AnySecura

Proactive Risk Alerts

Comprehensive threat detection and prevention platform

Identify · Analyze · Alert · Respond · Protect

Module Overview

AnySecura Proactive Risk Alerts combines three core capabilities to provide enterprises with advanced threat detection and prevention. By monitoring system activities, analyzing data flows, and managing endpoints, it identifies potential risks before they cause damage.

Early Warning Center

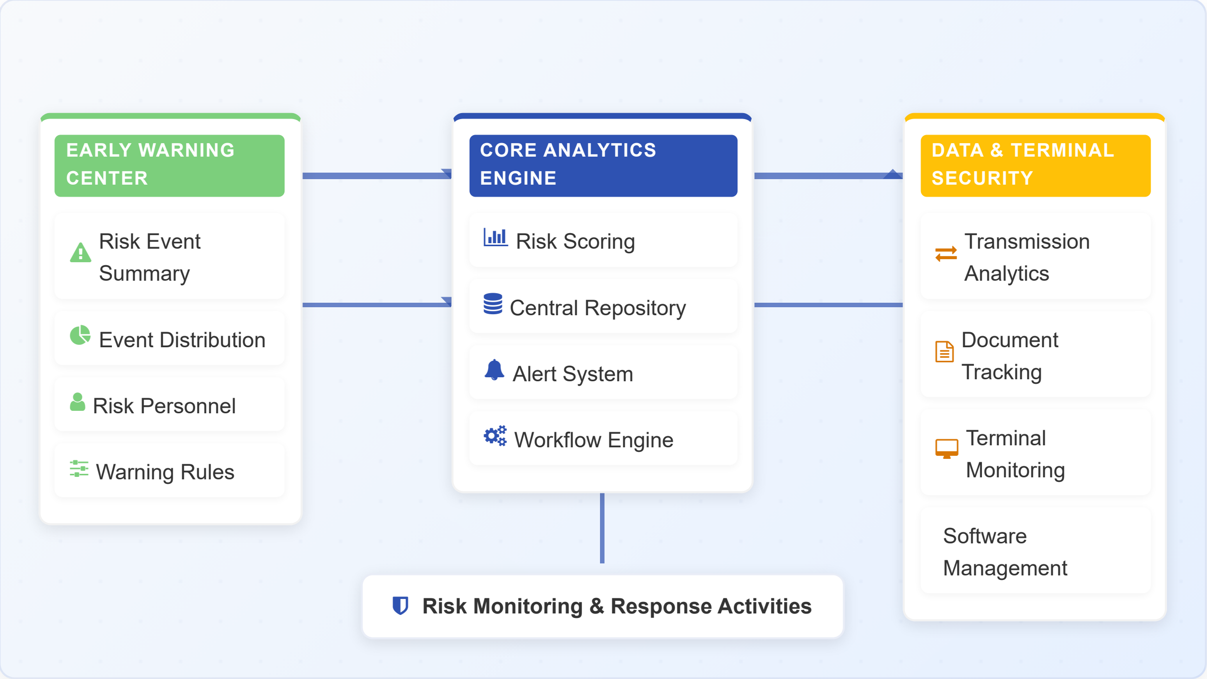
Centralized monitoring dashboard providing risk event summaries, level distribution, and detailed alerts. Configure warning rules based on event types, user behaviors, and file classifications with customizable sensitivity levels.

Data Security

Comprehensive tracking of data flows with outbound transmission statistics, channel distribution analysis, and detailed file trajectory mapping. Monitor document derivatives and maintain complete traceability of sensitive information.

Terminal Management

Complete visibility into software assets with operation statistics, usage tracking, and license management. Monitor installed applications, identify unauthorized software, and maintain software inventory with detailed usage metrics across all endpoints.

