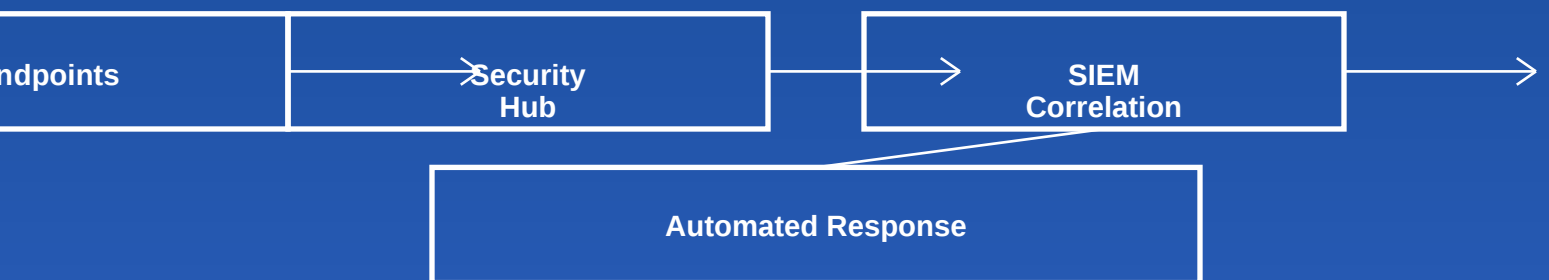


VCS One Security

Integration Guide

Security Setup & Integration Instructions



Quick Deployment

Automated Installation

VCS One Security offers multiple deployment options depending on your organization size and requirements.

Starter Edition

Designed for small organizations with up to 100 endpoints. Quick setup with minimal configuration.

- Run the automated installation script from the portal
- Configure admin credentials and organization details
- Deploy agent automatically to endpoints via domain policy or MDM
- Set up initial security policies from pre-built templates
- Enable automated updates and monitoring

Professional Edition

For medium-sized organizations with 100-1000 endpoints. Enhanced features and customization options.

- Install management console on dedicated server or cloud instance
- Configure multi-region deployment for geographic redundancy
- Set up integration with existing Active Directory/LDAP
- Deploy agents using SCCM, Intune, or custom deployment scripts
- Configure custom security policies and compliance frameworks
- Enable advanced threat detection and behavior analytics

Enterprise Deployment Process

Large-scale deployment for enterprises with 1000+ endpoints across multiple environments.

- Phase 1: Infrastructure setup with HA clustering for management console
- Phase 2: Network architecture configuration with dedicated security zones
- Phase 3: Integration with existing security stack (SIEM, IDS, firewalls)
- Phase 4: Staged agent rollout: IT infrastructure → servers → endpoints → BYOD
- Phase 5: Pilot testing with 10% of endpoints for validation
- Phase 6: Full deployment with monitoring and performance tuning
- Phase 7: Documentation, training, and handoff to operations team

Agent Deployment Across Endpoints

Automated and manual deployment options for diverse endpoint environments.

- Windows:** Group Policy, SCCM, Intune, Powershell scripts, MSI installer
- Linux:** Package managers (apt, yum, dnf), Ansible playbooks, systemd service
- macOS:** Jamf, Munki, MDM profiles, Apple PKG installer
- Cloud Instances:** Terraform, CloudFormation templates, startup scripts
- Containers:** Kubernetes DaemonSets, Docker sidecar, deployment manifests

Network Scanning Configuration

Automated discovery and scanning of network assets for comprehensive visibility.

- Automated network discovery using ARP, SNMP, WMI, SSH for asset enumeration
- Vulnerability scanning with credentialed and agent-based scans
- Port scanning and service enumeration for exposure assessment
- Continuous monitoring with scheduled weekly/daily scans
- Custom scan policies with whitelisting for critical systems

Initial Security Baseline

Establish starting point for security posture measurement.

- Run comprehensive discovery scan across all networks
- Identify and categorize all assets with business criticality
- Perform initial vulnerability assessment and risk scoring
- Document current security configurations and policies

Establish compliance baseline against selected frameworks

SIEM Integration

Splunk Connector Setup

Integrate VCS One Security with Splunk for centralized security monitoring and correlation.

Installation Steps

- Download Splunk universal forwarder and install on VCS One Security server
- Configure forwarder with index name and destination Splunk server details
- Install VCS One Security Splunk add-on from app catalog
- Configure data inputs for security events, alerts, and compliance data
- Create index-time and search-time field extractions for parsing
- Validate data flow with test searches and sample queries

Configuration Files

```
inputs.conf: [vcs:security:events] index = security_events sourcetype = vcs:security source =  
vcsone-security
```

QRadar Integration

Connect with IBM QRadar for advanced threat detection and security orchestration.

