STEALTH™

# Stealth(core)™

## Zero Trust Network Protection - Simplified

## HIGHLIGHTS

- ***Microsegment without complexity*** *using identity-based security to prevent unauthorized lateral movement with no existing network or application changes*
- ***Stop cyberattacks in progress*** *by dynamically isolating devices and users at the first sign of compromise*
- ***Protect data in motion*** *with industrial-grade AES-256 encryption and packet inspection enablement for authorized personnel*
- ***Automate security operations*** *through APIs and robust scripting support*
- ***Apply consistent security policies*** *with microsegmentation across data centers, physical servers, virtual machines and purpose-built devices*
- ***Reduce security and compliance*** *costs by limiting the scope of audits while reducing the need for expensive and complex static security controls*

"With the Unisys Stealth solution, we have been able to increase customer confidence reflected in increased revenue, lower operation costs through reduction of employee theft and PCI compliance."

- Manager – IT,
Large Latin American Supermarket Chain

## Control Risk and Manage Trust With Identity-Based Microsegmentation

In the digital age, traditional security can no longer protect a dynamic network environment against the growing threat of cyberattacks. Static security controls are difficult to manage, update and operate—increasing security and compliance costs, while limiting agility. Organizations need a new approach to security with a Zero Trust Network that trusts no user or device, on the inside or outside, only granting least-privilege access upon reliable identification.

Part of Unisys Stealth® security software suite, Stealth(core)™ distributed locally by Agilient provides foundational capabilities—identity-based microsegmentation, dynamic isolation, cryptographic cloaking and encryption of data in motion—that transform your existing network into a Zero Trust Network without added implementation and management complexity.

## Build a Zero Trust Network

Stealth™ reduces risk by creating dynamic, identity-based microsegments called communities of interest (COI). Stealth treats all network traffic as untrusted, permitting communication only when COI membership is confirmed. By establishing secure COI, Stealth separates trusted systems, users and data from the untrusted. It further reduces risk by encrypting all communication between Stealth-protected assets and cloaking them from unauthorized users. Stealth packet inspection enablement allows authorized personnel to inspect communications without compromising data in transit.

## Enable Dynamic Isolation

Through interoperability with existing security information and event management (SIEM) systems and user-friendly application programming interface (API) integrations, Stealth enables immediate action in response to security incidents, stopping attacks in progress. Stealth dynamically isolates devices and users at the first sign of compromise. It also utilizes identity management systems, such as Active Directory, to manage memberships to COI for efficient identity-based controls and management.

## Decrease Network Complexity and Costs

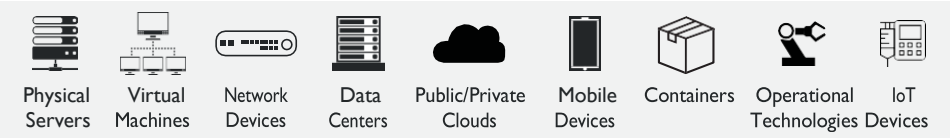
A software-only solution, Stealth is easy to use and deploy, requires no changes to your existing network or applications and allows you to reduce complexity, expense and operation of static security controls in your dynamic organization. A reduced attack surface limits the regulatory audit footprint for lower compliance costs.

## Automate Security Deployment

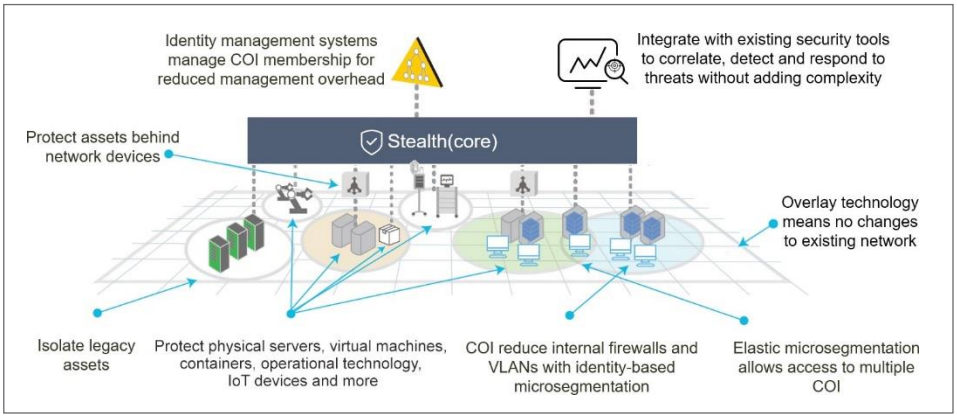
An expanded suite of standardized tools, including APIs and robust scripting support, enables unattended automated installation. These automation enhancements eliminate the need for repetitive and manual operations, reducing installation time and improving management capabilities.

## Adapt with Flexible Protection

Stealth(core) enables uniform security policies across a range of endpoints and workloads, including physical servers, virtual machines, operational technology (OT) and purpose-built devices. You can deploy Stealth incrementally and scale it efficiently using rich APIs and automation. The same protection extends to cloud and mobile environments using Stealth(cloud)™ and Stealth(mobile)™. Stealth is also capable of securing workloads behind network devices such as routers and load balancers.




## Stealth Protects Your Existing Network




## Why UNISYS and Agilient?

*In our digital world, critical applications and systems deliver vital access to energy, transportation, financial services and healthcare as well as strong national security and defense. Industry-leading organizations trust Unisys to maximize security posture across IT, OT and production environments. Unisys Security Solutions and Agilient combine expert consulting, advanced technologies and managed services that span the entire security lifecycle.*

| ENTERPRISE MANAGER REQUIREMENTS | |
|---|---|
| Hardware | Minimum:<br>6 GB RAM or greater<br>3-4 cores processor<br>30 GB disk space |
| Operating system | Windows Server 2012 R2 x64 and<br>Windows Server 2016 |
| Screen resolution | 1152 × 864 (minimum)<br>1440 × 900 (maximum) |
| Web browser | Internet Explorer 11.x<br>Firefox 35 or later |

| ENDPOINT REQUIREMENTS | |
|---|---|
| Windows operating system | Windows 7 and above<br>Windows Server 2008 R2 and above<br>Windows 10 IoT Enterprise |
| Linux operating system | RHEL 6.x, 32-bit and 64-bit<br>RHEL 7.x, 64-bit<br>SLES 11.x, 32-bit and 64-bit<br>SLES 12.x, 64-bit<br>SLES 15.x<br>Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 64-bit<br>CentOS 6.9 and CentOS 7.5, 64-bit |

agilient

**Contact securityinsights@agilient.com.au or visit www.agilient.com.au to learn more about how Agilient and Stealth(core) can help you transform your existing network into a Zero Trust Network.**