



# AnySecura

## Network Access Control

Comprehensive network security and access management solution

Monitor · Restrict · Isolate · Optimize · Protect

### NETWORK ACCESS CONTROL





# Module Overview

AnySecura Network Access Control integrates four core capabilities, providing enterprises with comprehensive network access management, monitoring, and security controls to protect sensitive data and optimize network performance.



## Granular Access Control

Restrict network access permissions by application, network address range, domain name, communication direction, and port range.



## Intranet Computer Discovery

Detect all computers connected to the intranet and promptly identify computers whose clients have been illegally uninstalled.



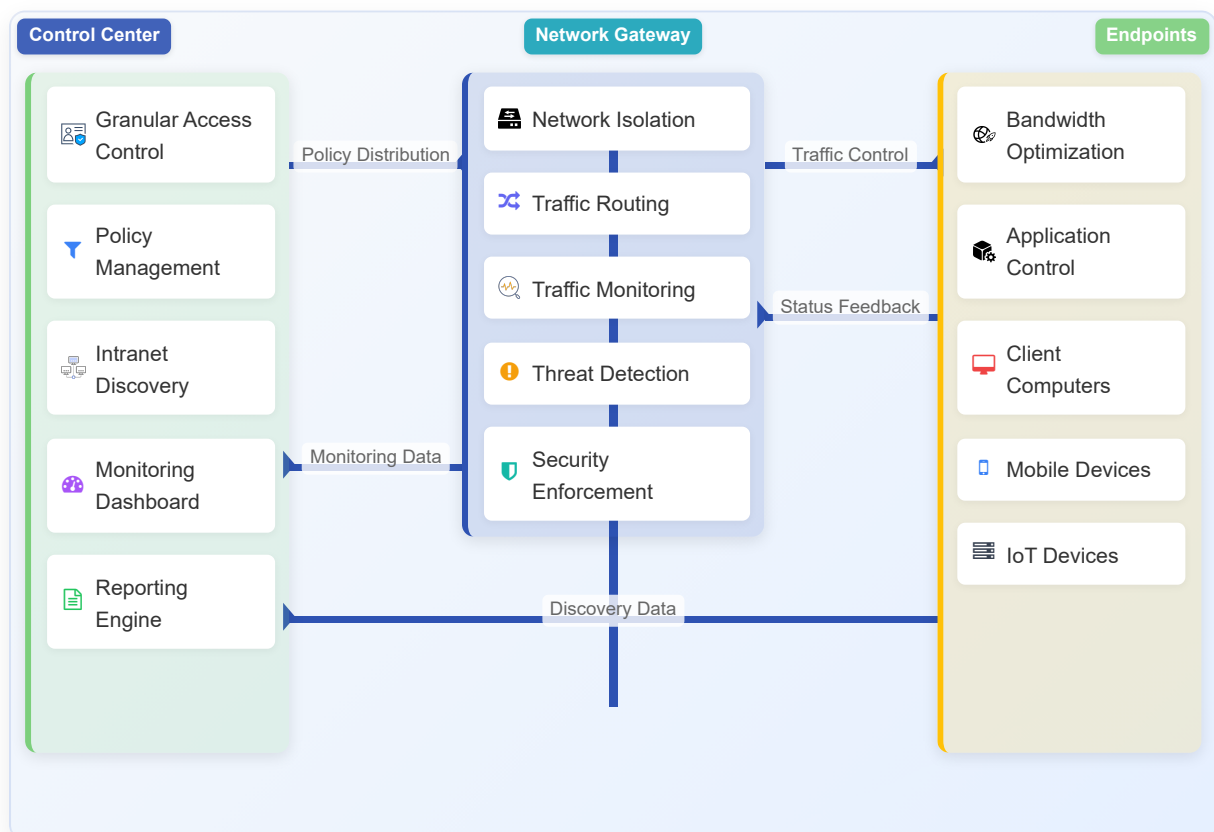
## Network Isolation

Establish network segmentation within the enterprise, setting up boundaries between departments or sensitive systems.



## Bandwidth Optimization

Prevent excessive bandwidth usage by restricting network access permissions of bandwidth-intensive applications.