- DSM Installation:** Deploy VCS One Security DSM (Device Support Module) on QRadar
- Log Source Configuration:** Create custom log source with protocol UDP/TCP, port configuration
- Event Parsing:** Configure regex-based parsing for event normalization
- Offense Rules:** Create QRadar offenses for high-risk security events
- Dashboards:** Build custom dashboards for VCS One Security data visualization

Log Forwarding Configuration

Syslog and API-based log forwarding to SIEM platforms.

Syslog Forwarding: Configure syslog targets (UDP/TCP/TLS) with custom formats (CEF, LEEF, JSON)

API Integration: REST API for near real-time event streaming with OAuth authentication

Filtering: Event filtering by severity, category, source to reduce log volume

Retry Logic: Automatic retry with exponential backoff for failed log deliveries

Compression: Gzip compression for network bandwidth optimization

Event Correlation Rules & Dashboard Configuration

Build correlation rules and dashboards for security monitoring.

Correlation Rules: Create rules detecting multi-stage attacks, lateral movement, privilege escalation patterns

Time Windows: Define temporal correlation windows for related events

False Positive Tuning: Whitelist known-good patterns reducing alert noise

Dashboard Configuration: Build executive, operational, and tactical dashboards

KPI Widgets: Track mean time to detect (MTTD), mean time to respond (MTTR), threat metrics

Alert Routing: Route high-severity alerts to SOC, email, Slack, PagerDuty channels

Identity & Access Integration

Okta Integration

Seamless single sign-on and user provisioning with Okta.

SSO Configuration

- Create Okta SAML application for VCS One Security in Okta admin console
- Configure SAML assertions with required attributes (email, groups, roles)
- Copy SAML metadata or configuration details to VCS One Security
- Configure VCS One Security as service provider with IdP metadata URL
- Test SSO flow with test user before enabling for all users

User Provisioning

Automated user lifecycle management via SCIM (System for Cross-domain Identity Management).

- Enable SCIM provisioning in Okta application settings
- Generate SCIM bearer token from VCS One Security admin panel
- Configure user attribute mapping (username, email, groups, roles)
- Set up group provisioning for role-based access control
- Enable automatic deprovisioning for disabled/deleted users

MFA Setup

Multi-factor authentication enforcement via Okta Verify or TOTP authenticators.

- Enable MFA enforcement for VCS One Security application in Okta
- Configure MFA policy: prompt for MFA on every login or based on conditions
- Set up backup methods: SMS, email, security questions
- Integrate with hardware tokens and biometric authenticators
- Test MFA flow with primary and backup methods

Azure AD Integration

Microsoft Entra ID (Azure AD) integration for enterprise identity management.

Identity Synchronization

Enterprise Application: Register VCS One Security as enterprise app in Azure AD

SAML SSO: Configure SAML-based single sign-on with certificate upload

Attribute Mapping: Map Azure AD attributes (UserPrincipalName, DisplayName, Groups) to VCS One attributes

User Assignment: Assign users and groups to application, enable automatic account provisioning

Conditional Access: Set up device compliance checks, location-based policies

Conditional Access & Role Mapping

Conditional Access Policies: Require MFA, managed devices, trusted networks for VCS One access

Device Compliance: Integrate with Intune for device compliance checks

Role Mapping: Map Azure AD groups to VCS One Security roles (Admin, Analyst, Viewer)

Dynamic Groups: Use Azure AD dynamic groups based on department, location, attributes

Audit Logging: Track sign-ins, MFA challenges, policy evaluations in Azure AD logs

Cloud Security Integration

AWS Security Hub

Centralize security findings from AWS services into VCS One Security.

Integration: Create VCS One Security product integration in Security Hub

Finding Format: Send findings in AWS Security Finding Format (ASFF) with custom severity mapping

Real-Time Sync: Publish findings via Security Hub BatchImportFindings API

Insights: Create custom insights in Security Hub for VCS One Security findings

Automation: Configure AWS EventBridge rules for automated response to findings

Azure Security Center

Integrate with Microsoft Defender for Cloud.

