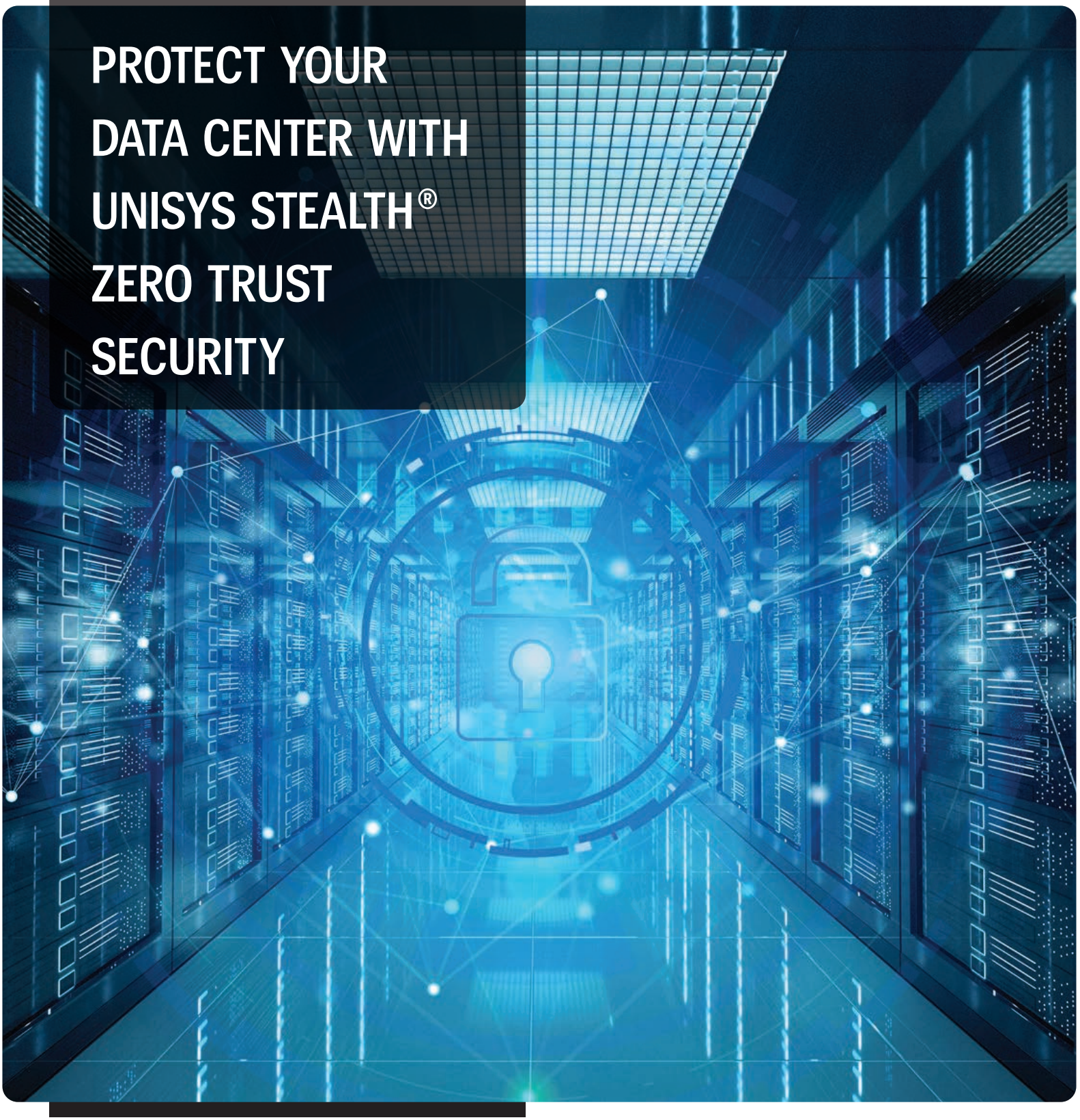
PROTECT YOUR DATA CENTER WITH UNISYS STEALTH® ZERO TRUST SECURITY



STEALTH™

Your network today extends well beyond the traditional boundaries once imposed by the company LAN and the four walls of the data center. Your business relies on access to sensitive information and applications from branch offices, IoT devices, mobile employees, partners, vendors, customers, suppliers. Cloud-based workloads are pushing your network edge farther and farther away from the control of IT. And in the post-pandemic world, the decentralization of your network has only accelerated.

