WHITE PAPER

Threatwise™

Security Architecture and Overview

The following document provides a detailed look at the key components of Threatwise security posture and architecture.

WHITE PAPER

About Threatwise

Commvault® Cloud Threatwise, delivers early warning cyber detection to surface external and internal attacks—before they reach your data. Using patented cyber deception technology, Threatwise simulates real resources using indistinguishable decoys (called threat sensors), to provide highly accurate alerts into threats before data encryption, exfiltration, or damage. With Threatwise, Commvault customers can proactively identify silent threats, minimize exposure, and respond sooner to avoid damage. For more information on Threatwise, please visit the following webpage.

THREATWISE ARCHITECTURE

Threatwise is architected for scale and performance:

The TSOC: Short for Threatwise Security Operations Console, the TSOC runs in the cloud and provides a web-based interface for user access. From the TSOC, users can deploy, configure, and administer the features and functionality of Threatwise.

The Appliance: Appliances are the primary mechanism for projecting Threat Sensors (or decoys) within your environment. Appliances can be deployed on-premise or in the cloud, both as a small, lightweight virtual image or hardware for sites requiring fanless systems (e.g., manufacturing floors). These Appliances directly interface with the TSOC, allowing you to set up, manage, and optimize these decoys to your data across on-premises, public cloud, or private cloud environments. The Threatwise Appliance image is hardened using CIS Level 1 hardening benchmark.

DATA RESIDENCY

Threatwise is a passive solution that captures minimal customer data. No information is collected from real customer assets themselves, as Threatwise only captures metadata associated with or used during an attack (e.g., IP and MAC addresses). All metadata captured is stored on the Appliance and remains within the customer's environment. Logs for detected incidents are captured and sent to the TSOC over encrypted links. To satisfy residency requirements, laws, and regulations, all metadata stored in the TSOC (such as alert notifications, setup, and configuration details) automatically reside in the Azure data center region nearest to where the TSOC is deployed.

IMMUTABILITY

Commvault leverages a hardened, multi-layered approach to data protection, providing robust controls that prevent various types of threats on logs and other metadata, ensuring full fidelity of required data. Natively, all data is protected at the storage level. All log data in the TSOC lives in a virtually air-gapped location, in an isolated security domain, decoupled from source environments. Multi-factor authentication, dual AES 256-bit at-rest encryption, firewalls, and zero-trust access controls block internal and external movement of data by unauthorized parties. All security protocols adhere to security best practices and are based upon NIST 800-53, SOC2 type II, and ISO27001:2013 guidelines and compliance requirements.

The Appliance is deployed in the customer's environment. Only metadata is stored within the Appliance related to decoys and threat sensors. No production infrastructure information or critical data is stored in the Appliance or TSOC. The Appliance is hardened using CIS Level 1 hardening benchmarks with secured access using APIs, certificates, and tokens from the TSOC.

NETWORKING AND COMMUNICATIONS

All network communications are managed via TLS (mTLS) using TLS 1.2 connections. Certificate generation, revocation, and renewal are automatically managed. Control connections from on-premises components to the Threatwise service control plane are outbound only over port 443, minimizing the network access necessary to leverage Commvault. Connections to cloud storage also use HTTPS on port 443 outbound only. All communication between the Appliance and TSOC is always encrypted in transit.

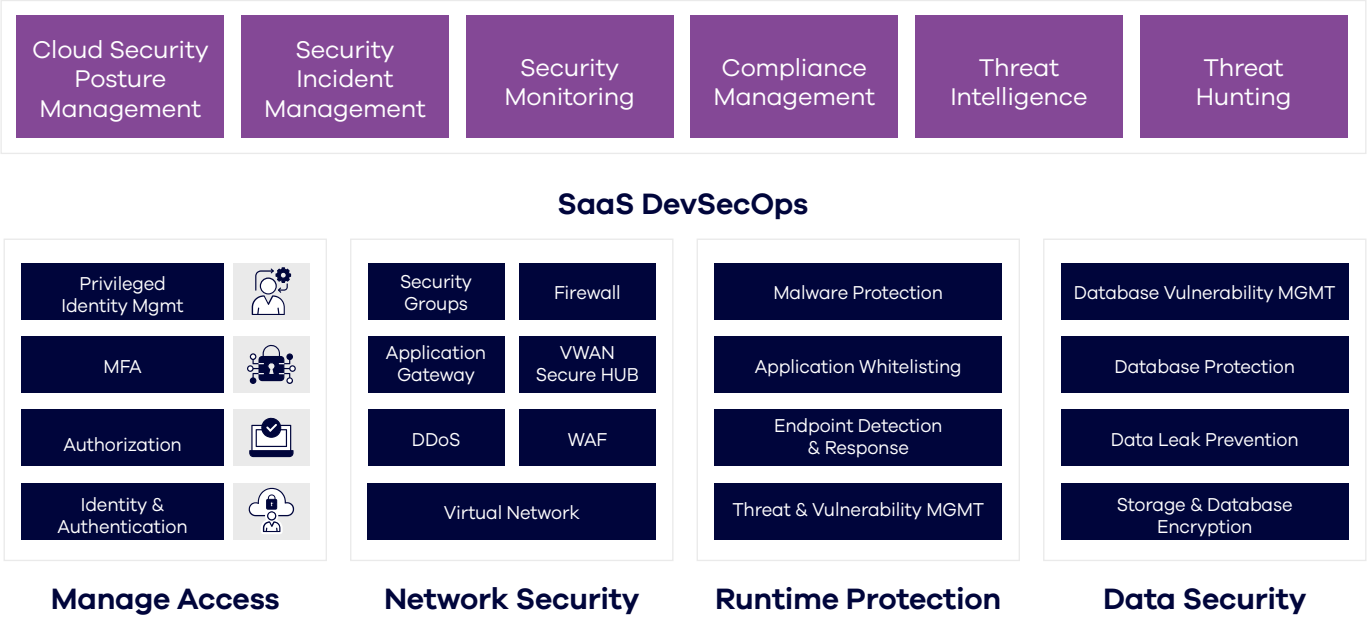
APPLICATION SECURITY

Commvault employs a DevSecOps approach to enhance end-to-end information and operational security. This includes following industry best practices to isolate test, dev, staging, and production environments. Testing and review for security risks are performed regularly by both in-house and external third parties, including routine penetration testing, red team activities, vulnerability assessments, and system and process audits.

