SECURE YOUR LEGACY SYSTEMS WITH STEALTH™

STEALTH™

Lack of Legacy Security

It's highly likely your IT infrastructure includes legacy systems – old hardware, applications, and computer systems that may be no longer supported by your technology vendors. They might be as seemingly inconsequential as a few PCs running Windows 95 on a loading dock, or as vital as an end-of-life minicomputer running your organization's accounting system. But what all legacy systems have in common is lack of security. Legacy systems often are under-patched or no longer patched at all, yet they can't easily be replaced or updated by an organization. (Sound familiar?) This endangers your entire IT environment.

Most legacy systems remain in place for a variety of reasons, including:

- They continue do their job
- Replacement costs may be too high
- They are not planned to be replaced until later

Legacy Loopholes

Maybe you're retaining some legacy technologies because they simply work well for the job. They are efficient and "finely tuned" to the task at hand, making replacement more of a disruption than it is worth. Taking down your ordering system for maintenance and replacement, for instance, could result in a major revenue hit that would render the move too costly to consider. You also may feel locked into your legacy systems because alternative, modern solutions are more expensive to run and time-consuming to implement. Or maybe you've been planning for some time to replace your legacy systems, but the timeline keeps getting pushed back, thereby leaving systems vulnerable. The last reason especially may be likely if your business has been disrupted by the global pandemic and resulting recession.

Regardless of the legacy loophole, you need protection for your legacy systems. One alternative to replacing legacy systems is patching. Unfortunately, many enterprises find that without through-testing, patches may cause instability in their finely tuned systems. And in the case of legacy systems near "end of life," manufacturers no longer provide you with reliable security for functional upgrades or patches, leaving users to "get by" with their old, unsupported systems.

When legacy systems cannot be upgraded or replaced, Unisys Stealth® protects your business processing and the devices themselves by isolating them, while avoiding the pitfalls of traditional network segmentation techniques.

Unisys Stealth Secures Legacy Systems

Unisys Stealth is software-defined security. It simplifies yet improves network security and serves as the backbone of your entire network Zero Trust strategy. Stealth™ blankets every corner of your organization's computing environment with one holistic, consistent, and unwavering security policy—from mobile phones and desktops, to servers, to cloud, and even IoT. In fact, Stealth orchestration and deployment are highly automated and centrally managed. As your security policies evolve, changes can be made once and instantly propagate across the enterprise. Meanwhile, Stealth monitors and enforces all your Zero Trust policies, automatically isolating violations and alerting administrators. With Stealth Zero Trust, security is seamlessly woven into the fabric of your entire network. It's the engine that drives your speed to security and speed to market.

The Stealth Zero Trust architecture secures users and applications based on identity and roles, meeting a common requirement in many compliance frameworks. Stealth enables you to achieve cost-effective compliance faster by limiting data access only to those users, devices, servers, and applications that absolutely must have it. By limiting user access, you reduce the number of devices and connections that audits need to examine. Stealth achieves this network micro-segmentation and compartmentalization by deploying highly secure IPsec tunnels that meet requirements for encrypting data in motion.

Stealth encrypts traffic, shields endpoints from unauthorized access, and provides you with the capability to conceal systems and users anywhere on the Stealth-enabled network.

This paper explores how you can use Stealth to isolate legacy endpoints (such as servers, workstations and other devices) that can't be upgraded, patched, replaced or decommissioned. Isolating these endpoints and allowing only required business access protects your trusted network from vulnerabilities introduced by these systems and also protects your endpoints themselves from compromise.

Legacy Systems Still Run Business

While many legacy systems are integral to business-critical application environments, they may be running on unsupported operating systems. A case in point: Mainstream support for Microsoft Windows 7 without Service Pack 1 (SP1) ended in April 2013. Support for SP1 ended in January 2015, and since then users have been on "extended support." Current research shows that even with extended support having ending in January 2020, Windows 7 still held roughly 23% of the worldwide desktop/laptop OS market share in July 2020, second only to Windows 10 at 59%.[i] It's easy to understand why legacy systems remain prevalent – they are stable, paid off, and still serve the business, they host applications that may be fundamental to operations, and they just work.

