unisys

Executive brief

Zero Trust, immeasurable security

Implementing Zero Trust for real results

Zero Trust at Unisys

At Unisys, we subscribe to the Zero Trust paradigm to secure our own infrastructure, embracing it's core concepts:

- Trust no user or device
- Trust nothing inside or outside the private network
- Enforce least privilege access

We've brought these concepts to life by operationalizing Zero Trust in our environment in a variety of ways:

- We don't trust laptops connecting to servers, so we establish session-based security in real time
- We don't trust the network, so we eliminated office networks
- We don't trust site-to-site connectivity, so we eliminated private network links

In today's economy, the growth in cyber connections is mirrored by the growth in cyber risks. Confidence in enterprise security has been eroding for years, with hacks, attacks and data breaches top of mind for executives everywhere. At risk is the loss of sensitive data, potential fines and reputational damage.

The problem is that traditional solutions are showing their cracks as cyber risks grow. VPNs have porous security, few organizations can stop an attack in its tracks and backups are far too risk prone to promptly restore operations after an attack.

What's needed is a better approach to cybersecurity – which is exactly what Unisys delivers. Our experience is broad, our expertise is deep and our solutions are innovative. We respond to emerging trends in cybersecurity with solutions and services designed to secure your environment, no matter how many connections you make.

Commit to Zero Trust

The Unisys approach to cybersecurity starts with Zero Trust. Access is granted securely only to the data and applications your people need to do their jobs – just when they need it and only for the time required.

Unisys can help you implement a Zero Trust architecture that meets the challenges of next-generation cybersecurity.

- **Minimize the attack surface** by limiting access to devices and data with Unisys Always-On Access™.
- **Respond to attacks** faster with Dynamic Isolation.
- **Recover from attacks** with confidence using Cyber Recovery.

Always-On Access

Controlling secure user access to network resources is increasingly important – particularly as your remote workforce grows. For this critical task, most organizations use VPNs. But VPNs are risky.

The problem is that they're built on an assumption of what it means to be in an office – namely that once you're in, you should be able to roam wherever you want. Whether or not this level of access was ever true for physical offices, it is extremely risky in a digital world.

We help you ditch the VPN in favor of a Zero Trust architecture that protects your network by granting access to resources based on user identity. We call this Always-On Access.

Leveraging microsegmentation, this solution grants secure user access to applications and data – but not to the underlying infrastructure. Access is determined based on least privilege in accordance with the principles of Zero Trust. This reduces the attack surface without impeding authorized access for employees.

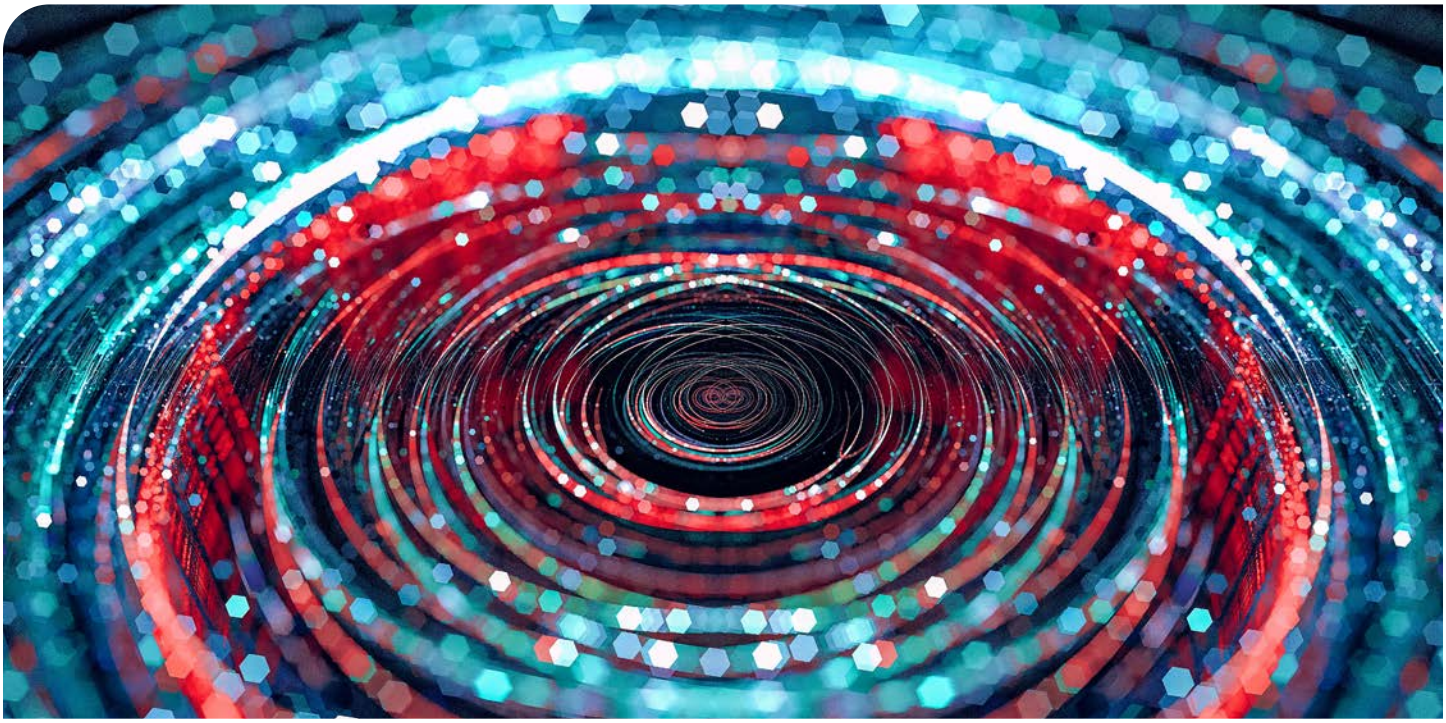
With Always-On Access, the user security experience is seamless and consistent – in the office, at home or on the road, with no VPN required. What's more, an Always-On Access deployment can be extended to eliminate private network links between corporate offices – saving money and further shrinking the attack surface. Your organization is better protected against bad actors seeking to exploit vulnerabilities.

