VMware Advanced Cyber Compliance

Elevated cyber risk management and compliance for VMware Cloud Foundation

An organization's ability to withstand cyber risk and manage compliance is a cornerstone of its ability not to succeed, but to survive. In today's modern threat landscape, plagued by ever-evolving cyberattacks and increasingly stringent regulations, the path to enabling robust security, resiliency and compliance enforcement is beset with challenges.

Today, IT teams face the daunting task of running these mission-critical operations with limited visibility, extensive manual intervention, and lack of advanced tools. And even if they do have the right resources in place, the integration process of point products from different vendors exposes them to unaddressed gaps, hinders their ability to efficiently allocate IT resources and ultimately results in financial loss in the form of fines, data loss or many other undesirable consequences.

VMware Advanced Cyber Compliance (ACC) is engineered to solve these pressing challenges. It combines the power of VMware by Broadcom's proven technologies to deliver unmatched cyber risk management and compliance for VMware Cloud Foundation environments.

Key Benefits

- **Enforce security** – Compliance drift detection and remediation. The ability to remediate critical security issues across private clouds with powerful remediation automation.
- **Maintain compliance** – Use 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.

Continuous Compliance Enforcement at Scale

Desired state monitoring and remediation powered by VMware Salt

To enable continuous compliance enforcement at scale, VMware Advanced Cyber Compliance is powered by VMware Salt to provide configuration checks with remediation, compliance, and vulnerability management for private cloud compliance and vulnerability remediation. With VMware Salt, SecOps teams can work together to define a corporate IT security policy, scan systems against it, detect vulnerabilities and non-compliance issues, and actively remediate the infrastructure.

Chasing compliance drift on existing systems is challenging. VMware Stack actively scans for compliance drift and provides automated remediation to enforce defined security policies—saving resources, improving security posture, and reducing risk.

It 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.

Key Benefits

- **Reduced attack surface** exposed to any potential cyber threats
- **Simplified compliance** with reduced time spent in auditing dependencies
- **Improved efficiency** with applications running lighter and deployed faster

Key Benefits:

- **1-Minute RPOs** with enhanced vSphere replication
- **Automated testing** of recovery plans and audit reports
- **Orchestrated restore** for 1000s of VMs with one click
- **Customizable policies** to perform recovery operations

Reduced attack surface with secure-by-design container images

Chiseled Ubuntu containers enhance security, simplify compliance, and improve operational efficiency in deploying workloads. Chiseled containers include only the minimum required dependencies like libraries or drivers reducing the container image size. For example, chiseled containers for applications like .NET and Java have image size that is 50% or smaller than the normal Ubuntu image.

Automated Cyber and Disaster Recovery

Recovering data in the face of any threat that could hinder its availability is essential for any organization's ability to continuously operate and remain compliant. VMware Advanced Cyber Compliance enables customers to confidently and quickly recover from cyberattacks, traditional disasters and operational failures. It integrates all the capabilities needed to orchestrate, automate and streamline recovery operations across on-premises VCF sites at scale.

The capabilities included as part of this VCF advanced service extend beyond the individual value of its components to strengthen platform resilience. Disaster recovery with RPOs as low as 1-minute powered by enhanced vSphere replication enables customers to minimize data loss for their mission-critical applications. They can also customize replication, protection and retention levels of their snapshot copies seamlessly from a single operating panel. All this can be done at a scale of thousands of VMs to enable protection for large enterprise environments. Operational recovery can also be done using vSAN data protection, which is already included in core VCF entitlements but complements the value of VMware Advanced Cyber Compliance.

VMware Advanced Cyber Compliance also enables customers to protect and recover data stored in on-premises VCF sites in the face of modern cyberattacks. IT teams benefit from next-generation validation tools to identify clean restore points, a VCF isolated clean room with push-button network isolation, as well as non-disruptive testing and restore point iterations. Cyber recovery across on-premises VCF sites is currently available as a VMware Validated Solution.

Enhanced Platform Security and Incident Response

Reduced attack surface with secure computing

Confidential computing addresses the trust gap in computing, between workloads and the hardware platforms. With confidential computing technologies, we can replace this implicit trust on the underlying hardware platform with actual tests to ensure that the platform is trustworthy. Techniques such as encrypting workload data in memory are especially helpful in shared and multi-tenant environments. VMware Advanced Cyber Compliance enables support for Intel and AMD confidential computing technologies like Intel TDX and AMD SEV-SNP, allowing attestation of computing platforms and the workloads, as well as enabling data-in-use encruption in memory and inside CPUs.

Key Benefits:

- **Reduced attack surface**, limiting access and enforcing integrity protections, thereby reducing the amount of trust needed in hardware
- **Protection** against leaky security boundaries in CPU and memory
- **Secure isolation** between workloads, enabling sharing and collboration in shared environments
- **Maintain** regulatory compliance

Reliable visibility into security health with proactive assessments

The proactive compliance assessments ensure that VMware Advanced Cyber Compliance customers receive comprehensive, actionable insights derived from an in-depth examination of collected log bundles. These assessments equip customers with valuable and actionable intelligence from the Proactive Support team to maintain a healthy and optimized environment, improving resiliency, reliability, and security.

The reports cover the following areas:

- **VMware Security Vulnerabilities:** Identify potential risks and provide actionable guidance, based on deployed versions.
- **Upgrade Recommendations:** Suggest timely updates to maintain optimal performance and compatibility.
- **Certificate Expiration Notifications:** Alert on upcoming expirations to ensure uninterrupted operations.
- **Firmware & Driver Validation:** Verify all versions against compatibility guides and provide necessary recommendations.
- **Additional Insights:** Include any other relevant information, features, or steps as needed to optimize the environment.

Expanded incident response

VMware Advanced Cyber Compliance customers receive 10/7 support for Severity 2 issues, in addition to 24/7 support for Severity 1 issues. This ensures that Severity 2 issues can be addressed by Broadcom support as they arise, seven days a week.

Scheduled IT activities, such as upgrades, disaster recovery testing, and compliance reviews, frequently occur during weekends. For unforeseen issues of lesser criticality that arise during such activities, customers can engage with Broadcom support, even on weekends.

Ready to learn more about VMware Advanced Cyber Compliance? Visit our webpage or contact one of our Sales Representatives.

vmware® by Broadcom

Item No: Advanced Cyber Compliance_V3 11/25