The risks associated with your dependence on legacy systems for business processing run wide and deep – security vulnerabilities, compliance challenges, increased failure rate, incompatibility with contemporary products, stunted innovation. Yet you may choose (or are forced) to maintain outdated systems running critical business applications, even knowing these systems introduce business and security threats. Somehow securing these systems while they remain vital allows you to safely sustain operations while longer-term plans can be developed.

Need a Feasible Security Approach

Even though you realize that migrating your legacy systems to the cloud will take a long time, you are keenly aware of the organization's need for a nondisruptive security solution that works today. You could try segmenting legacy systems and environments, effectively isolating them with limited and strictly enforced access, but accomplishing this is easier said than done. Nonetheless, the fact remains that isolating specific endpoints and allowing only required business communications not only protects your trusted network from vulnerabilities introduced by the outdated systems, it also protects the endpoints themselves from compromise.

The challenge is that if you embrace the concept of segmentation and isolation, there's a good chance you'll struggle with actual architecture and implementation. Traditional segmentation using VLANs and network firewalls yields segments that are too large and encompassing to be effective. Segments comprised of many users and legacy systems and other servers or devices dilute access control and the intended security. And it's not feasible to create VLANs or deploy network firewalls and manage firewall rules sufficiently granular to achieve the desired results. Smaller segments are prohibitively expensive and complex to manage. You need a different tactic.

Unisys Stealth as an Isolation Strategy

Unisys Stealth is a software-based, identity-managed endpoint segmentation and isolation solution suitable for limited tactical or enterprise-wide deployment, regardless of your existing physical network topology. Stealth allows you to micro-segment, encrypt traffic, remain opaque to attackers, and remediate threats throughout an enterprise. Stealth creates overlay networks that are cryptographically separated from your underlying infrastructure and each other, independent of the physical network. Stealth can be deployed to selectively isolate systems from the general network, and tightly control access in a very granular manner. The isolation controls can be configured for any network-connected endpoint on the internal network, in the cloud, or anywhere a connected endpoint resides.

How Stealth Isolates and Protects

Stealth renders selected network endpoints, such as legacy systems, inaccessible to any users or other systems not explicitly 1) authorized for the same logical secure communication group or 2) allowed to communicate by a predefined "clear-text filter." The concept of membership in a logical secure communication group, called a Community of Interest (COI), is central to the Stealth solution.

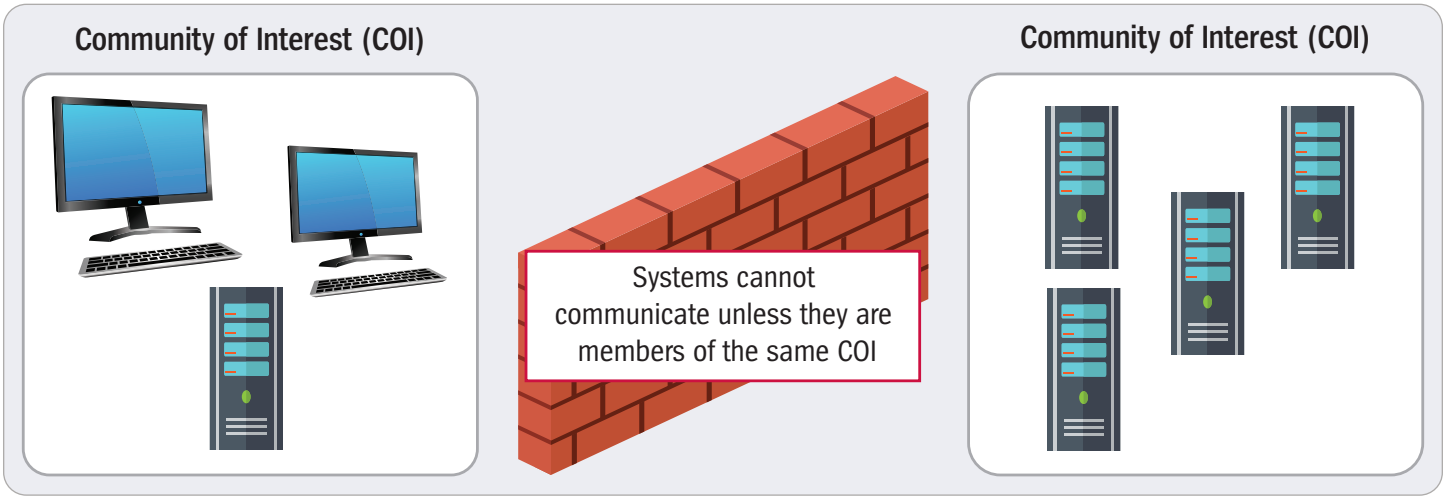
In general, members of a specific COI can communicate with each other, while non-members cannot. Filters may further restrict communications within a COI, based on IP addresses, protocols, and TCP/UDP port numbers. Filters can also be defined to allow selective clear-text communication outside the COI.

