VMware vRealize Automation SaltStack SecOps

KEY BENEFITS

- Enforce security – Remediate critical security threats across on-premises or cloud infrastructure with powerful vulnerability remediation automation.
- Maintain compliance – Use out-of-the-box Center for Internet Security (CIS) certified content to provision IT systems that start compliant and stay that way.
- Reduce risk – Employ powerful SecOps automation that goes beyond scanning to actually find and fix critical IT vulnerability and compliance issues.

VMware vRealize® Automation SaltStack® SecOps is the compliance and vulnerability management component of vRealize Automation, delivering full-service, closed-loop automation for IT system compliance and vulnerability remediation. With SaltStack SecOps, security and operations teams can work together to define a corporate IT security policy, scan systems against it, detect vulnerabilities and non-compliance issues, and actively remediate them—all from a single platform.

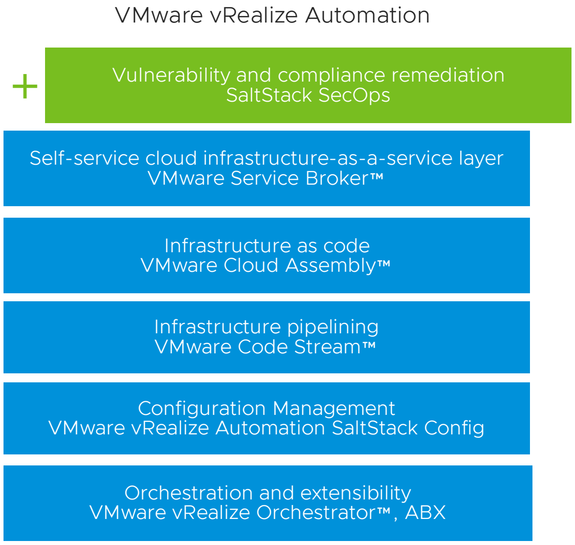

VMware vRealize Automation
+
Vulnerability and compliance remediation
SaltStack SecOps
Self-service cloud infrastructure-as-a-service layer
VMware Service Broker™
Infrastructure as code
VMware Cloud Assembly™
Infrastructure pipelining
VMware Code Stream™
Configuration Management
VMware vRealize Automation SaltStack Config
Orchestration and extensibility
VMware vRealize Orchestrator™, ABX

FIGURE 1: SaltStack SecOps adds infrastructure security and compliance to vRealize Automation.

SecOps automation built for modern security requirements

Security and IT operations teams must work together to keep modern data centers compliant and secure, but their efforts are often crippled by disparate toolsets, misaligned workflows, and competing priorities. It's time for that to change. SaltStack SecOps is a powerful add-on component for vRealize Automation that gives IT operations and security teams the automation tools and content they need to build and maintain secure, compliant IT infrastructure—on premises or in the cloud.

SaltStack SecOps provides:

- Continuous operating system compliance enforcement
- Automated vulnerability detection and remediation
- Immediate insights into the state of your IT systems

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller. For detailed product specifications and system requirements, refer to the SaltStack SecOps documentation.

Pre-built, certified IT security content

Most organizations must comply with multiple regulations and standards, each made up of thousands of individual requirements and checks. SaltStack SecOps includes a database of up-to-date, certified security content based on CIS and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) frameworks, allowing teams to detect compliance issues and enforce requirements for multiple compliance standards with a single action.

Continuous compliance enforcement

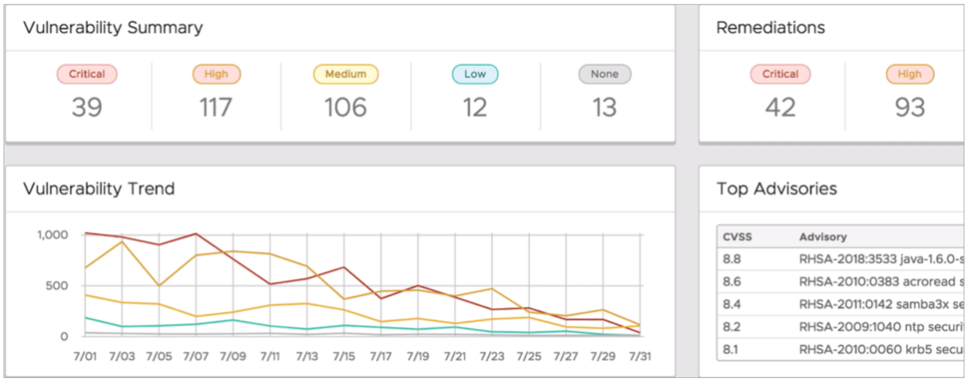
Chasing compliance drift on existing systems can feel like a recurring nightmare. SaltStack SecOps actively scans for compliance drift and provides automated remediation playbooks to enforce defined security policies—saving resources, improving security posture, and reducing risk.

SaltStack SecOps enables collaboration and quick action, while still supporting governance and control. Administrators can apply role-based access controls that allow security and IT professionals to work within their scope of duties to define compliance and security policies, scan systems against them, remediate issues, and track trends.

Closed-loop vulnerability management

Security scanners can report avalanches of vulnerabilities that operations teams must translate into IT tickets, investigate, prioritize, test, fix, and then report back to security. SaltStack SecOps brings the power of vulnerability automation to operations teams by scanning IT systems for more than 15,000 OS and infrastructure vulnerabilities, and then providing out-of-the-box automation workflows that remediate them.

In addition to native vulnerability scanning, SaltStack SecOps is also capable of ingesting scans from third-party solutions, including Tenable, Rapid7, Qualys, and Kenna, for fast, automated vulnerability remediation.



Vulnerability Summary

Critical	High	Medium	Low	None
39	117	106	12	13

Remediations

Critical	High
42	93

Vulnerability Trend

Top Advisories

CVSS	Advisory
8.8	RHSA-2018:3533 java-1.6.0-s
8.6	RHSA-2010:0383 acroread s
8.4	RHSA-2011:0142 samba3x se
8.2	RHSA-2009:1040 ntp securi
8.1	RHSA-2010:0060 krb5 secu

FIGURE 2: Track vulnerabilities across your IT footprint and remediate them with out-of-the-box vulnerability automation workflows.

Item No: 724181aq-ds-word-vreal-auto-ssso-uslet 2/21