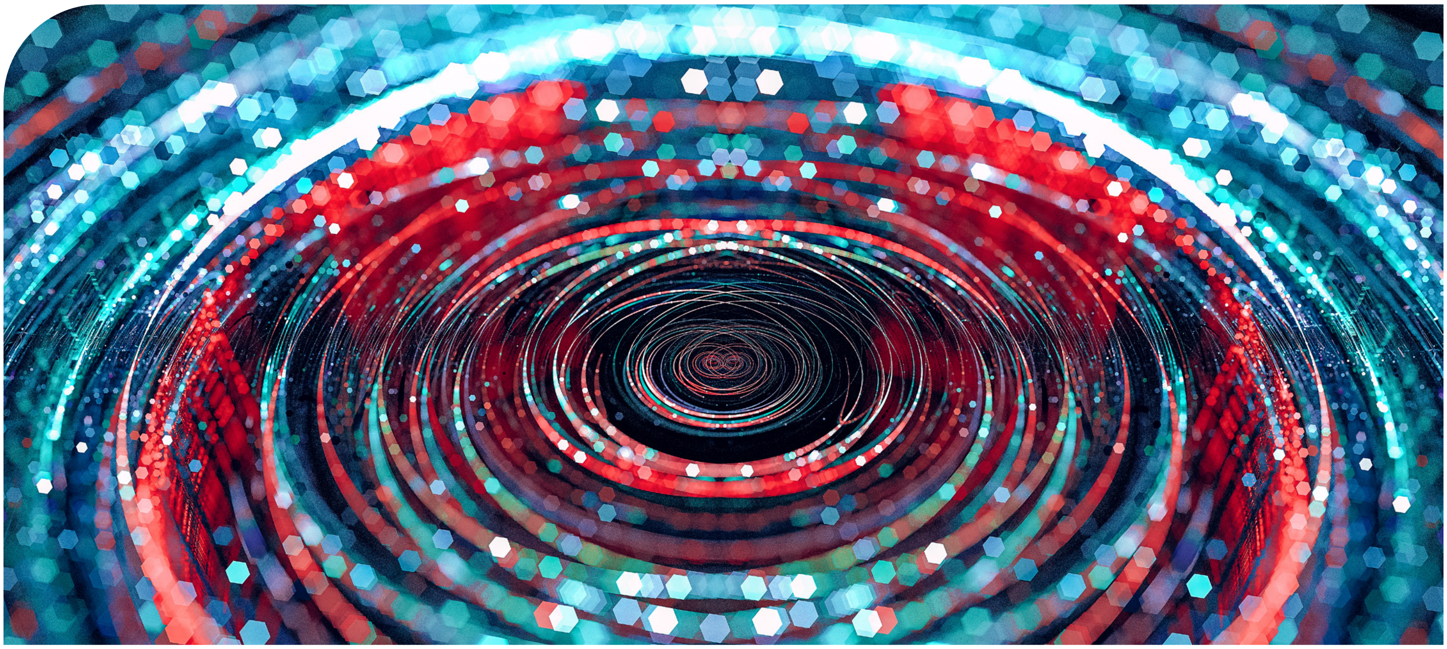

Use case

Zero Trust security at Unisys

Industry challenge

Cybersecurity, the art of the possible

At Unisys, when we talk cybersecurity, we realize our challenge is no different from that of industry at large. In this age of cloud-enabled digital transformation, cybersecurity is an ever-urgent, ever-expanding trial. We recognize that a breach-proof enterprise is impossible. We aspire instead to a robust security posture, armed with rapid detect-and- respond capability—one guided by the principles of Zero Trust.

Cybersecurity, in particular Zero Trust security, is “the art of the possible.” Leaders of all enterprises are challenged to do what is feasible, achievable – to take advantage of solutions that are immediately available and have been deployed successfully by their creators. Nobody wants to be the test case user for Zero Trust security.

Unisys identified five major cybersecurity challenges common to most enterprises in their Zero Trust journey:

Slow response allows bad actors to do more damage. Across the industry, numerous studies have reported the mean time to identify a breach is typically more than 200 days, and the mean time to contain one is more than 70 days. Enterprises need to accelerate their ability to isolate an intrusion, defuse it, and limit the damage.