Every Stealth endpoint must have an associated identity. For Windows desktops, the identity typically is that of the currently logged-on user. With other operating systems, identity can be determined through a Microsoft Windows domain Kerberos ticket, domain account credentials, a "user" certificate (typically corresponding to a service account) or a computer certificate.

Stealth introduces the concept of a "Role" for determining membership in a COI. Your endpoint identities are mapped to Roles when Stealth environment components are being defined, either directly (e.g. individual user accounts) or indirectly (through group membership). During authorization, Stealth software presents the endpoint's identity to a Stealth Authorization Service. The Authorization Service determines what Role is appropriate for that identity and the endpoint is given the COI keys and filters for the associated Role.

Membership in a common COI is determined by a proprietary Stealth protocol called Secure Community of Interest Protocol (SCIP), and until that membership is confirmed by both endpoints, no non-SCIP packets may be sent between them. SCIP is invoked when one endpoint tries to initiate communications with another endpoint.

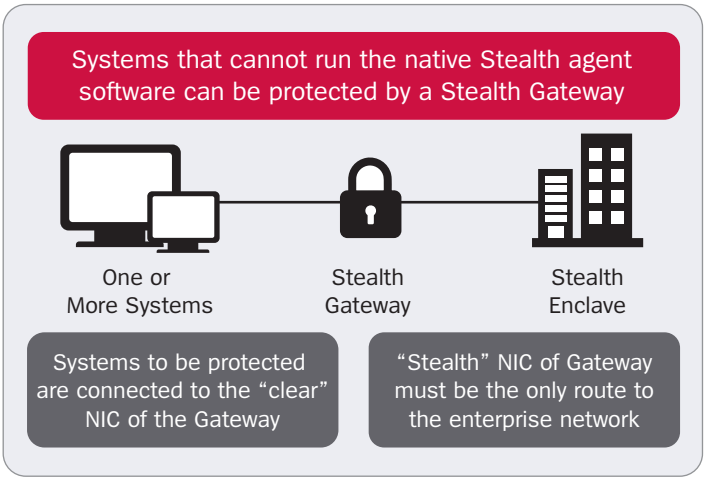
That first packet to be transmitted causes SCIP to begin the COI negotiation and Stealth tunnel establishment process. Once common COI membership is confirmed, SCIP creates a secure association between the two endpoints; further communication uses industry-standard IPSec. The cryptography used by SCIP and IPsec meets very stringent, government-mandated requirements for algorithms and key strengths. Packets sent to a Stealth-protected endpoint from a non-COI member (unless a filter is explicitly defined to accept the packets) are dropped. That is how Stealth endpoints remain dark on a network and unresponsive to scans, malware probes, or other unauthorized access.



Stealth Isolating Legacy Systems

This paper has mentioned Stealth endpoints and endpoint identity and the Stealth SCIP protocol, which suggests there is software executing on the system being protected. In many cases, that is true. But in the case of legacy systems, it may not be possible or appropriate to add software to the system requiring protection, so you need to bring Stealth isolation as close to the individual endpoint as possible.

Endpoints running operating systems for which there is no native Stealth agent, or for other reasons where it is not appropriate to add software, participate in Stealth networks through the use of a Stealth Gateway.



