VMware SASE Security Assessment Service

At a glance

VMware SASE Security Assessment assesses the configuration and alerts of every SASE component to ensure the optimal stealth security of the implementation.

Key benefits

- Confidence that deployment and Operations are secure
- Potential discovery of security risks
- Recommendations to harden your VMware SASE deployment

Pricing and scoping

The VMware SASE Security Assessment Service will be delivered remotely and will include the security assessment of the SASE components (Orchestrator, Gateway, Edges and Cloud Web Security). For pricing, please contact your local VMware representative.

For more information

For more information about this service, please reach out to your local VMware representative.

Terms and conditions

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware Professional Services General Terms and Conditions.

www.vmware.com/files/pdf/services/tc.pdf

The VMware SASE Security Assessment Service ensures. the deployment and operation of your VMware SASE implementation aligns with VMware's security best practices.

Note: This service requires VMware SASE Orchestrator access.

The VMware SASE Security Assessment Service includes the following:

Analysis of current implementation

The following activities will help us analyze the current implementation and configuration of the VMware SASE components and provide a set of recommendations for hardening existing and new SASE services.

VMware SASE Security Assessment

VMware team will conduct a review of the VMware SASE deployment. This will include a security assessment of the different SASE components:

- VMware SASE Orchestrator
- VMware SASE Gateways
- VMware SASE Edges

VMware Cloud Web Security

Assess the security policies implemented in accordance with best practices and security governance of the enterprise. This would include:

- SSL inspection
- URL filtering
- Content filtering
- Content inspection

Proposed next steps

Review the outcomes and remediation recommendations, if any, resulting from the above listed activities.

VMware will provide a report outlining identified issues and any potential vulnerabilities and/or potential defects in order to mitigate the attack surface.