



Unisys Stealth Solution Suite

You can't hack what you can't see. Changing the Security Paradigm.



Introduction

The best way to keep something secure is to make it invisible. Unisys designed the Unisys Stealth Solution™ (“Unisys Stealth”) with this simple concept in mind: develop a tool to cloak data, applications and users from hackers on any network, anywhere, anytime.

Today's business users are accessing sensitive company data around the globe and around the clock, not only on company devices but personal ones as well. This new world has changed the requirements for data security and is one of the biggest challenges of CIO's and CISO's, and a constant concern for CEO's.

Unisys Stealth is a visionary approach to solve today's security challenges. Security is not about building a fortress; it's about creating secure communities. Unisys Stealth grants access based on trusted identity, cloaks connections and is designed to obscure end-points to hackers to remove your infrastructure from harm's way. You can't hack what you can't see.

Changing the Security Paradigm

Increasingly sophisticated security threats are rising exponentially, internally and externally, attempting to steal and profit from an enterprise's data. The *McAfee Threats Report* for March 2012 shows the number of *malware threats rising over 83 million*. Results from the *Unisys Security Index* from March 2012 show *59% of global respondents are very concerned about un-authorized access to or misuse of their personal information*.

The current security paradigm, which attempts to achieve network security using an intricate design that includes costly physical infrastructure, frequently from multiple vendors, is clearly not good enough. Also, once it is in place, organizations are reluctant to make a change and cannot even be sure their data is protected.

Unisys Stealth changes the security paradigm. Unisys Stealth is a single security technology that increases data protection, simplifies management and reduces reliance on physical infrastructure. Unisys Stealth eliminates the trade-off between cost and risk, because trade-offs are not good enough.

Good Enough Security is Not Good Enough

Securing your infrastructure and intellectual property to keep ahead of hackers is a never-ending battle. New viruses, scams, and malware attack organizations everyday costing impacted organizations \$5.5M annually, according to a recent Ponemon Institute survey. Organizations make tradeoffs between the cost to secure information and the risk of compromise, settling for just enough with the hopes that the holes are not exposed.

To secure the environment to meet the seven security principles listed below using traditional offerings requires multiple solutions from multiple vendors. This creates complexity, system overhead and is cost prohibitive.

- Confidentiality
- Integrity
- Availability
- Authorization
- Authentication
- Non-repudiation
- Audit-ability

Traditional security is focused on fortifying the boundaries but not really addressing the limitations of physical security. Once a hacker gets through the wall, they are free to compromise information across the network costing organizations millions, lost IP, and their reputation.

Unisys Stealth offers a visionary approach to managing the seven security principles within one suite of tools.

Unisys Stealth is designed to secure the infrastructure by cloaking data communication end points on the network, making them obscure to outside hackers and segmenting the network virtually, not physically; even if hackers could break through the perimeter, they would be contained in a controlled area limiting access and risk.

Beyond securing the end points, remote users, datacenters, and data, Stealth provides an audit trail to help comply with SOX rules, HIPAA requirements and other regulations. Stealth can layer with existing security, reduce the need for expensive hardware solutions, and replace outdated security products when it is time to upgrade, thus reducing the need for multiple vendors and complex configurations.

With Stealth, you get ahead of hackers with enterprise -class security, never settling for good enough again.

Stealth Differentiation

Without having to reconfigure your network, Stealth enables you to achieve a combination of defense-grade security, flexibility and business value.

Unmatched Data Security

Unisys Stealth has passed extensive testing and is NSA EAL4+ certified. It offers unprecedented, certified data security from internal or external theft, misuse, or corruption.

Simplified, Agile Security Management

Unisys Stealth user administration is integrated with identity management systems, such as Microsoft Active Directory and Radius OTP. Because Unisys Stealth segregates networks based on the user's identity and not by physical network jack, users are able to freely move about in the organization while maintaining their "logical location" in the network.

Easy to Deploy

Unisys Stealth does not require any application changes or expensive network re-engineering. And it is easy to incrementally integrate into an existing network infrastructure.

Different Approach to VLAN

Unisys Stealth offers a cost effective, easy to implement alternative for network segregation. While VLANs separate networks from switch port to switch port, Unisys Stealth segregates networks from endpoint to endpoint, thus offering protection for the "last 100 feet."

