Secure Configurations and Streamline Compliance

VMware Capabilities At a Glance

Improve your cloud security and compliance posture with real-time visibility into resource relationships, misconfigurations, risk scores, and activity logs across a multi-cloud environment, with the ability to quickly resolve security findings via alerts or automated remediation. Ensure continuous compliance with custom policies or out-of-the-box security rules based on industry standards.

VMware Aria Solutions

- VMware Aria Automation
- VMware Aria Automation for Secure Clouds
- VMware Aria Automation Config
- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks

Multi-cloud environments deliver business agility that gives organizations a competitive edge. Yet keeping enterprise data and infrastructure secure and compliant becomes increasingly difficult with each new cloud. Escalating cyber threats and increasing competition for security talent mean organizations are challenged to effectively manage risk, maintain governance, and ensure their multi-cloud environments remain in compliance with legal and regulatory obligations.

VMware Aria cloud management solutions empower IT operations teams to proactively reduce misconfigurations and harden assets while enforcing compliance guardrails across environments. VMware solutions also improve collaboration between developer, security, and operations (DevSecOps) teams, enabling organizations to proactively detect and remediate violations before they negatively impact users and the business.

Misconfigurations and threats challenge organizations

The cost of ransomware incidents worldwide is expected to exceed $265 billion by 2031.[1] Unpatched vulnerabilities—the most prominent attack vector exploited by ransomware groups[2]—continue to plague organizations. Through 2023, at least 99 percent of cloud security failures will be the customer's fault,[3] according to Gartner. While cloud data breaches make headlines, reports rarely describe the root cause, which is often a simple misconfiguration. In a recent survey, one in six companies (17%) said it had a public cloud security breach due to a misconfiguration in the last year.[4]

Without a better approach to strengthening security and streamlining compliance in multi-cloud environments, organizations face challenges including:

- Stolen data and outages that decrease brand loyalty and trust
- Risk of fines and litigation due to non-compliance with industry or government mandates
- Too much time and budget spent manually chasing security and compliance issues
- Lack of visibility into risky cloud misconfigurations
- Inability to detect and respond to threats before they become a problem
- Increasing threat surfaces and vulnerabilities that invite cybercriminal intrusion

[1] ZDNet. "The Cost of Ransomware Attacks Worldwide Will Go Beyond $265 Billion in the Next Decade." June 7, 2021.
[2] Ivanti. "Ransomware Spotlight Year End Report," 2021.
[3] Gartner, "Hype Cycle™ for Cloud Security, 2021," Tom Croll and Jay Heiser. July 27, 2021.
[4] VMware. "CloudHealth," 2021.

"VMware Aria Cost powered by CloudHealth, for the first time, creates a single view of our cloud activity, across multiple territories. We're no longer hunting for information. It's all there at the click of a button."

Johan Marais
Sr. Platform Services Manager
Discovery Holdings

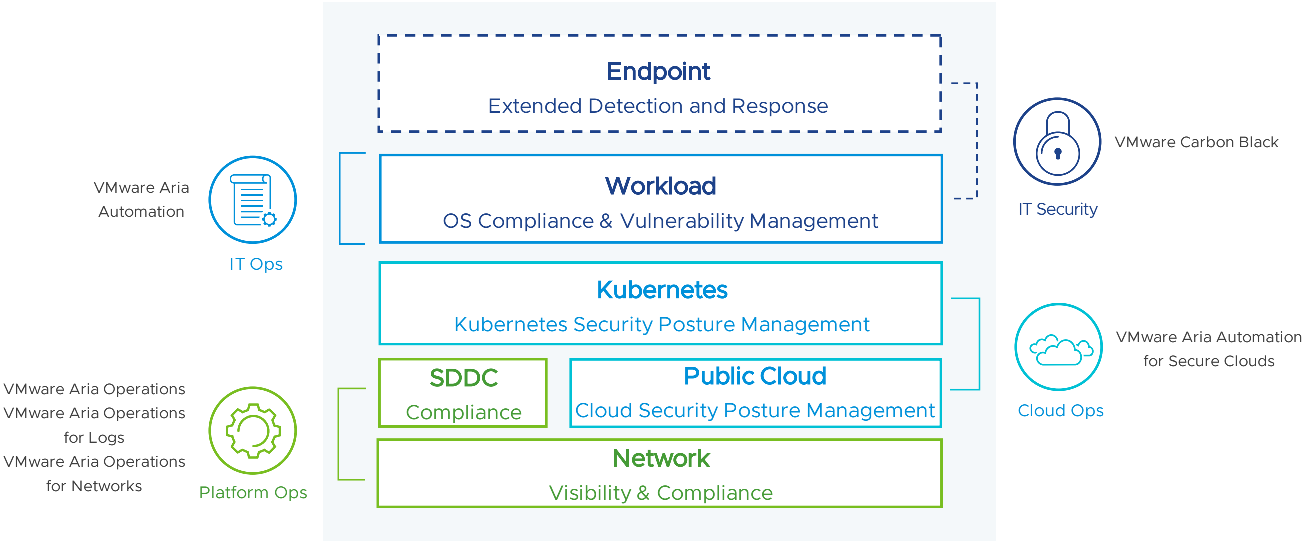
Inconsistent processes coupled with manual solutions prevent IT organizations from effectively governing data, infrastructure, and operations. In contrast, teams that manage risk by applying intelligent management and enforcement approaches have tremendous advantages, including being able to detect new security and compliance violations in less than six seconds of a configuration change event.[5]