To prevent unauthorized or malicious access, Threatwise service deployment uses layered security, including firewalls, WAF, and MFA. Application Security assessments and vulnerability checks are regularly performed to maintain security hygiene and posture. Commvault also follows Open Web Application Security Project (OWASP) Top 10 best practices to secure web services and APIs and maintains SOC2 Type II and ISO.IEC 27001:2013 certifications.

Security updates are automatically applied to Threatwise on a regular cadence. Security updates are also seamlessly pushed to customer Appliances without user intervention.

SECURITY ARCHITECTURE



DATA SECURITY

Separate Security Domain

Threatwise leverages a 100% cloud-native architecture in a separate security domain from the customer and Commvault security boundaries. One-way, TLS-encrypted secure tunnels are used without a physical network connection.

Data Segregation

Threatwise is a secure-by-design SaaS offering. While using Threatwise, no actual customer data is captured or stored. Metadata generated by Threatwise is isolated and stored in virtually air-gapped locations, with unique data encryption keys per customer. Commvault also leverages zero-trust access controls, only permitting owners (customer) access through the Threatwise service.

Data Access

Metadata within Threatwise is not accessible or readable by Commvault employees. Access to metadata stored within Threatwise is solely subject to policies and authorized user permissions established and managed by the customer.

Data Owner Right to Delete Data

Any log and metadata stored can be permanently deleted, so it is no longer available for usage and review. Requesting to delete metadata can only be made by customers using appropriate channels, including their dedicated Customer Success Manager or the Commvault Support Team. Once metadata has been securely deleted, it cannot be restored.

IDENTITY AND ACCESS MANAGEMENT

Access control is based on the Principle of Least Privilege according to Zero-Trust models and is designed to limit privileged and unauthorized access to both data and service infrastructure. We employ industry-standard security best practices aligned to NIST 800-53 security guidelines for all access to our services with tight audit- controls managed via best-in-class security and DevSecOps tools, services, and processes.

User Application Access

Passwords

Threatwise supports SAML 2.0 and MFA authentication, allowing customers to implement their password management controls and policies. Password complexity is enabled, requiring at least 12 characters, using three unique characters, and cannot contain more than two characters from the username. Password change frequency is 42 days, and at least three past password histories are logged. Threatwise uses lockbox and vaults to secure customer passwords and credentials.

Logon Attempts

Administrators can limit the times a user can attempt to logon to Threatwise. After the limit is reached, the user account is locked for the time period defined by the administrator. For more information, see Limiting User Logon Attempts.

Two-Factor Authentication

When Two-Factor Authentication is activated, users must enter a 6-digit PIN (Personal Identification Number) along with their passwords to access Threatwise.

SAML Support

Threatwise supports SAML authentication. SAML can be used to create a single identity for each user for a single sign-on logon for all applications. A SAML User Registration Workflow is available to create usernames.

Privacy

Threatwise prevents users and administrators who are not tenant owners from seeing the data on the client. This includes Commvault employees and personnel who do not have access to customer data.

Infrastructure Access

Physical Access

Threatwise is a Software as a Service utilizing the cloud's shared responsibility model. Commvault helps ensure all data and access to the data is secured while leveraging the cloud service provider for perimeter and physical access controls. Threatwise operates within data centers that are hosted by Microsoft Azure, and verifies annual attestation of such hosting services by AICPA (SSAE 18) and ISO-qualified auditors. Customers are responsible for ensuring appropriate controls are implemented to prevent unauthorized access to the Appliance deployed in their environment, as well as appropriate security controls implemented for SAML/AD environments.

GOVERNANCE AND RISK MANAGEMENT

Commvault is ISO27001:2013 and SOC 2 Type II compliant, maintaining and implementing industry-standard security and privacy policies aligned to NIST 800-53 security guidelines. Best-in-class cloud and SaaS service configuration management tools are employed to ensure any deviations from configurations detected are remediated automatically. All access is logged for audit and compliance reasons. Compliance with information security policies and procedures is strictly enforced, and all Commvault's employees receive training to ensure they remain aware of their role in maintaining the security, availability, and confidentiality of customer data, among other job responsibilities.

Audit Trail
Commvault audit trails allow customers to track user actions within Commvault services and can help determine the root cause or source of operations performed within the environment. All changes are logged per Commvault SRE and DevSecOps requirements and follow SOC2 Type II and ISO27001:2013 compliances and standards.

Incident Response Plans
Commvault has a comprehensive Incident Response Plan (IRP) program, tested annually by a certified third party as part of our normal ISO and SOC2 certification requirements. Daily scanning is performed and procedures are tested through internal and external audits.

Business Continuity
Commvault Disaster Recovery (DR) procedures are based on the Commvault Business Continuity and Disaster Recovery (BCDR) policies. The DR procedures encompass all production services within Threatwise, are well established, reviewed every year, and continuously enhanced at scale to support our customers.

GDPR
When providing services, Commvault ensures compliance with specific GDPR requirements for data processors. When third parties are appointed to act as sub-processors, appropriate terms are in place to comply with the GDPR and safeguard customers' data. Please see our GDPR Compliance page for more details.