Higher Security with Less Disruption

VLANs "fail open" potentially exposing data, while Unisys Stealth "fails closed" on connection error, enhancing the protection of users on the network. Also, VLAN changes are disruptive, while Unisys Stealth updates are made through the identity management system and do not interfere with availability.

Alternative to VPN

Unlike traditional VPNs, Unisys Stealth uses unique security techniques to offer protection for the end-point, the communication channel from a remote location into the internal network, and from the intranet boundary all the way to the Stealth-protected servers and applications.

World-Class Intellectual Property

Unisys Stealth incorporates proprietary technologies, including those that enable the cloaking of Stealth devices from unauthorized eyes. These technologies are protected under an issued U.S. Patent and numerous pending Patent Applications.

Stealth Solution Offerings

The Unisys Stealth Solution Suite is unique because clients increase data security while simplifying security management, and clients can use public networks such as the Internet without exposing their data communications to cyber threats.

Stealth can be deployed within any industry; it is particularly applicable to healthcare, legal firms, financial services, public sector and Federal government agency environments, which all possess critically private information and are subject to stringent data security regulations.

Stealth offers military-grade capabilities designed to protect data and information across the entire enterprise - LAN, WAN, wireless, 3G, 4G and satellite networks, public or private – helping protect your valuable assets within any data center and across any multi-site enterprise.

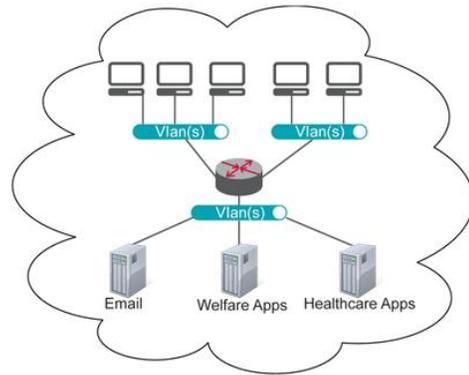
Data Center Segmentation

Enterprise data centers have been evolving over the last decade predicated by innovations in server virtualization and consumerization of IT. Today's security reality presents a critical need to restrict access to certain assets, specifically the servers executing strategic applications and housing the most sensitive data.

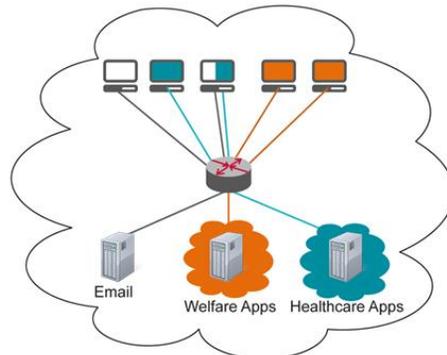
The traditional tiered network architecture accomplishes critical server and database security by physical network separation from other data center assets. Expensive and inflexible hardware configurations are deployed, but the infrastructure is still subject to the risks of VLANs and firewalls. If business requirements necessitate a change, a VLAN must be rewired and routers moved. Flat networks are more flexible and easier to administer, but any system on the network can see and access any other system. Thus, flat networks expose large portions of the enterprise when a compromise occurs.

Unisys Stealth provides a superior solution to either configuration. With Unisys Stealth, separation of critical servers and databases is achieved by using software to create secure group of users which we call Communities of Interest (COI). Far less network equipment is required leading to cost savings as physical tiers are retired. And on already flat networks, Stealth compartmentalizes the servers with COI, so that systems in different COI cannot see or communicate with each other. The result is cost efficiencies with much greater protection.

Traditional tiered network



Stealth Data Center Segmentation: Only the users in the "orange COI" can see and access the Welfare Application Server. Only the users in the "blue COI" can see and access the Healthcare Application Server. None of the servers can directly communicate with each other. One of the users in the blue COI is running the optional dual tunnel feature (configured only by the administrator) to concurrently access the Healthcare server via Unisys Stealth and the Email server in clear text.