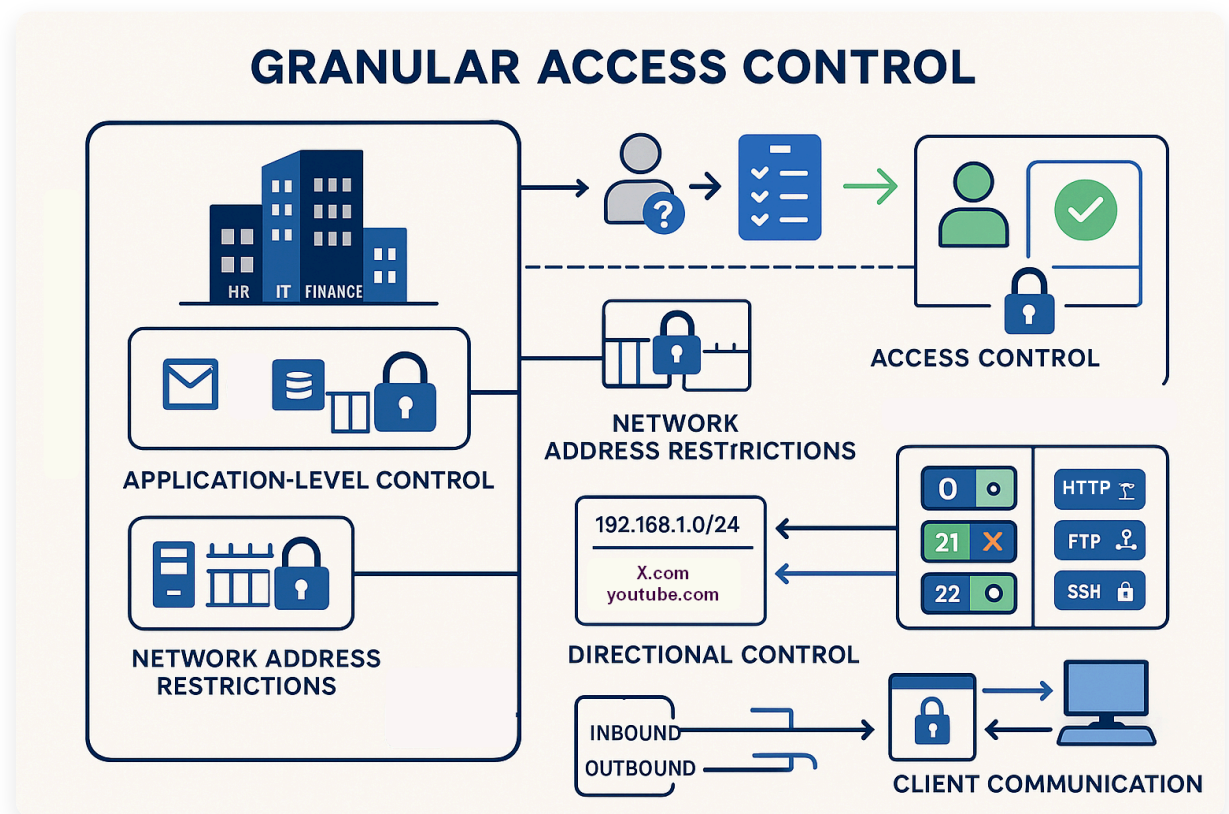




# Granular Access Control

Comprehensive control over network access permissions to ensure secure and appropriate network usage across the enterprise.

- ✓ **Application-level Control:** Restrict network access permissions for specific applications based on security policies.
- ✓ **Network Address Restrictions:** Control access based on IP address ranges and subnet configurations.
- ✓ **Domain Name Filtering:** Allow or block access to specific domain names and websites.
- ✓ **Directional Control:** Manage inbound and outbound network communication separately for enhanced security.
- ✓ **Port Management:** Control access to specific network ports to prevent unauthorized services and protocols.
- ✓ **Time-based Policies:** Apply network restrictions during specific time periods to align with business requirements.
- ✓ **Client Communication Control:** Manage network communication between clients and external computers.