What hasn't changed, however, is that your data center serves as the hub of this ever-expanding network of interconnected devices, people, and data. This makes your data center an attractive target for hackers because typically it houses your organization's most sensitive data and applications. These may include financial information, IP and trade secrets, customer data, as well as the HR, ERP, CRM, finance, supply chain, and other applications that serve as your business and operational backbone.

The attack vectors and areas of exploitation are varied and include: porous corporate networks that are responding to an increasing number of API calls; open ports; unsecured devices; lax, missing or unenforced security policies; partner access to sensitive data and applications; configuration errors; missed updates and patches; outdated and unsupported hardware and software; insider threats; malware (in all its forms); and open, unsegmented network architectures inside the data center. The list is long and grows longer by the day as you expand your digital footprint.

Cloudy Complexity

Unless it is completely cloud-based, you run your data center alongside one or more public cloud providers. While giving your organization an elastic infrastructure that responds quickly to changing business resource needs, this scenario introduces vulnerabilities as the attack surface expands to include any security issues within your cloud provider's infrastructure or with its employees. And then there are containers and virtual machines, which are spun up and decommissioned with such ease and frequency their numbers can increase. Microservices architectures also add to the problem as application functionality is being broken apart into independently deployable services that are called by many different applications across your enterprise.

This growing complexity creates a spaghetti diagram of east-west/north-south data and application traffic that is nearly impossible to decipher, track, or effectively secure. Nor are these dependencies static. Every time someone or something is added to or removed from the network, your diagram changes. It is precisely this complexity that allows bad actors to hide in plain sight – exploring your network, learning patterns, and finding security holes – until the time is right to strike.

High Walls and Deep Waters

The traditional castle-and-moat security strategy that places the deepest water and highest walls around the data center's perimeter does little to protect your data and applications inside.

Once an intruder breaches your perimeter, they are free to roam undetected and undeterred, for long periods of time. They do this by a variety of means, including using PowerShell commands to move around without triggering IDS/IPS systems. In fact, the average dwell time for hackers before they are discovered often is measured in months, not days, or hours. Some malware goes undetected for years. Even when your networks are segmented using firewalls, subnets, and VLANs, configuration errors and complex, inflexible routing schemes can create as many problems as they solve.

Given all of these issues, the key to greater security is focusing your efforts on protecting what thieves are after in the first place: data. This can be done by using encryption and by limiting and controlling access. Both approaches are enabled and enhanced by implementing Zero Trust cybersecurity architectures that, unlike perimeter-style defenses that only see the outside world as a threat, work by assuming all network traffic is suspect and cannot be trusted. This is where Unisys Stealth® comes in.

Unisys Stealth Zero Trust Data Center Solution

Unisys Stealth is software-defined security. It simplifies yet improves network security and serves as the backbone of your whole-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.

With Stealth, orchestration and deployment are highly automated and centrally managed. As your security policies evolve, changes can be made and instantly propagated across the enterprise. Meanwhile, Stealth monitors and enforces your Zero Trust policies, automatically isolating violators 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.

Stealth delivers Zero Trust through micro-segmentation, compartmentalization, and the creation of Communities of Interest (CoIs). These secure enclaves rely on hyper-secure IPsec tunnels between CoI endpoints that encrypt data from end-to-end. Outsiders cannot gain access into the CoI, and data cannot be exfiltrated out.

Applications and servers within the CoI will not respond to pings, scans, or other means of network reconnaissance, rendering attackers blind to network topology and application dependencies. All elements within the CoI are invisible to outsiders, thanks to Stealth's patented SCIP protocol that "cloaks" endpoints. Best of all, Stealth scales quickly, easily and works on any existing TCP/IP network—on-premise, in the cloud, or integrated into your partner's network.

