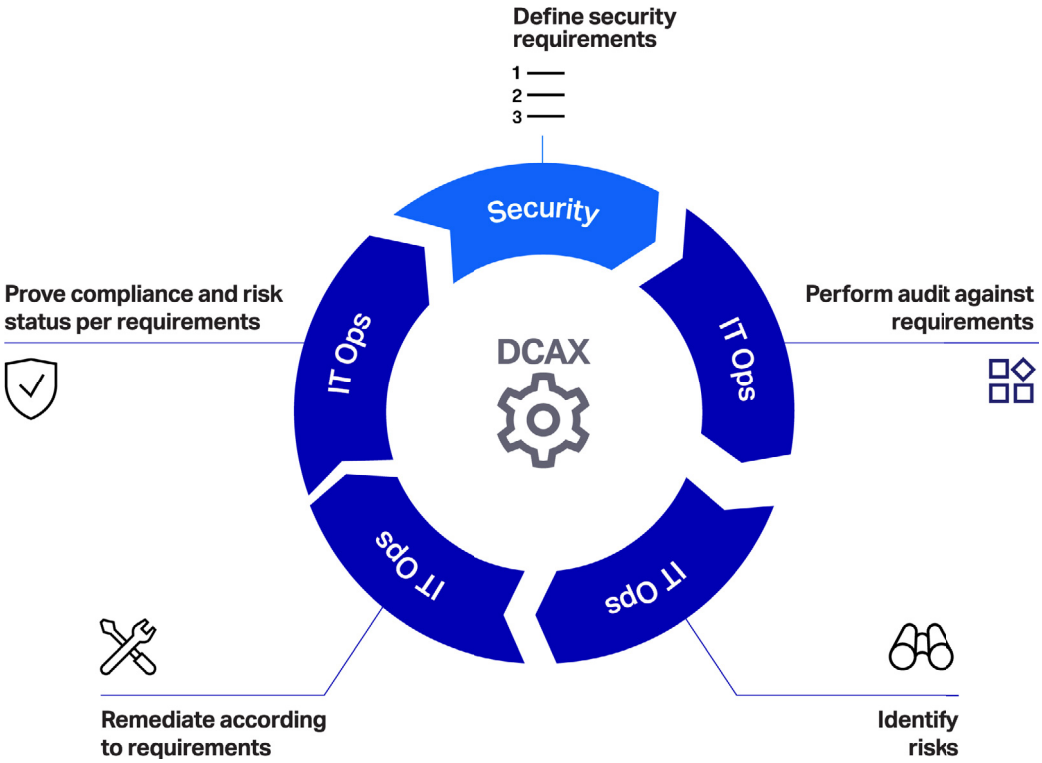

Figure 6. Proving security requirements

Learn more at
www.microfocus.com/dca
docs.microfocus.com/itom/ITOM:Data_Center_Automation/Home
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™