Strengthen security and streamline compliance in distributed environments

Organizations across industries strengthen security postures, advance governance, and improve compliance with VMware Aria cloud management solutions. As part of a strategic cloud operating model powered by VMware Aria, VMware solutions move overburdened IT staff away from performing manual configuration tasks and chasing threats to work on projects that boost innovation and competitive differentiation. At the same time, VMware Aria gives executives and boards of directors confidence the business is resilient to cyberattacks and insider threats while empowering IT leaders to reduce infrastructure and application misconfigurations that negatively impact revenue, productivity, security, and compliance postures.

Organizations can simplify hardening tasks while preventing unauthorized access. They can monitor for non-compliance and automatically remediate when needed. They can shift-left, establishing guardrails for clouds and applications that enable the business to accelerate digital transformation. Teams using VMware Aria benefit from consistent, automated operations enforcement of cloud workloads and cloud services; intrinsic security built into hybrid and public cloud frameworks; and third-party integration that helps ensure DevSecOps teams are working smarter together to combat malicious intent and human errors.

VMware Multi-Cloud Security and Compliance Capabilities


Endpoint
Extended Detection and Response
Workload
OS Compliance & Vulnerability Management
Kubernetes
Kubernetes Security Posture Management
SDDC
Compliance
Public Cloud
Cloud Security Posture Management
Network
Visibility & Compliance
VMware Aria Automation
IT Ops
VMware Aria Operations
VMware Aria Operations for Logs
VMware Aria Operations for Networks
Platform Ops
VMware Carbon Black
IT Security
VMware Aria Automation for Secure Clouds
Cloud Ops

[5] VMware. "CloudHealth Secure State Platform Telemetry," 2022.

Experience It Today

- Request a trial: VMware Aria Automation, VMware Aria Automation for Secure Clouds, or VMware Aria Operations
- Try a Hands-on Lab: VMware Aria Automation

Resources

Review our other briefs:

- Accelerate Delivery Automation
- Unify Operations and Improve Performance
- Simplify Cloud Cost and Capacity Management

Take a deep dive at VMware Aria Automation Config and VMware Aria Automation for Secure Clouds

See where VMware Aria cloud management services are hosted globally

Modern, multi-cloud security and compliance

VMware Aria solutions feature capabilities for cloud workloads, cloud services, and cloud infrastructure. They empower IT teams to more effectively manage risk and maintain governance within and across clouds while ensuring their multi-cloud environments remain in compliance.

4 Ways VMware Aria Strengthens Security & Compliance

1 Continuous security configuration and vulnerability

2 Comprehensive compliance management

3 Shift-left security

4 Advanced network security

1 Continuous security configuration and vulnerability management

Organizations using VMware Aria reduce risk at scale by establishing and enforcing configuration best practices within and across multi-clouds.

- **Cloud Workloads**—Organizations define optimized, compliant software states and then enforce them across the entire environment. Powerful, intuitive event-driven configuration automation rapidly deploys and configures virtual machines (VMs), servers, containers, and network devices on any cloud or on-premises network. This empowers organizations to speed time to market; expand application scale, scope, and business impact; and dynamically adapt application and cloud resources to meet changing needs. IT teams lower risk and enforce IT regulatory standards for digital cloud platforms with integrated compliance and automated drift remediation. Moreover, VMware Aria solutions help teams strip away unnecessary software from digital infrastructure to limit potential vulnerabilities that cyberattackers or insider threats could exploit for gain.
- **Cloud Services**—With VMware software, operations teams improve cloud security and compliance postures with organization-wide standards and fine-tuned policies to protect hundreds of services across multi-cloud environments. An intelligent cloud data model improves risk visibility with real-time visibility, multi-cloud inventory search, and over 1,000 best practices rules to detect 95 percent of security and compliance violations within 6 seconds of a cloud configuration change notification. This helps teams reduce misconfigurations and prioritize threats with advanced risk correlation, visual risk context, and a secure auto-remediation approach.