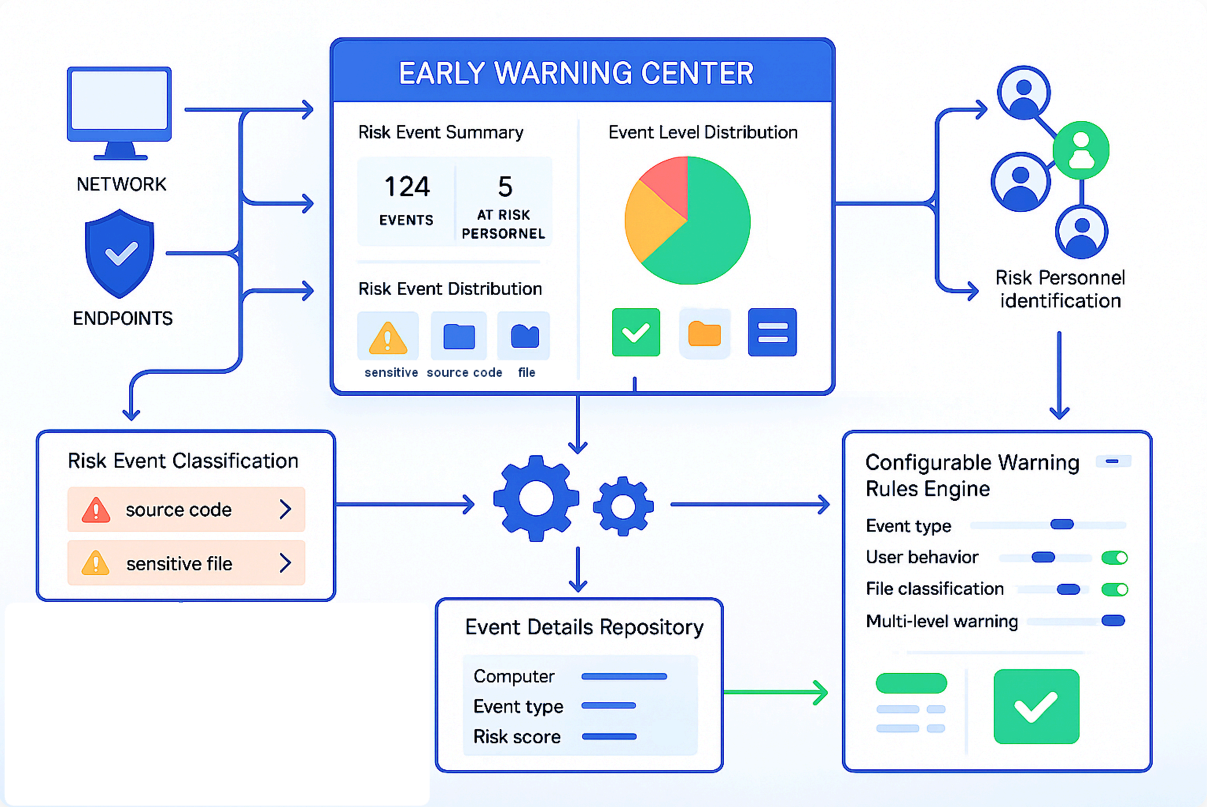


Early Warning Center

Required Integration: This module requires the **Document Operation Control Module** to be fully functional.

Centralized monitoring and alert system that identifies potential security risks before they escalate, providing actionable intelligence for proactive threat mitigation.

- **Risk Event Summary:** Comprehensive overview of total risk events, at-risk personnel counts, and classification by risk levels (high, medium, low).
- **Event Level Distribution:** Visual breakdown of security events by severity to prioritize response activities.
- **Risk Event Distribution:** Classification of predefined security events such as source code transmission via IM or sensitive file uploads.
- **Risk Personnel Identification:** Focused view of security events by individual users to quickly identify high-risk individuals.
- **Risk Event Details:** Comprehensive listing of security events with detailed metadata including computer information, event type, risk score, and file operation metrics.
- **Configurable Warning Rules:** Customizable alert parameters based on objects, event types, user behaviors, file classifications, and statistical cycles with multi-level warning thresholds.