VPNs expose more assets than necessary for individual users. When users need access to an enterprise’s applications, the only way in is through the VPN, but that opens the entire intranet to the user. It also requires network administrators to constantly add and subtract access by third-party contractors, vendors, and partners - a complex and time-consuming task for IT.

Assets on the cloud can inadvertently expose access. One of the biggest challenges organizations face is that moving workloads to the cloud opens up new attack vectors. Typical security issues in the cloud include data exposure from simple misconfiguration, lack of focus on host management vulnerabilities and non-compliance with regulatory requirements.

Conventional microsegmentation is expensive and can take years to perfect. Enterprises need a platform that provides immediate, powerful security benefits while they proceed with microsegmentation.

Cybersecurity implementation is typically disruptive and capital-intensive. Enterprises need a solution that doesn’t require them to reconfigure their entire environment, so that they can deploy it rapidly, and which requires only OpEx, not CapEx investment.

Security solution

Achieve Zero Trust security with Unisys

Unisys has been proactively overcoming these challenges in our own Zero Trust implementation. We took a phased approach, repeatedly testing, perfecting, and then expanding. We took years, so that you can do it in months.

Protecting our core – We started with our fundamental systems. We used Unisys Stealth® for foundational capabilities—identity-based microsegmentation, dynamic isolation, cryptographic cloaking and encryption of data in motion. We transformed our existing environment into a Zero Trust Network without network or application changes. As we did so, our implementation was so transparent and so non-disruptive that most of our users were unaware of it.

Confidence in the cloud – As we moved data to the cloud, we had confidence that it would be protected, thanks to Unisys Stealth. Realizing that anything you can see can be hacked, but what you can't see is much less likely to be hacked, we cloaked our presence on the cloud with Stealth. Although we share cloud-space with hundreds of other tenants, intruders are challenged to discover our presence.

Limited-Access VPN – By installing Stealth on all of our thousands of Unisys workstations, we are now able to give each user limited access to targeted applications only, without exposing our entire intranet. This has massively reduced our attack surface and exposure to user error. Ultimately, the goal is to eliminate VPN access for all but a few power users who need specialized network access.

Streamlining our network

Leveraging the use of Stealth on all user endpoints, we've re-architected to eliminate corporate office networks and most site-to-site connectivity. This has reduced operational costs and strengthened our Zero Trust security posture. There's no longer a network to breach in a corporate office - if a bad actor breaks into the Unisys wifi network, all they have is access to the Internet.

Enabling dynamic isolation – To rapidly quarantine compromised devices and prevent malicious activity from traveling laterally across our network, we enabled dynamic isolation. Within seconds of detection, Stealth applies dynamic security rules and reduces or removes access paths between workloads, leveraging the enterprise's existing detection, prevention and network traffic analysis solutions.

Again, we took our time to perfect our deployments, so that we are prepared to do it in a matter of months for you.

Business value

All the security that's possible today, proven in a large, complex enterprise

Our ongoing Stealth deployments have already delivered generous value to Unisys, and there is more to come. So far:

- Our core systems are cloaked to those who would wish to steal, damage, or hold them hostage.
- Our public cloud workload is obscured to other tenants, which gave us the confidence to shift 90% of our data to the cloud. This made us less dependent on our host's security measures.
- We can be confident that our network is not unnecessarily exposed to severe damage from end user error or malicious intrusion.
- We have improved end user experience, providing a seamless, consistent approach in the office, at home or traveling. And, our users can securely "wifi anywhere" without a VPN.
- We are saving $2.5 million per year by eliminating private networks and their associated costs.
- And above all, Unisys is prepared for the future, whatever it brings. Unisys is able to address both current and emerging security challenges with our Zero Trust implementation.

Unisys is positioned to bring similar Zero Trust security and business value to you, just as we have for government and commercial organizations around the world. Call us today to learn more.

For more information visit unisys.com/security.

unisys

unisys.com