Connector API: Use Azure Security Center API to fetch security recommendations and alerts

Security Findings: Map VCS One Security findings to Security Center security score

Workflow Automation: Azure Logic Apps for automated remediation workflows

Continuous Export: Stream security findings to Azure Event Hub or Log Analytics

Compliance Assessment: Integrate with compliance dashboards in Security Center

GCP Security Command Center & CloudTrail/Logs Integration

Google Cloud Platform security monitoring and integration.

Security Command Center: Create custom findings via SCC API for cloud resource security issues

Cloud Logging: Export logs from Cloud Logging to VCS One Security via log sinks

CloudTrail Equivalent: Integrate Cloud Audit Logs for user activity and API call monitoring

Resource Scanning: Scan GCP resources using Cloud Asset Inventory API

BigQuery Integration: Export security findings to BigQuery for analytics

CloudTrail/Logs Integration & Resource Scanning

Stream CloudTrail events to VCS One Security for AWS user activity monitoring

Ingest CloudWatch Logs via Kinesis Firehose delivery stream for log analysis

Configure Azure Monitor log forwarding to VCS One Security via Event Hub

Set up GCP Cloud Logging export to Pub/Sub with cloud functions for transformation

Implement continuous cloud resource scanning with change detection and alerting

Incident Response Setup

Playbook Creation

Define structured response procedures for common security incidents.

- Create playbook templates for malware, phishing, data breach, insider threat scenarios

- Define severity levels (Critical, High, Medium, Low) with response SLAs

- Document step-by-step investigation procedures with decision trees

- Specify automated actions (quarantine, block, notify) for immediate containment

- Assign responsibility matrices with escalation paths

Response Team Configuration

Configure incident response teams with roles, responsibilities, and availability.

- Team Structure:** Define team roles: Incident Manager, Security Analyst, Forensics Specialist, Communications Lead

- On-Call Rotation:** Configure rotation schedules with escalation chains

- Contact Methods:** Primary (phone, Slack) and secondary (email, SMS) contact methods

- Availability:** Define business hours vs. after-hours response procedures

Notification Setup

Multi-channel alerting for incident notification and updates.

- Email Notifications:** HTML template emails with incident details, severity, playbook links

- Slack/Teams Alerts:** Real-time notifications with rich formatting, action buttons, threading

- PagerDuty:** Critical incident escalation with phone calls, SMS

- SMS Text:** Backup communication channel for critical incidents

- Custom Webhooks:** Integration with ticketing systems, ITSM platforms

Jira Ticket Automation & Escalation Procedures

Automated ticket creation and management for incident tracking.

Incident Tickets: Auto-create Jira tickets from security alerts with severity, affected assets, evidence

Status Sync: Update VCS One Security incident status based on Jira ticket state changes

Comment Sync: Bidirectional sync of comments between VCS One and Jira

Custom Fields: Map VCS One attributes to Jira custom fields (CVSS score, business impact)

Assignment Rules: Auto-assign tickets to security team based on classification

Escalation Procedures

Define escalation triggers: no response within SLA, severity increase, executive impact

Configure escalation paths: Analyst → Team Lead → CISO → Executive Team

Set up automated escalation reminders with countdown timers

Implement dual-approval workflows for critical containment actions

Document after-hours escalation to on-call managers

Compliance Automation

Streamlined compliance management with automated evidence collection and reporting.

Framework Selection

Select applicable frameworks: PCI-DSS, ISO 27001, SOC 2, GDPR, HIPAA, NIST CSF

Import framework control catalogs from VCS One Security library

Customize controls for industry-specific requirements

Map existing security controls to framework requirements

Control Mapping & Continuous Monitoring

Control Mapping: Link security controls, policies, evidence to framework requirements

Automated Evidence: Screenshots, log exports, configuration snapshots captured on schedule

Continuous Monitoring: Real-time compliance status with automated alerting for violations

Remediation Tracking: Issue management with deadline enforcement and progress tracking

Report Generation: Automated monthly/quarterly compliance reports with executive summaries

Audit Preparation

Pre-populate auditor questionnaires with automated evidence links

Generate pre-audit checklist with compliance gaps and remediation recommendations

Prepare evidence packages with organized documentation and metadata

Schedule mock audits to validate preparedness and identify improvements

Security Support

- **Documentation:**
<https://vcsmv.com/security/docs>
- **Best Practices:**
<https://vcsmv.com/security/guides>
- **Video Tutorials:**
<https://vcsmv.com/security/videos>
- **Community Forum:**
<https://vcsmv.com/community>
- **24/7 Support:**
support@vcsmv.com

Value Creating Solutions Sdn Bhd

<https://vcsmv.com> | support@vcsmv.com