ASIMILY

Technical Architecture Report

Detailed Analysis of Platform Architecture, Deployment Models, Integration Capabilities, and Implementation Best Practices

Report Date: February 05, 2026

Version: 1.0 | Classification: Confidential

SYSTEM ARCHITECTURE

Platform Components

The Asimily platform consists of four core architectural components that work together to provide comprehensive cyber asset and exposure management capabilities. These components are designed to operate in diverse network environments while maintaining security and performance requirements.

1. Data Collectors

Data Collectors are lightweight appliances or software agents deployed within customer networks to gather device information through multiple discovery methods. Collectors support both physical appliance and virtual machine deployment formats.

- Passive Network Monitoring: SPAN port or network TAP integration for traffic analysis
- Protocol-Based Discovery: Native protocol communication (SNMP, WMI, SSH, Modbus, DICOM)
- API Integration: Direct integration with network infrastructure and management systems
- Agentless Operation: No software installation required on managed devices

2. Processing Engine

The Processing Engine applies patented AI/ML algorithms and Asimily Labs research to transform raw device data into actionable intelligence. This includes vulnerability correlation, risk scoring, and prioritization analysis.

- Real-time processing of device discovery and change events
- MITRE ATT&CK framework mapping for attack vector analysis
- Risk scoring algorithms incorporating device context and exploitability
- Automated identification of compensating controls and mitigations

3. Management Console

The web-based Management Console provides the primary user interface for security teams, offering dashboards, reporting, configuration management, and workflow tools.

- Role-based access control with multi-tenant support
- Customizable dashboards and reporting templates
- Integration APIs for SIEM, SOAR, and ticketing systems
- Mobile-responsive design for on-the-go access

4. Remediation Services

Remediation Services provide active risk reduction capabilities including network segmentation guidance, configuration management, and automated patching workflows.

- Network policy generation for microsegmentation implementation
- Configuration backup, comparison, and restoration services
- Firmware validation and safe deployment orchestration
- Password management and credential rotation services

DEPLOYMENT MODELS

On-Premises Deployment

On-premises deployment provides maximum control and is suitable for organizations with strict data sovereignty requirements or air-gapped networks. All platform components run within customer-managed data centers.

- Complete data retention within customer environment
- No external connectivity required for core functionality
- Integration with existing backup and disaster recovery systems
- Customizable update schedules for maintenance windows

Cloud Deployment (SaaS)

The SaaS deployment option reduces infrastructure overhead while maintaining security through encrypted communications and customer data isolation.

- Automatic platform updates and feature releases
- Elastic scaling based on device volume and network complexity
- 99.9% uptime SLA with redundant infrastructure
- Multi-region availability for latency optimization

Hybrid Deployment

Hybrid deployment combines cloud-based management with on-premises data collection, offering a balance between operational flexibility and data control.

- Local collectors for sensitive network segments
- Cloud-based analytics and management console
- Encrypted tunneling for secure data transmission
- Flexible configuration for regulatory compliance

Air-Gapped Deployment

Air-gapped deployment supports highly secure environments without internet connectivity, using manual update processes and isolated infrastructure.

- Complete isolation from external networks

- Offline update mechanisms via secure media transfer
- Full functionality without cloud dependencies
- Suitable for critical infrastructure and classified environments

INTEGRATION ARCHITECTURE

SIEM Integration

Asimily integrates with leading Security Information and Event Management platforms to enrich security operations with IoT/OT-specific context and threat intelligence.

- Splunk: Native app with pre-built dashboards and correlation searches
- IBM QRadar: Custom DSM support for device event parsing
- Microsoft Sentinel: Data connector with KQL query templates
- LogRhythm: Open Collector integration for log forwarding
- Syslog: Standard syslog format for universal SIEM compatibility

SOAR Integration

Security Orchestration, Automation and Response integration enables automated workflows for device incident response and remediation actions.

- Palo Alto XSOAR: Pack with playbooks for IoT incident response
- Splunk SOAR: Custom actions for device quarantine and isolation
- ServiceNow SecOps: Vulnerability response workflow integration
- REST API: Generic webhook support for custom SOAR platforms

Network Infrastructure

Direct integration with network infrastructure enables automated device discovery, segmentation policy deployment, and network access control.

- Cisco: ISE, DNA Center, and switch integration via APIs
- Aruba: ClearPass and switch configuration management
- Juniper: Mist and EX switch series support
- HPE: Network automation for ProCurve and Comware platforms
- Generic: SNMP and CLI-based management for vendor-agnostic support

IT Service Management

ITSM integration ensures device security activities align with existing change management and incident response processes.

