UNISYS | Securing Your Tomorrow®

Use Case

Learn more about how Unisys Stealth solutions and services help organizations architect, build, and maintain Zero Trust at www.unisys.com/Security.

STEALTH™

Request an Assessment at www.unisys.com/contact-us

Increase Compliance Agility

While regulatory compliance may mean different things to different organizations, what they all have in common is the need to meet or exceed the cybersecurity and data privacy controls that come with working with specific types of data or doing business in regulated industries.

- In healthcare, it's HIPAA. If you work with credit card data, it's PCI/DSS. If you do business in the European Union, it's GDPR. For the US government, it's FISMA, FedRAMP and a host of others. The list of compliance frameworks is a long one and varies by industry.
- Most of these regulations are broadly written to focus on an ideal end-state, not how to get there. In most instances they are not prescriptive; they do not dictate the technologies, procedures, or polices that have to be in place to meet their requirements.
- Technologies that meet compliance requirements today may fall short tomorrow.

Stealth Zero Trust Compliance Solution

Unisys Stealth® is software defined security. It simplifies and improves network security and serves as the backbone of your Zero Trust security strategy. Stealth™ overlays every corner of your organization's computing environment with one holistic, consistent, and unwavering security policy —from desktops toservers, cloud, mobile and even IoT.

- Stealth delivers identity-based microsegmentation by creating cryptographic communities of interest (COIs) that limit access to just the other users, applications and data also assigned to the COI. Stealth COI's are dark to unauthorized uses and data cannot be exfiltrated.
- Stealth uses hyper-secure IPsec tunnels leveraging robust, military grade encryption to strongly protect data from end to end.
- 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.
- Stealth monitors and enforces all your Zero Trust security policies, dynamically isolating potential threats and alerting administrators. Stealth security is seamlessly woven into the fabric of your entire network. It's the engine that drives your Zero Trust security strategy.

Stealth helps you achieve regulatory compliance – it limits the scope of audits by reducing the number of endpoints that can reach data that must be secured. Because data is isolated in highly secure, cloistered enclaves, Stealth allows auditors to focus on just the users, applications, and devices that have access to sensitive data. In addition, Stealth activity logs give auditors a clear path to follow while confirming network protection guidelines in certain frameworks.

Reduce Compliance Cost and Complexities

By deploying Stealth, you get both speed-to-compliance and speed-to-audit—all with your existing infrastructure and applications. There is no need to rip and replace anything. By relying on cryptographic IPsec tunnels to establish COI based on least privilege access to networks, applications, and data, you can sleep well at night knowing you have deployed one of the most advanced cybersecurity platforms in the industry. Compliance is simplified and auditing is streamlined.

- Enables you to build a trusted and secure network on top of an existing infrastructure
- Reduces infrastructure attack surfaces while expanding network reach and access, dramatically reducing systems and users that are subject to audit
- Encrypts data in motion, meeting a key requirement of many compliance frameworks
- Prevents data exfiltration ensuring privacy to non-approved applications and users
- Renders attacker's network reconnaissance efforts ineffective—protecting data in motion within hyper-secure, compliant COIs
- Ensures easy-to-deploy role-based compliance protections for every user and endpoint on the network