Unisys Stealth® Microsegmentation Protects the Critical Six Key Elements of Stealth

What is microsegmentation?
Microsegmentation is a security strategy that segments your network into smaller elements and manages them with IT security policies.

Think of traditional security as a bank vault, and microsegmentation as a safe deposit box inside it. Microsegmentation allows you to quickly and easily separate physical networks into logical microsegments. Each microsegment is protected, dramatically lowering risk. If a threat gets inside the vault, it can only unlock the boxes with the right keys.

What is Unisys Stealth?
Stealth™ is a software suite trusted by government and commercial organizations to protect sensitive systems from cyber threats with identity-driven, software-defined microsegmentation.

Stealth creates communities of interest (COI) that establish exclusive communication channels between members based on trusted identities. Community members cannot initiate or accept communication from non-members and cryptography restricts non-members from intercepting intra-community communications.

What can you do with Stealth?

Know your network
Visualize, model and design informed security

Cloak critical assets
Cryptographically hide critical assets from adversaries

Easy microsegmentation
Isolate assets, regardless of environment, network or device

Enable adaptive security
Integrate existing security tools to correlate, detect and respond

Encrypt data in motion
Prevent packet sniffing with AES-256 encryption

Prevent fraud
Verify identities with physical and behavioral biometrics

How Stealth Works

Integrate with existing security tools to correlate, detect and respond to threats without adding complexity

Add behavioral biometrics and multifactor authentication

Stealth Intercept
Encrypt data in motion

Prevent fraud
Verify identities with physical and behavioral biometrics

Consistent security scheme for cloud workloads

Elastic microsegmentation allows access to multiple COI

Overlay technology means no changes to existing network

Live network visibility

Stealth (core)

Identity and Access Management

Security Information and Event Management

Application

Presentation

Session

Transport

Data Link

Physical

NIC

Stealth (mobile)

Stealth (aware)

Stealth (cloud)

Identity management systems manage COI membership to reduce management overhead

Reduce mobile attack surface

Protect assets behind network devices

Isolate legacy assets

Protect physical servers, virtual machines, purpose-built devices, operational technology and more

COI reduce internal firewalls and VLANs with identity based microsegmentation

Integration with Identity Management

Identity and Access Management

Security Information and Event Management

Stealth (Cloud)

Stealth (mobile)

Stealth (aware)

Stealth (core)

Stealth Intercept

Encryption

Data in motion

Transparent to applications

Integration with Identity Management

Automation APIs

Seven Key Elements of Stealth

Identity based microsegmentation

Encrypted data in motion

Asset cloaking

Transparent to applications

Integration with Identity Management

Automation APIs

六 Key Elements of Stealth

身份基準のマイクロセグメンテーション

データの暗号化

資産の隠蔽

透明性

統合

自動化API

Unisys Stealth® Microsegmentation Protects the Critical

What is microsegmentation?
Microsegmentation is a security strategy that segments your network into smaller elements and manages them with IT security policies.

Think of traditional security as a bank vault, and microsegmentation as a safe deposit box inside it. Microsegmentation allows you to quickly and easily separate physical networks into logical microsegments. Each microsegment is protected, dramatically lowering risk. If a threat gets inside the vault, it can only unlock the boxes with the right keys.

What is Unisys Stealth?
Stealth™ is a software suite trusted by government and commercial organizations to protect sensitive systems from cyber threats with identity-driven, software-defined microsegmentation.

Stealth creates communities of interest (COI) that establish exclusive communication channels between members based on trusted identities. Community members cannot initiate or accept communication from non-members and cryptography restricts non-members from intercepting intra-community communications.

What can you do with Stealth?

Know your network
Visualize, model and design informed security

Cloak critical assets
Cryptographically hide critical assets from adversaries

Easy microsegmentation
Isolate assets, regardless of environment, network or device

Enable adaptive security
Integrate existing security tools to correlate, detect and respond

Encrypt data in motion
Prevent packet sniffing with AES-256 encryption

Prevent fraud
Verify identities with physical and behavioral biometrics

How Stealth Works

Integrate with existing security tools to correlate, detect and respond to threats without adding complexity

Add behavioral biometrics and multifactor authentication

Stealth Intercept
Encrypt data in motion

Prevent fraud
Verify identities with physical and behavioral biometrics

Consistent security scheme for cloud workloads

Elastic microsegmentation allows access to multiple COI

Overlay technology means no changes to existing network

Live network visibility

Stealth (core)

Identity and Access Management

Security Information and Event Management

Application

Presentation

Session

Transport

Data Link

Physical

NIC

Stealth (mobile)

Stealth (aware)

Stealth (cloud)

Identity management systems manage COI membership to reduce management overhead

Reduce mobile attack surface

Protect assets behind network devices

Isolate legacy assets

Protect physical servers, virtual machines, purpose-built devices, operational technology and more

COI reduce internal firewalls and VLANs with identity based microsegmentation

Integration with Identity Management

Identity and Access Management

Security Information and Event Management

Stealth (Cloud)

Stealth (mobile)

Stealth (aware)

Stealth (cor)