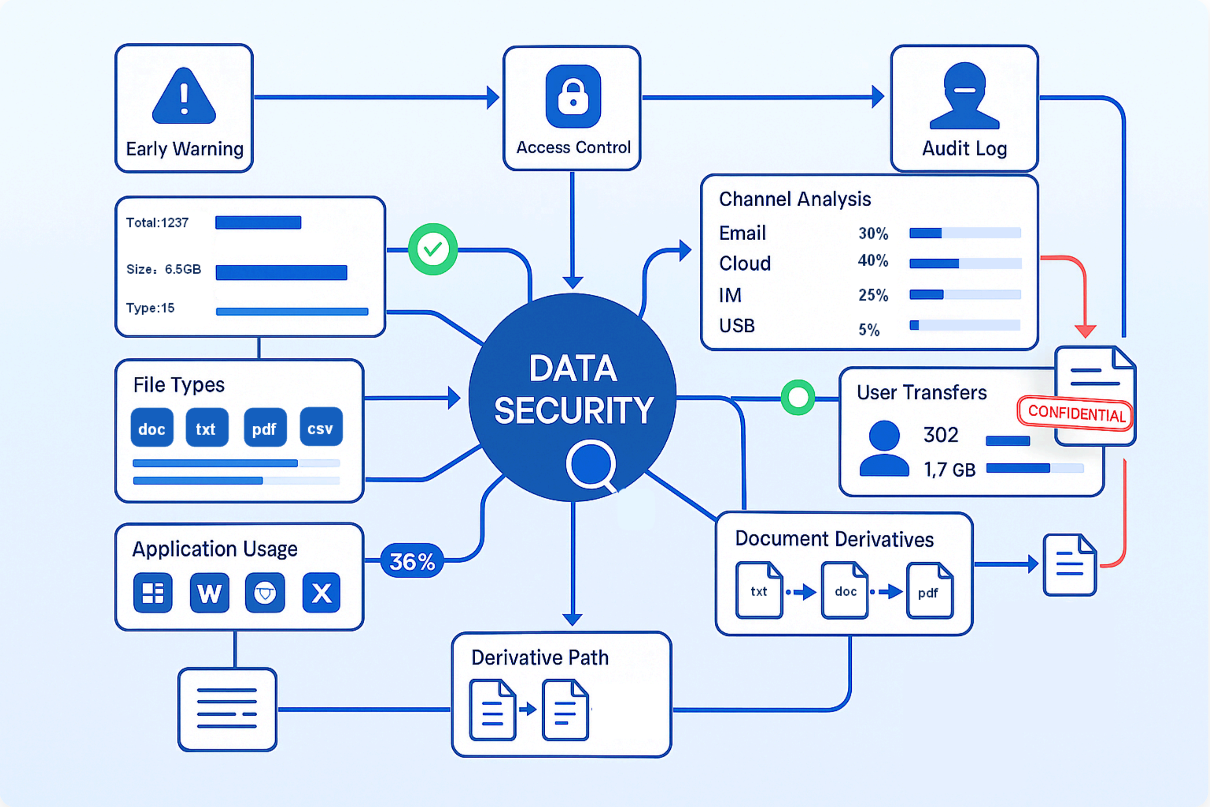


Data Security

Required Integration: This module requires the **Document Operation Control Module** to be fully functional.

Comprehensive monitoring and analysis of data flows to prevent unauthorized information leakage and maintain complete visibility of sensitive document movements.

- **Outbound Transmission Statistics:** Detailed metrics on document outflow including total count, size, and user involvement metrics.
- **Transmission Channel Analysis:** Quantitative assessment of data outflow through various channels to inform management strategies.
- **File Category Distribution:** Classification of outbound files by type for targeted audit and risk assessment.
- **User Transmission Statistics:** Tracking of individual user activities including file counts, sizes, and transmission patterns.
- **Application Distribution:** Analysis of which applications are used for data transmission with associated metrics.
- **Document Derivative Tracking:** Comprehensive monitoring of file modifications, copies, and transformations with complete traceability.
- **Derivative Trajectory Mapping:** Visual representation of document movements and transformations over time for forensic analysis.