- ServiceNow: Bi-directional integration for CMDB sync and ticketing
- BMC Remedy: Automated ticket creation for high-risk vulnerabilities
- Jira Service Management: Issue tracking for remediation workflows
- Cherwell: API-based integration for asset and ticket management

API REFERENCE

REST API Overview

Asimily provides a comprehensive REST API for programmatic access to platform capabilities, enabling custom integrations and automated workflows.

```
Base URL: https://api.asimily.com/v1
Authentication: OAuth 2.0 Bearer Token
Rate Limiting: 1000 requests/hour per API key
Content-Type: application/json
```

Key API Endpoints

Device Management:

```
GET    /devices              # List all devices
GET    /devices/{id}         # Get device details
GET    /devices/{id}/vulns   # Get device vulnerabilities
POST   /devices/query        # Advanced device search
```

Vulnerability Management:

```
GET    /vulnerabilities      # List vulnerabilities
GET    /vulnerabilities/{id} # Get vulnerability details
GET    /risk-score          # Calculate risk for devices
```

Reporting:

```
GET    /reports              # List available reports
POST   /reports              # Generate custom report
GET    /reports/{id}/export  # Download report (PDF/CSV)
```

SECURITY SPECIFICATIONS

Data Protection

Asimily implements comprehensive security controls to protect sensitive customer data throughout the platform lifecycle.

- Encryption at Rest: AES-256 for all stored data
- Encryption in Transit: TLS 1.3 for all communications
- Key Management: HSM-backed key rotation every 90 days
- Data Segregation: Customer-specific database schemas in multi-tenant deployments

Authentication & Authorization

Multi-layered authentication and granular authorization controls ensure appropriate access to platform capabilities.

- SSO Support: SAML 2.0 and OIDC integration (Okta, Azure AD, Ping)
- MFA Enforcement: TOTP and hardware token support
- RBAC: Role-based access control with custom role definitions
- Audit Logging: Comprehensive access logging for compliance reporting

Compliance Certifications

Asimily maintains current certifications for major security and privacy frameworks:

- SOC 2 Type II: Annual audit with 99.9% control effectiveness
- ISO 27001: Information security management system certification
- HIPAA: Business Associate Agreement (BAA) available
- GDPR: Data Processing Agreement (DPA) and EU data residency options

IMPLEMENTATION GUIDE

Pre-Deployment Requirements

Successful Asimily deployment requires network preparation and resource allocation before installation begins.

- Network Access: SPAN port or network TAP for passive monitoring (1 Gbps recommended)
- Compute Resources: 4 vCPU, 16GB RAM, 500GB storage per collector
- Network Connectivity: Outbound HTTPS (443) for cloud components
- Credentials: Read-only service accounts for target systems (SNMP, WMI, SSH)

Typical Implementation Timeline

Phase 1 - Discovery (Weeks 1-2):

- Collector deployment and network connectivity validation
- Initial device discovery and inventory compilation
- Baseline configuration establishment

Phase 2 - Analysis (Weeks 3-4):

- Vulnerability assessment and risk scoring
- Prioritization model tuning for environment specifics
- Integration configuration (SIEM, ticketing, CMDB)

Phase 3 - Remediation (Weeks 5-8):

- High-risk vulnerability mitigation
- Segmentation policy implementation
- Automated remediation workflow activation

Phase 4 - Optimization (Weeks 9-12):

- Workflow refinement and team training
- Reporting and dashboard customization
- Continuous improvement process establishment

BEST PRACTICES

Discovery Optimization

Maximize device discovery coverage while minimizing network impact through strategic configuration of discovery methods.

- Deploy multiple collectors for geographically distributed networks
- Use protocol-specific discovery for known device types (Modbus for OT, DICOM for medical)
- Schedule active scanning during maintenance windows for sensitive devices
- Maintain updated SNMP community strings and service account credentials

Risk Prioritization

Effective risk reduction requires focusing on vulnerabilities that pose actual threats to your specific environment.

- Customize risk scoring weights based on business criticality
- Use Risk Simulator before major remediation efforts
- Consider compensating controls when evaluating vulnerability severity
- Track mean time to remediate (MTTR) metrics by risk level

Operational Excellence

Maintain platform effectiveness through regular review and continuous improvement.

- Weekly review of newly discovered devices and vulnerabilities
- Monthly assessment of risk trends and remediation progress
- Quarterly platform health checks and integration testing
- Annual policy review and compliance assessment

CONCLUSION

The Asimily platform provides a technically robust solution for cyber asset and exposure management, with flexible deployment options, comprehensive integrations, and proven scalability for enterprise environments.

Successful implementation requires careful planning around network architecture, integration requirements, and operational workflows. Organizations that follow best practices for discovery, prioritization, and remediation typically achieve significant risk reduction within the first 90 days of deployment.

For detailed technical documentation, API specifications, and integration guides, contact Asimily support or access the customer documentation portal.

For technical support: support@asimily.com

Documentation: https://docs.asimily.com