

GET ADVANCED CYBER RESILIENCE IN THE NOW PLATFORM®

KEY FEATURES AND BENEFITS

Dynamic Isolation™

Unisys Stealth Dynamic Isolation™ capability lets you rapidly isolate anomalous or potentially compromised endpoints, providing your organization time to investigate and remediate the situation without further compromise of your users, data or systems.

Dynamic Isolation can:

- *Improve resilience to threats inside the enterprise with fast detection and response*
- *Isolate a user, device and other threats to quickly minimize damage*
- *Neutralize threats and restrict access appropriately*
- *Leverage automation and analytics to continually improve security detection and response*

Identity-Based Micro-Segmentation

Stealth creates cryptographic communities of interest (COIs) that limit access to users, applications and data assigned to the COI.

Hyper-Secure IPsec Tunnels

Stealth provides military-grade encryption to strongly protect data from end to end.

Orchestration and Deployment

Stealth processes are highly automated and centrally managed, so changes to security policies instantly propagate across the enterprise.

Work Better and Safer in the Now Platform® with Unisys Stealth

Add Unisys Stealth® protection to your ServiceNow® environment and experience a new level of resilience in your security operations center. Unisys Stealth helps analysts quickly address security threats within the Now Platform®, allowing companies to remain up and running and retain access to vital services and devices even if part of the network is compromised.

The Now Platform with Unisys Stealth enables your IT team to resolve problems faster and smarter by using automation to quickly isolate the threats that impact your business most. This effectively scales their ability and enables them to take on the ever-present high volume of phishing and ransomware.

Stealth™, when incorporated into the Now Platform, enables organizations to quickly respond to security threats and dynamically isolate devices in near real time—and it's as easy as pressing a button on the ServiceNow console. This capability gives ServiceNow customers a single place to track and act upon security incidents that occur in their environment.

In this way, Unisys Stealth and ServiceNow provide a single pane of glass for analyzing and consolidating the massive number of potential threats that flow into your data center. Should an endpoint or server become compromised, Stealth automation and Dynamic Isolation capabilities can shut it down instantly before it spreads.

Respond to Threats Faster with Dynamic Isolation™

Unlike other cybersecurity technologies, like quarantine, Unisys Stealth Dynamic Isolation capabilities are unique when it comes to operability and recovery. Usually, quarantined devices are out of commission until they are reimaged. But with Stealth, the forensics team, the operations team, and other critical services essential for operation can virtually move an asset out of production to a secure software-defined remediation environment and—in the same way—move it back into production after the threat is neutralized.

Dynamic Isolation works in conjunction with your SIEM software and threat detection tools to prioritize security operations by identifying endpoints that have already been compromised. This allows operations and security incident response teams to quickly access the endpoint and use ServiceNow security processes and technologies to remediate the incident remotely, without widespread disruption. As a result, the security team can quickly isolate the endpoint with surgical control and minimal configuration to eliminate downtime.

Unisys Stealth Dynamic Isolation bring fast isolation and fast deisolation to the Now Platform. It enables an enterprise to instantly remove a single device (or 10,000 devices, if necessary) from the network at malware speed and bring them back just as quickly—with one click, or in a completely automatic way.

While other cybersecurity solutions focus on detection and inundate the IT team with alerts, ServiceNow and Stealth can align related threats, prioritize them, and provide IT professionals with a quick and easy way to respond to them.

Unisys Stealth Extends Security, Resilience and Trust

Unisys has long helped organizations achieve the security and stability they need when executing and delivering large-scale transformations. With comprehensive industry knowledge, Unisys understands that different organizations have different needs, and designs its solutions accordingly. Everything is security-centric, using an always-on approach to create a resilient enterprise

so organizations can keep the lights on when they come face to face with security threats. It's a proven zero-trust and micro-segmentation model of threat management and operational resilience that fits perfectly within the Now Platform. With increased security comes accelerated innovation, service delivery, and lower costs as the focus shifts from crisis to confidence.

ServiceNow Makes Work, Work Better

ServiceNow drives digital transformation and makes the world of work, work better for people by digitizing and automating workflows across an enterprise. This cloud-based platform enables solutions that help companies quickly deliver new apps to market while diminishing the need for IT service staff. These digital workflows create great experiences and unlock productivity for employees and the enterprise.

As businesses grapple with disruption and uncertainty, ServiceNow helps them manage each crisis, build resilience, and mitigate risk enterprise-wide.

Most solutions are too slow to address catastrophic cybersecurity events.

The Ponemon Institute says the mean time to detect a breach is 197 days. Responding to a breach typically takes another 69 days.



*Unisys Stealth is different.
It acts at malware speed.*

Unisys Stealth enables endpoints—and, thus, people and systems—to continue working even when they're in safe mode.

**To learn how Unisys Stealth and the
Now Platform can protect your workplace, visit
www.unisys.com/strategic-alliance-partners/servicenow**



For more information visit www.unisys.com

© 2021 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.