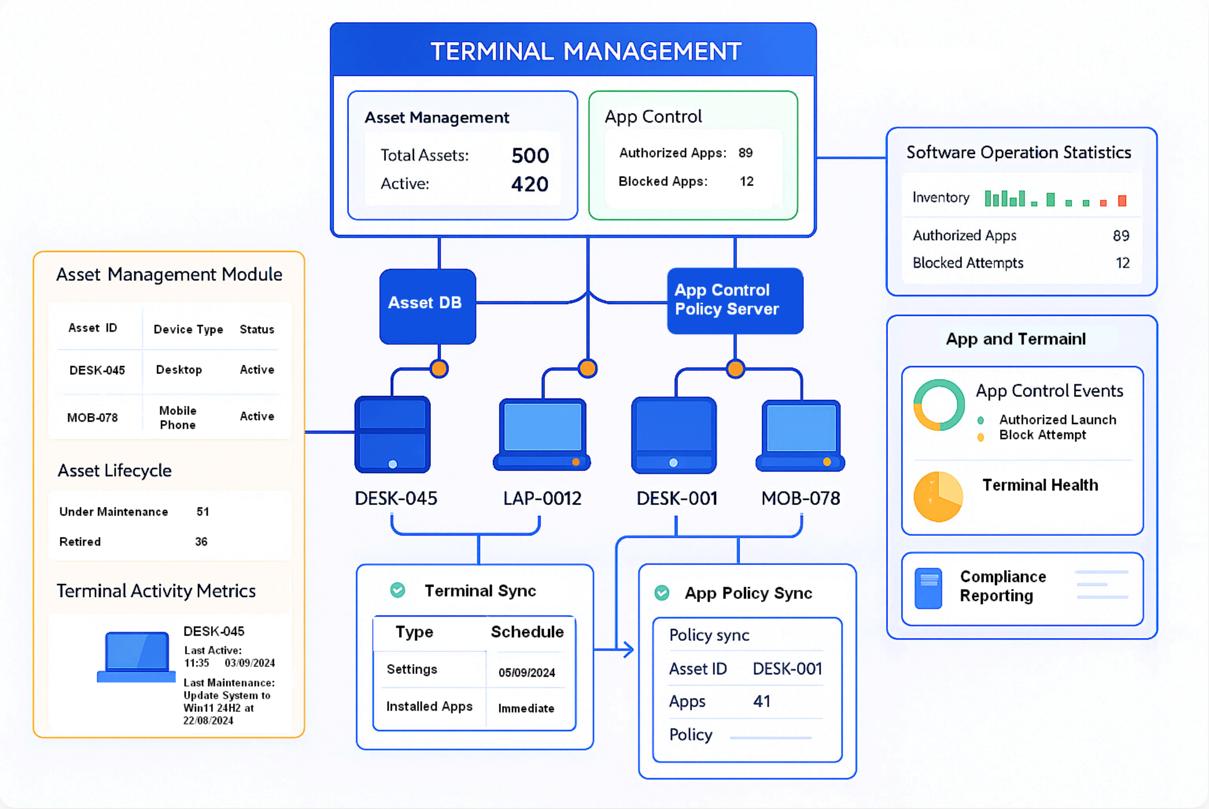


Terminal Management

Required Integrations: This module requires both **Asset Management Module** and **Application Program Control Module** to be fully functional.

Comprehensive oversight of endpoint assets, software inventory, and application usage to maintain security and compliance across all devices.

- **Software Operation Statistics:** Complete inventory of enterprise software including usage patterns, installation metrics, and categorization.
- **Usage Rate Analysis:** Visual metrics on key software utilization with detailed logs on installation and usage patterns.
- **License Compliance Monitoring:** Tracking of commercial software licenses with visualization of authorized vs. installed counts and overuse identification.
- **Terminal Activity Metrics:** Statistics on computer counts, power status, and active devices across the enterprise.
- **Detailed Software Analytics:** Comprehensive metrics including installation rates, usage patterns, idle software identification, and version tracking.
- **Custom Software Library:** Configurable software categorization with custom grouping, classification, and management capabilities.



Asset ID	Device Type	Status
DESK-045	Desktop	Active
MOB-078	Mobile Phone	Active

Under Maintenance	51
Retired	36

DESK-045
Last Active: 11:35 03/09/2024
Last Maintenance: Update System to Win11 24H2 at 22/08/2024

Type	Schedule
Settings	05/09/2024
Installed Apps	Immediate

Policy sync

Asset ID	DESK-001
Apps	41
Policy	

Application Scenarios

1. Source Code Leak Prevention

The Challenge

A software development company faces risks of intellectual property theft through unauthorized source code transmission. They need to detect and prevent employees from sending code through instant messaging, email, or cloud storage services before leaks occur.

The Solution with AnySecura

Implementing **Early Warning Center** and **Data Security** capabilities (requires **Document Operation Control Module**):

1. Configure custom warning rules for source code file patterns and extensions
2. Monitor outbound transmission through IM, email, and cloud upload channels
3. Set up real-time alerts for high-risk code transmission activities
4. Track complete document trajectories to identify leakage patterns
5. Generate comprehensive reports on code transmission attempts

Results Achieved

- ✓ 92% reduction in unauthorized code transmission attempts
- ✓ 100% detection rate of high-risk code transmission activities
- ✓ 3 successful prevention of major intellectual property leaks

2. License Compliance Management

The Challenge

A large enterprise faces potential legal and financial risks due to unmanaged software licenses. They need visibility into installed software across all endpoints to ensure compliance with licensing agreements and avoid penalties.

The Solution with AnySecura

Leveraging **Terminal Management** capabilities (requires **Asset Management Module** and **Application Program Control Module**):

1. Complete inventory of all installed software across enterprise endpoints
2. Tracking of commercial software licenses against installation counts
3. Visual alerts for over-licensed software and compliance violations
4. Identification of unused software for license optimization
5. Automated reports on license status and compliance metrics

Results Achieved

- ✓ Eliminated license compliance violations across the enterprise
- ✓ 35% reduction in software licensing costs through optimization
- ✓ Complete visibility of software assets across all endpoints

Core Values & Benefits

Proactive Threat Detection

Identify potential security risks before they escalate with advanced warning systems and configurable alert thresholds.

Comprehensive Visibility

Complete oversight of data flows, user activities, and endpoint assets for enhanced security awareness.

Data-Driven Insights

Actionable intelligence through advanced analytics and visualizations to support security decision-making.

Regulatory Compliance

Meet industry requirements with comprehensive audit trails, documentation, and compliance reporting capabilities.

Ready to Enhance Your Security Posture?

Learn More About Solutions

Contact Our Experts

www.anysecura.com

support@anysecura.com