Learn More About Our Products

- Watch VMware Cloud Management on YouTube
- Read our latest VMware Cloud Management blogs and VMware Aria Automation for Secure Clouds blogs
- Follow us on Twitter
  @VMwareAria
  @VMwareAriaAuto
  @VMwareAriaOps
  @VMwareAriaCost

Licensing

Get started with one flexible license: VMware Aria Universal Suite

2 Comprehensive compliance management

IT teams under pressure to stay up to date with ever-changing regulatory standards and industry best practices can take advantage of VMware Aria to improve compliance.

- **Cloud Workloads**—The software uses event-driven automation to detect changes in the workload and auto-remediate drift by enforcing the desired state. VMware Aria also features more than a dozen out-of-the-box compliance templates (i.e., Payment Card Industry [PCI], Health Insurance Portability Accountability Act [HIPAA], Federal Information Security Management Act [FISMA], Defense Information Systems Agency [DISA], Sarbanes–Oxley Act [SOX] and more) for the multiple clouds that come with VMware Aria. Teams can also create their own custom templates.
- **Cloud Services**—Frameworks continuously benchmark and automate reporting. The software tracks compliance scores, including open violations and the progress different teams are making or have made to resolve issues. Teams can create security policies and scan systems, including in-guest workloads, for common vulnerabilities and exposures (CVEs), then immediately apply appropriate updates or patches to remediate. Seamless integration also allows teams to import security scans from third-party scanning services, then immediately remediate these advisories as well.

3 Shift-left security

With VMware Aria, organizations can efficiently operationalize cloud security programs while boosting developer, security, and operations teams collaboration. Teams can take advantage of dashboards that continuously display results, including anomalies, and monitor suspicious activity. Real-time visibility allows staff to detect security events and misconfigurations within minutes as well as build a unified approach for managing risk across clouds using both security rules and custom guardrails. Shifting left or verifying security configurations earlier in the delivery pipeline allows organizations to proactively remediate violations before production. VMware Aria automates cloud security operations with an API-first platform that easily integrates with other IT, security, and developer tools. For example, teams can:

- Proactively identify and resolve violations through API-based verification within CI/CD pipelines.
- Enable developers to manage cloud risk with role-based access controls for monitoring security and compliance findings.

4 Advanced network security

Teams using VMware Aria have complete coverage in a converged networking and security stack that puts security next to every user and workload, protecting all user-to-app and app-to-app communications—inside and among clouds. They also simplify firewall deployment and operations, eliminate blind spots, and deliver security as code while improving user and distributed workload protection.

Why VMware Aria?

- **Proven solution** from a trusted vendor and market leader
- **Multi-cloud visibility** across private, hybrid, and public clouds
- **Comprehensive capabilities** from a single platform with a common control plane and data model
- **Ultimate flexibility** to choose SaaS, on premises, or a combination of both in one license
- **Broadest ecosystem** that is extensible with 220+ integrations
- **Leading IT in sustainability**, helping customers reduce environmental impact

Uniting and empowering security teams to take action

Organizations trust VMware to protect their muti-cloud environments and bridge the developer and security divide for faster and smarter security. In addition to the powerful, preventive IT operations security capabilities that VMware Aria delivers, the VMware security product portfolio features protections that are built-in and distributed with control points—users, devices, workloads, and networks. VMware security also includes comprehensive cloud and end-point threat detection and remediation.

Learn more about securing configurations and streamlining compliance

Organizations with successful multi-cloud strategies automate configuration policies and proactively enforce compliance as well as harden environments to reduce threat surfaces and build security into their delivery pipelines with VMware Aria solutions. These include VMware Aria Automation, VMware Aria Automation for Secure Clouds, VMware Aria Automation Config, VMware Aria Operations, VMware Aria Operations for Networks, and VMware Aria Operations for Logs.

In addition to securing configurations to manage risk and streamline compliance, VMware Aria solutions empower organizations to simplify cloud cost and capacity management, optimize performance, and accelerate delivery automation.

Learn more at www.vmware.com/go/aria.

Item No: vmw-sol-brief-secure-configurations-compliance-v5 1/23