Because Stealth is an overlay networking technology that works at OSI Layer 3 (the network layer), application latency is not an issue. Lightweight agents are installed on all endpoints to facilitate authentication. Roles and authorizations come from either Microsoft's Active Directory or LDAP calls to Identity and Access Management (IAM) systems.

Endpoints such as low-power IoT sensors and devices are protected via Wire component that sits between the device(s) and your data center. Secure Virtual Gateways (SVGs) act as the de facto agent for these devices, allowing them to be assigned to CoIs. SVGs can be configured to apply different roles to single or ranges of IP addresses.

CoIs do more than limit endpoints and user access to just the data and applications they require: They help simplify your data center architectures and topologies and your compliance auditing as well as by speeding up the detection and isolation of malware and Advance Persistent Threats (APTs) when they materialize.

Via its EcoAPI, Stealth integrates with third-party Security Information and Event Management (SIEM) tools which can trigger Stealth to dynamically isolate suspected bad users or devices in seconds. This helps protect you from highly destructive, fast-moving and networkwide malware attacks like the WannaCry and NotPetya viruses that cost companies and governments in 150 countries billions of dollars in lost revenue and direct costs.

By enforcing least-privileged access to data and applications, Stealth renders insider threats less impactful. And the same security policies work everywhere regardless of environment—on-premise, in the cloud, or hybrid.

To speed deployment and increase precision of security rules, Stealth automatically suggests micro-segementation policies for endpoints and applications. Stealth is managed using an intuitive interface in conjunction with a robust set of PowerShell cmdlets and RESTful APIs.

Stealth has been enhanced to include these Zero Trust capabilities:

- Automated, robust enterprise security that features AI and machine learning capabilities to reduce complexity by translating thousands of network communication flows into a streamlined set of security policies. The easy-to-use deployment Wizard enables quick implementation, while a robust API framework automates all Stealth installation, configuration and deployment activities – which can be done remotely and with thousands of endpoints installed at the same time in minutes.
- A state-of-the-art visual interface that provides unmatched ease-of-use. Stealth's visualization of the network environment makes it easy for organizations to spot potentially harmful traffic that needs to be secured immediately. It also provides at-a-glance insight into the applications and traffic flows that are protected by Stealth.
- A comprehensive, real-time security dashboard that provides you with a clean, simplified look at the status of your network in a single view. This enables you to safely address your business outcomes with immediate insights about the environment to enable informed decisions, meet compliance requirements and improve the overall security of your enterprise.

Stealth Data Center Benefits

By deploying Stealth, you get speed to security and speed to Zero Trust—all with your existing data center infrastructure and applications. You won't have to rip, replace, or deploy new infrastructure of any kind. This means reduced costs for you.

One benefit of Stealth over solutions such as subnets and VLANs is that it enables organizations to run data centers securely with less expense and management overhead by reducing reliance on complex integration of security solutions such as firewalls and Access Control Lists (ACLs). This lessens network complexity, which, by itself, improves an organization's risk profile. As another benefit, Stealth significantly reduces the attack surface by limiting the number and type of users and devices that are visible to the outside world.

Because Stealth is deployed as an overlay network using endpoint agents for authentication and authorization, it easily can be extended to grant partners and vendors secure access to only the applications and data they need to provide services—and nothing more. Even if they are hacked—like the HVAC provider in the Target breach—Stealth contains the breach to just those systems and prevents data exfiltration.

And, as a software-defined framework takes over your data center operations and management, Stealth can evolve right alongside it, scaling up and out as needed. For example, one Unisys client used Stealth to help reduce its data center footprint from 52 data centers to just two.

Best of all, Stealth offers peace of mind to IT security leaders and their cybersecurity teams by providing a Zero Trust security strategy that uses one of the most proven, cost-effective end-to-end security systems available on the market today. Stealth currently is deployed worldwide across a wide range of verticals including federal, financial, pharmaceutical, industrial, energy, medical, education, and the DOD, and has yet to be breached by penetration testing or red teams.

The world is changing, and you must adapt to stay ahead of data center threats. Stealth serves as the backbone of your Zero Trust security strategy by micro-segmenting data centers into hyper-secure enclaves that keep users safe and hackers out.

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

For more information visit www.unisys.com