Dynamic isolation

Your teams must quickly isolate compromised devices before an attack spreads laterally throughout your network. Typically, this means taking the device out of commission. Dynamic Isolation works differently.

Rather than powering down or decommissioning a potentially compromised device, Dynamic Isolation simply isolates it until your teams can investigate. You can apply different levels of isolation with varying degrees of restrictiveness based on the relative risk profiles of a given security event. This helps to limit the impact on business operations, giving your organization the flexibility to maintain as much functionality as possible.

In scenarios of high confidence, Dynamic Isolation can be automated as well. Take, for instance, a server that is configured to never make outbound communications. If our technology detects that such a communication is attempted, it can automatically and immediately isolate the device. Once remediated, bringing the device or user back online is as simple as restoring standard security policies. This helps to speed the ongoing work of cyber detection and response.



Cyber recovery

Like many organizations, you may configure your network so that your backup servers can access your corporate servers. The problem is, these backup servers are often accessible from user-based infrastructure, such as laptops, desktops and virtual machines.

But what if you have to recover from your backups after a security incident corrupts critical systems? If these backups are connected to the corrupted production systems, how can you ensure they're clean?

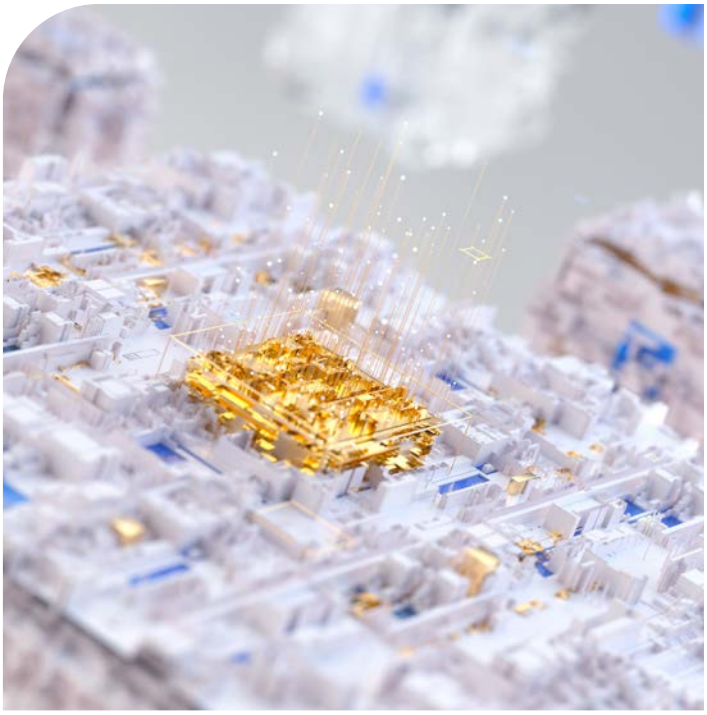
Unisys helps you solve this problem through a unique integration with the Dell Cyber Recovery solution that automates the replication, analysis and creation of gold copies of critical data to a Cyber Recovery vault.

We've built a cryptographic wrapper around the Dell solution to protect it from unauthorized users and devices, ensuring that clean backup data is protected and available to quickly restore business operations.

Backups are highly vulnerable because they're often connected to live systems but monitored with only a fraction of the same diligence. We help to ensure that what happens in your production environment does not cross into your backups. When disaster strikes, you can create a clean white room on the fly and start the recovery process with confidence.

Protect your systems and your reputation

With Zero Trust security expertise from experienced Unisys cybersecurity professionals, you can move to the next generation of cybersecurity, where access is based on identity and least privilege.



No special hardware is needed, and our technology works across on-premises, cloud and hybrid environments – seamlessly integrating with existing architectures to improve cybersecurity for you, your employees and your customers.

To meet today's challenges, cybersecurity must be modernized. Unisys can help you transform cybersecurity so that you can keep your systems safe, your risk exposure low and your reputation intact.

To learn more about Cybersecurity Solutions from Unisys, visit www.unisys.com/solutions/cybersecurity-solutions.

unisys

unisys.com

12/22 22-0509