Stealth Secure Virtual Gateway (SVG)

One Stealth Gateway option is Secure Virtual Gateway (SVG). SVG allows non-Stealth-enabled systems (the legacy systems, generally known as the clear-text endpoints) to participate in COIs. The SVG acts as a Layer 3 router between your clear-text endpoints (the legacy systems) and a Stealth network and must be configured so that the SVG is the only route between the systems to be protected and the rest of the network. Where security is your paramount concern, the network segment between the protected legacy systems and the SVG should be as short as possible, and physically secured.

The SVG does not interfere with normal operations of your legacy systems. Because no software installation is required, your systems continue to execute the same applications with little or no network reconfiguration and can be prevented from reaching any other network locations, particularly the Internet. They also can be granted access to specific resources, such as the enterprise's core IT services. Your legacy systems can be configured to communicate with both Stealth endpoints and other systems in the Stealth-enabled network that are not running Stealth software.

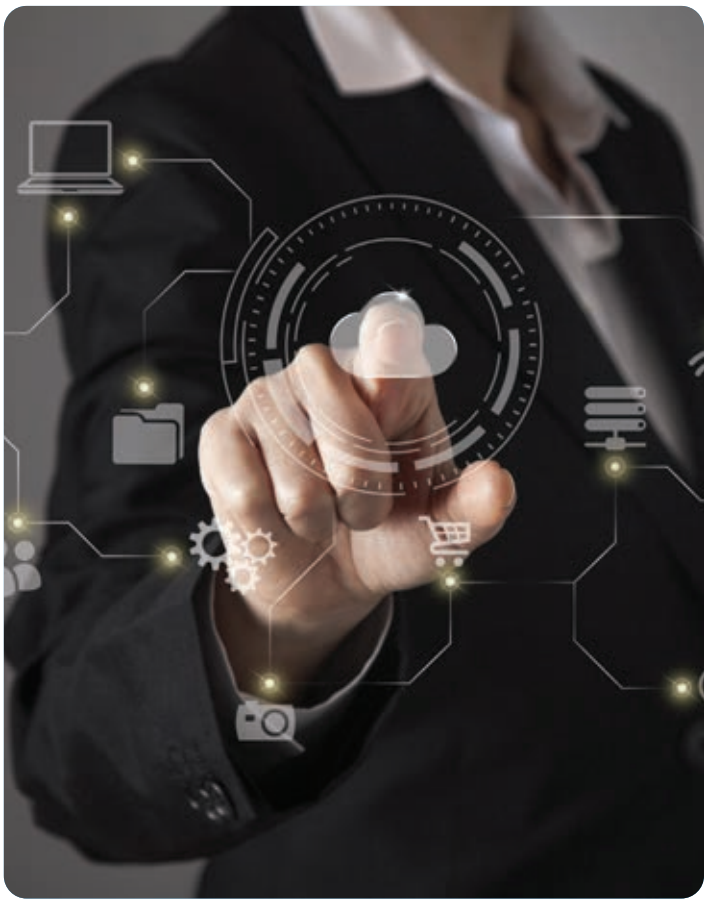
Account credentials are configured in the SVG for each of your protected legacy systems to provide the required endpoint identity. The credentials determine, through the normal Stealth Authorization method, the Role into which each of your protected legacy systems should be authorized.

One SVG can serve multiple groups of legacy systems and one SVG can map to multiple existing VLANs. The SVG software itself can be run on either a virtual machine or a physical machine and the SVG software deliverable includes the required operating system.

Stealth Smart Wire

Another option for your legacy systems to be protected by Stealth is through the use of Smart Wire. Smart Wire acts as a Layer 2 bridge and, to be protected, must be connected between the systems and the rest of the network. As with SVG, where security is of paramount concern, the network segment between the protected systems and the Smart Wire should be as short as possible, and physically secured.

A single identity/credentials is configured in Smart Wire. The configured identity/credentials determine, through the normal Stealth Authorization method, the single Role into which each protected legacy system should be authorized.



Choosing SVG Versus Smart Wire

Since the SVG acts as a Layer 3 router, whereas the Smart Wire acts as a Layer 2 bridge, the location of your systems to be protected from a networking perspective and their proximity to the Stealth Gateway are key to determining the appropriate option. Smart Wire is intended for systems or devices in the same broadcast domain that are configured very close to the Smart Wire, such as a set of legacy fixed-function workstations. Systems protected by SVG can be routable – perhaps legacy servers in the data center.

