VMware Aria Automation for Secure Hosts

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 secure host automation that goes beyond scanning to find and fix critical IT vulnerability and compliance issues.

VMware Aria Automation™ for Secure Hosts is the compliance and vulnerability management add-on component of VMware Aria Automation, delivering full-service, closed-loop automation for IT system compliance and vulnerability remediation. With VMware Aria Automation for Secure Hosts, 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.

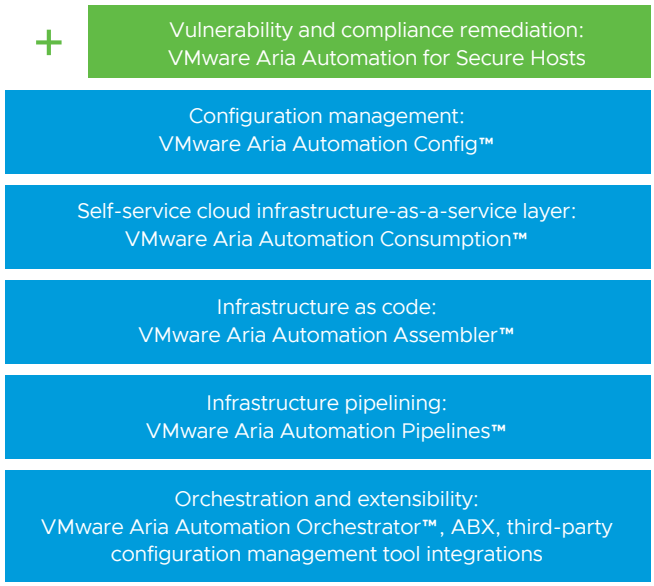

Figure 1: VMware Aria Automation for Secure Hosts adds infrastructure security and compliance to VMware Aria Automation.

Built for modern security requirements

Security and IT operations teams must work together to keep modern data centers compliant and secure, but disparate toolsets, misaligned workflows, and competing priorities often cripple their efforts. VMware Aria Automation for Secure Hosts is a powerful add-on component for VMware Aria 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. VMware Aria Automation for Secure Hosts provides continuous OS compliance enforcement, automated vulnerability detection and remediation, and 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 VMware Aria Automation for Secure Hosts 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. VMware Aria Automation for Secure Hosts 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. VMware Aria Automation for Secure Hosts actively scans for compliance drift and provides automated remediation playbooks to enforce defined security policies by saving resources, improving security posture, and reducing risk.

VMware Aria Automation for Secure Hosts 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. VMware Aria Automation for Secure Hosts 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, VMware Aria Automation for Secure Hosts is also capable of ingesting scans from third-party solutions, including Tenable, Rapid7, Qualys and Kenna, for fast, automated vulnerability remediation.

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

Item No: 1861500aq-ds-vmw-aria-auto-sec-hosts-uslet 2/23