# Intranet Computer Discovery

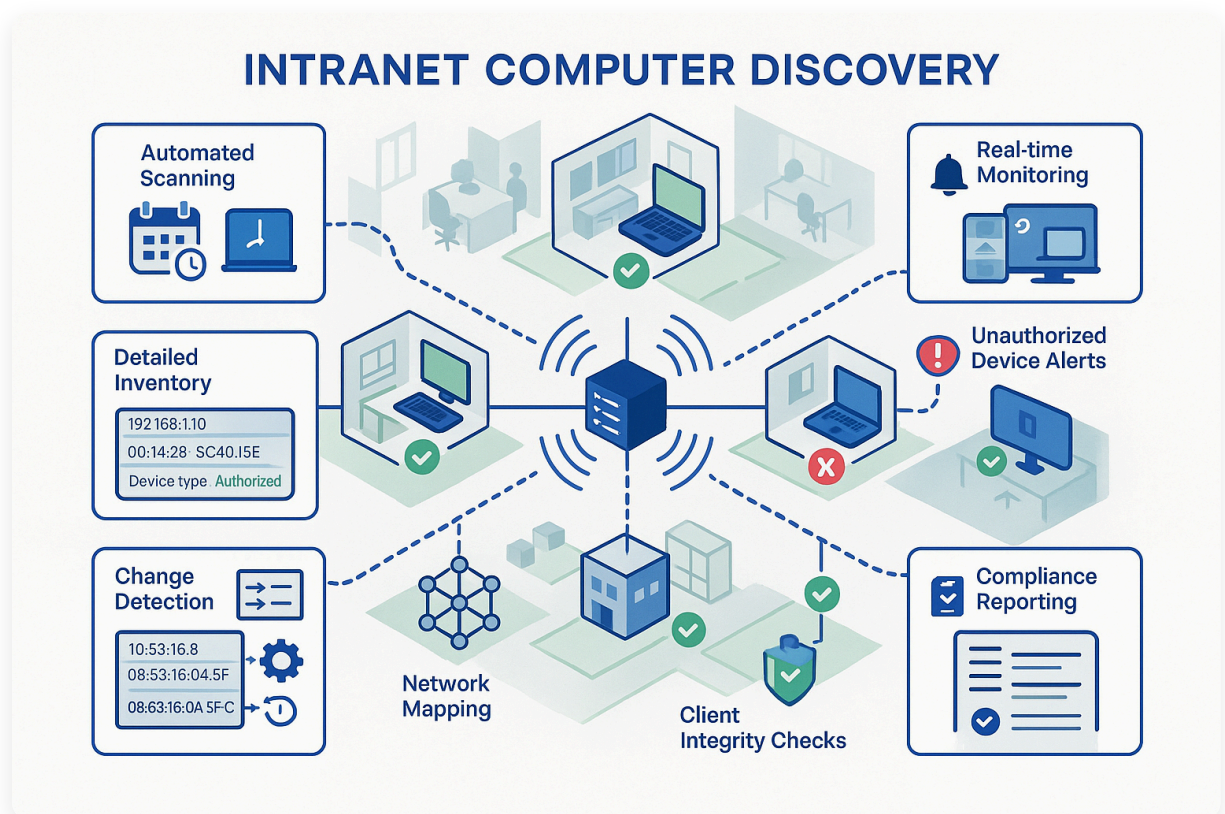
Comprehensive visibility into all devices connected to the enterprise network, ensuring complete control and security.

## Device Detection

- 🔍 **Automated Scanning:** Regularly scan and identify all computers connected to the intranet.
- 🔍 **Real-time Monitoring:** Continuous detection of new devices joining the network.
- 🔍 **Detailed Inventory:** Collect comprehensive information about each discovered device.
- 🔍 **Network Mapping:** Visual representation of all connected devices and their relationships.

## Security Monitoring

- 🛡️ **Unauthorized Device Alerts:** Immediate notifications about unknown devices on the network.
- 🛡️ **Client Integrity Checks:** Promptly identify computers whose security clients have been illegally uninstalled.
- 🛡️ **Change Detection:** Monitor and log changes to device configurations and network connections.
- 🛡️ **Compliance Reporting:** Generate reports on network device status for security audits.