	Stealth Smart Wire	Stealth Secure Virtual Gateway
Typically Front Ends	IP-based device that cannot host Stealth agent, sitting outside data center	A server that is running an operating system that is not supported by Stealth
Typically Deployment Location	Field- e.g. on a factory floor	Data center
Scalability	Currently, up to 5 clear-text endpoints can connect to 1 instance of the Smart Wire	Currently, up to 1,000 clear-text IP addresses can connect to 1 instance of the Stealth SVG
Number of Stealth Roles Supported	One Role-all devices configured to one Smart Wire participate in the same Stealth Role	Up to 1,000 Stealth Roles

Stealth Micro-Segmentation

As noted, creating small-enough segments to effectively protect your legacy systems using traditional technologies (essentially VLANs and internal firewalls) is prohibitively expensive and very complex to manage. How is Stealth a better approach? As a software-based solution, Stealth segments, as defined by COI membership, can be created and modified without impacting your operations or making and testing changes to your underlying infrastructure. Without the need for an IP address, Access Control List (ACL) or physical configuration changes, implementation not only is faster, it is less prone to error.

The resulting deployment is more agile because redefining COI membership and hence accessibility is accomplished simply by changing which of your endpoint identities are associated with which Stealth Roles. Stealth micro-segmentation is very flexible and will not "break" or require change if legacy assets move within your network. Stealth enforces common security policies in on-premises data centers, multiple sites, and public/private/hybrid cloud providers. With Stealth software, it doesn't matter what variety of physical networking devices are already deployed throughout your enterprise. Stealth micro-segments create many small, secure logical networks, immediately and inherently reducing the attack surface.

When Legacy Is Upgraded

Your business evolution at some point requires upgrading, replacing, or decommissioning legacy endpoints. Micro-segmentation remains a powerful strategy for protecting other critical assets across your enterprise – the value of an investment in Stealth is not limited to the short term. In fact, Stealth often is initially implemented to solve an immediate problem such as isolating legacy systems, and then the deployment expands as cybersecurity requirements progress. Stealth software easily scales, and new identities can be easily added to incorporate wider protection.

Legacy Systems Do Not Require Legacy Thinking

Traditional approaches to protecting legacy systems include segmentation and restricting access that are rooted in "separate silo" techniques. This tactic facilitates IT at the expense of business needs because the systems to be protected and the users of those systems must conform to the infrastructure. The inferior security provided and the negative impact to your business as a result of that model require changing to a contemporary solution. After all, just because your systems are outdated does not mean their security needs to be. Quite the contrary.

Unisys Stealth protects legacy and other vulnerable or high-value assets by defining and dynamically deploying micro-segmentation security polices to permit, restrict or completely block communication among these resources. Stealth enables the quick deployment of software-defined network segments, providing these benefits:

- **Risk is mitigated** – protected endpoints are segregated from the rest of the network, which protects both your devices and the network.

- **Cost and complexity are contained** – identity-based software solution reduces your reliance on physical IT infrastructure and provides only tightly controlled access.
- **Threat spread is reduced or eliminated** – Stealth COIs contain a threat inside a specific micro-segment. Even if a system is compromised, nothing can be sent outside the COI – lateral network traffic is restricted to within the COI.
- **Attack surface is compacted** – segregated endpoints are hidden, and unauthorized access is thwarted both inside and outside the enterprise.
- **Security management is simplified** – Stealth is easy to scale and adapt to your emerging needs.

Stealth thus provides CISOs and their cybersecurity teams with peace of mind knowing they are implementing a Zero Trust security strategy using one of the most proven, cost-effective, end-to-end security systems available on the market today. Stealth is currently deployed worldwide across all verticals including federal, financial, pharmaceutical, industrial, energy, medical, education, and the DoD. As your organization continues to face uncertain times and economic conditions, Stealth offers security you can rely on.

[i.] NetMarketShare. Global operating system market share, July 2020.

For more information or to request a demo, contact us at
www.stealthsecurity.unisys.com/contact-us/

For more information visit www.unisys.com