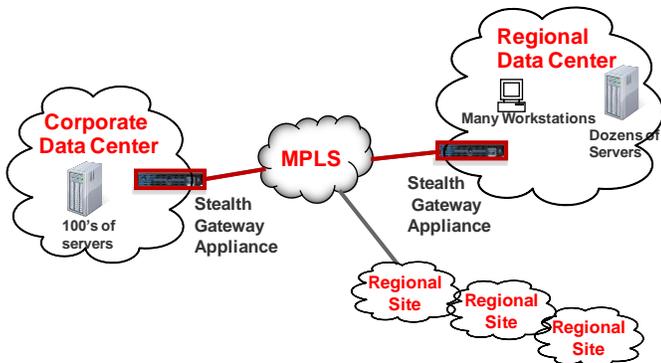
Regional Isolation

As companies look to multiple geographies for new business opportunities, they get exposed to new security challenges. Confidentiality requirements or geopolitical security threats may necessitate that systems at geographically dispersed centers be kept separate from the corporate data center. However, some regional access to the enterprise data center is required. And some 'super-users' may require access to a subset of systems at any location.

Consider an information embassy designed to protect data and resources within its boundaries and to control and secure access to and from the embassy. Unisys Stealth is designed to provide a solution to the regional data center challenge.

Using COI, Unisys Stealth helps secure sensitive data, servers and applications within a regional data center, as well as corporate assets in the enterprise data center, to accomplish these objectives:

- Isolate regional or site assets from local threats
- Further segregate regional assets from each other
- Allow selective and secure regional access to the enterprise network



Unisys Stealth is designed to secure the regional data center as well as the information assets developed at the site from local threats. Using Unisys Stealth to connect the regional data center, through a Stealth gateway “border crossing agent”, back to the corporate data center provides access to corporate servers, data, and applications to only those with explicit permission.

How Stealth Works

Stealth employs a Unisys-developed information security architecture with four important elements that revolutionizes the approach to data protection.

1. The cryptographic service module provides FIPS 140-2 certified AES-256 encryption.
2. Stealth’s Information dispersal algorithm and data reconstitution scheme allows Stealth “shredded” messages to only be reassembled by Stealth.
3. Stealth creates a logical tunnel between data communication end-points to only those who are pre-identified as part of a COI. COI members seem as though they are alone on the network, and members have zero visibility to anyone or any devices not in the same COI.
4. Stealth executes very low in the protocol stack to conceal the endpoint from attack and deny unauthorized access. There are no changes required to applications in order to be protected by Unisys Stealth.

The COI capability combined with executing very low in the protocol stack enable endpoints to be dark on the network, as if they were “invisible”.

When a Stealth-enabled endpoint receives a message off the network, if the message is not a Stealth formatted message containing the specific key material for the COI authorized for the endpoint, the message is dropped. Stealth does not respond with any type of “negative acknowledgement” – it simply disregards the message. Hackers attempt to locate devices on a network by broadcasting network messages, and even a negative reply provides hackers what they want to know: the IP addresses of systems they can further probe for vulnerabilities. Stealth endpoints are removed as a target for hackers because the endpoints cannot be located by non-COI members.

An organization manages its COI members based on their user credentials and defined access rights, integrated with the organization’s identity management system, such as Microsoft Active Directory (AD). This integration provides seamless COI membership control and the ability to rapidly respond to business changes without re-cabling or physical network modification.

Why Unisys Security?

At Unisys, we design and develop mission-critical solutions that secure resources and infrastructure for governments and businesses. Our approach integrates resource and infrastructure security, creating the most effective and efficient security environment possible and freeing our client to focus on best serving its citizens and customers. Unisys security solutions can be found worldwide in 600+ airports, 1,500 government agencies, 100+ banks, among others.

The Unisys Security Index is a biannual global study that provides statistically robust insights into the attitudes of consumers on a wide range of security-related issues, including National security concerns related to terrorism and health epidemics; Internet security related to spam, virus, and online financial transactions; Personal security concerning physical safety and identity theft. For more information visit: <http://www.unisyssecurityindex.com/>

Acknowledgements

Unisys Stealth Solution Suite provides AES-256 encryption and a FIPS 140-2 certified cryptographic engine, which uses SecureParser®, a product of Security First Corporation.

For more information visit <http://www.unisys.com/stealth>

©2012 Unisys Corporation. All rights reserved. Specifications are subject to change without notice.

Unisys, the Unisys logo and Unisys Stealth Solution are registered trademarks or trademarks of Unisys Corporation. All other trademarks referenced herein are acknowledged to be the property of their respective owners.

Printed in the United States of America

August 2012