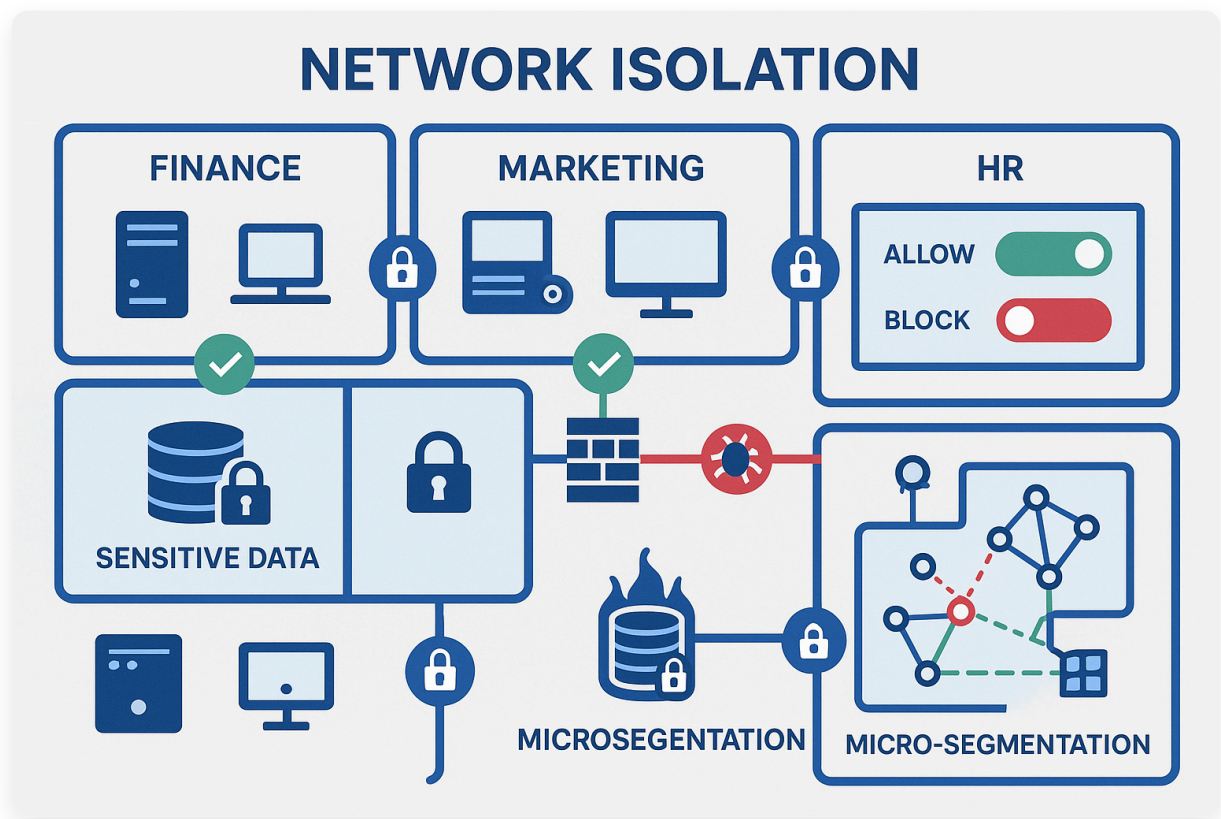




# Network Isolation

Advanced network segmentation capabilities to create secure boundaries within the enterprise infrastructure.

-  **Departmental Segmentation:** Establish network isolation between departments, such as Finance and Marketing.
-  **Sensitive Data Protection:** Create isolated zones for systems handling confidential information.
-  **Custom Isolation Rules:** Define granular policies for which network segments can communicate with each other.
-  **Controlled Access Points:** Establish secure gateways between isolated segments for authorized communication.
-  **Micro-segmentation:** Create fine-grained network zones based on specific security requirements.
-  **Breach Containment:** Prevent lateral movement of threats across the network through isolation barriers.
-  **Isolation Visualization:** Graphical representation of network segments and their connection rules.














# Bandwidth Optimization

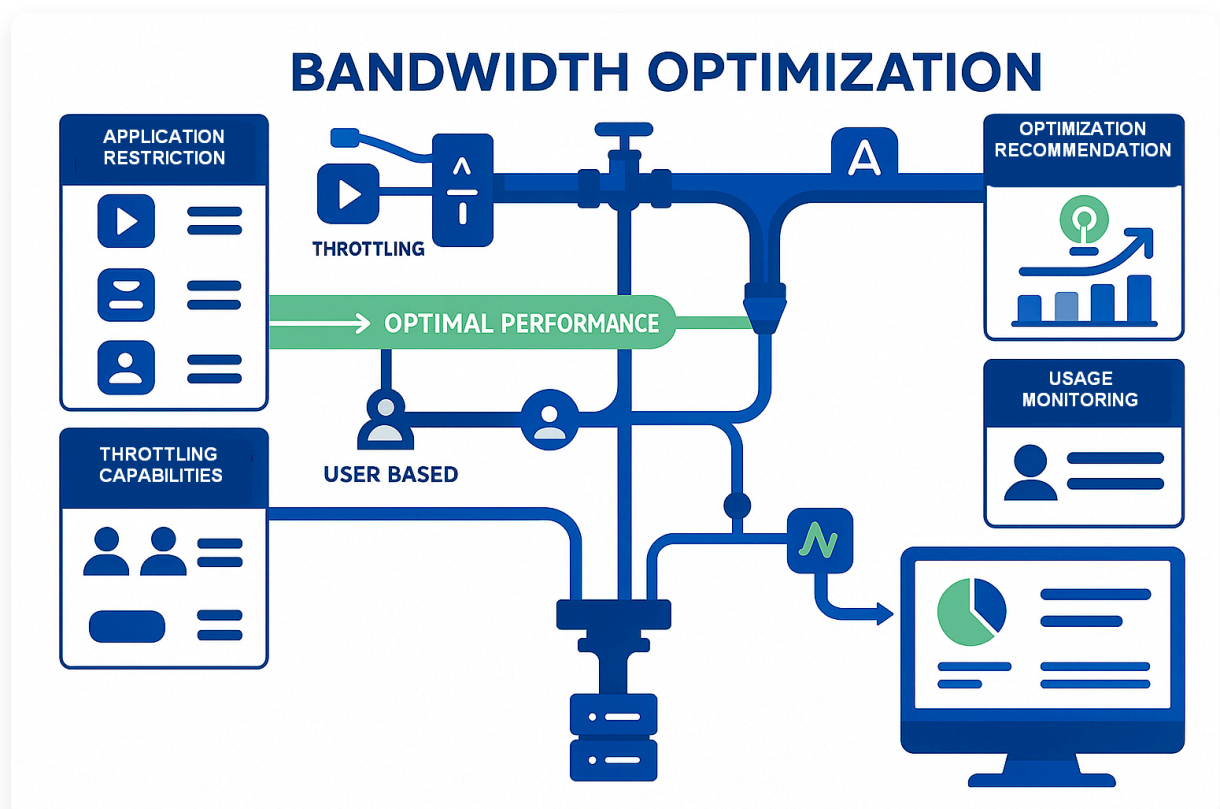
Comprehensive management of network bandwidth to ensure optimal performance and prevent excessive resource consumption.

## Bandwidth Control

-  **Application-based Restrictions:** Control network access permissions of bandwidth-intensive applications.
-  **Throttling Capabilities:** Limit bandwidth usage for specific applications like P2P download software.
-  **User-based Allocation:** Assign bandwidth quotas based on user roles or departments.
-  **Priority Management:** Ensure critical business applications receive sufficient bandwidth.

## Performance Optimization

-  **Usage Monitoring:** Track bandwidth consumption patterns across the network.
-  **Peak Time Management:** Implement stricter controls during periods of high network usage.
-  **Anomaly Detection:** Identify unusual bandwidth usage that may indicate issues or misuse.
-  **Optimization Recommendations:** Receive suggestions for improving network performance based on usage patterns.
-  **Reporting Dashboard:** Visual representation of bandwidth usage and optimization metrics.



# Application Scenarios



## 1. Departmental Network Isolation

### The Challenge

A large enterprise needs to protect sensitive financial data while enabling appropriate cross-department communication, lacking clear network boundaries.

### The Solution

Implementing **Network Isolation**:

1. Create separate network segments for key departments
2. Configure strict access controls for sensitive segments
3. Establish controlled channels for authorized communication
4. Monitor for unauthorized access attempts

### Results

- ✓ Complete protection of sensitive financial data
- ✓ 95% reduction in unauthorized access attempts



## 2. Network Performance Optimization

### The Challenge

A company experiences network slowdowns during business hours due to employees using bandwidth-intensive applications.

### The Solution

Deploying **Bandwidth Optimization**:

1. Identify and classify bandwidth-intensive applications
2. Restrict non-business applications during working hours
3. Allocate priority bandwidth to critical business tools
4. Set reasonable quotas for non-business use during off-peak times

### Results

- ✓ 75% improvement in network performance
- ✓ 90% reduction in non-business bandwidth consumption
- ✓ 30% increase in employee productivity



## Core Values & Benefits



### Enhanced Network Security

Protect sensitive data and systems through granular access controls and network segmentation, minimizing the risk of unauthorized access.



### Complete Visibility

Full visibility into all devices connected to the network with real-time monitoring and alerts for potential security issues.



### Optimized Performance

Ensure optimal network performance by preventing bandwidth abuse and prioritizing critical business applications.



### Regulatory Compliance

Meet industry regulations and data protection requirements through controlled network access and comprehensive audit capabilities.

## Ready to Take Control of Your Network Security?

 [Learn More About Solutions](#)

 [Contact Our Experts](#)



[www.anysecura.com](http://www.anysecura.com)



[support@anysecura.com](mailto:support@anysecura.com)

© 2025 AnySecura SOFTWARE PTE. LTD. All rights reserved. Enterprise-grade security solutions.