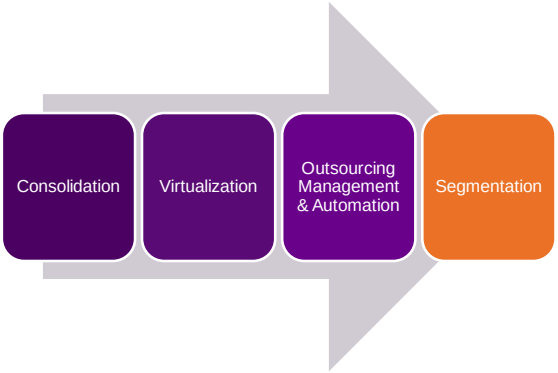
UNISYS

Unisys Stealth Solution Suite

Secure Data Center Segmentation: Cloak your Strategic Applications

Data Center Evolution

Data centers have evolved significantly over the last decade driven by business requirements to become more cost effective and efficient, and enabled by technology created to do just that. First, enterprises consolidated the data centers creating a unified corporate computing center. Next, servers and storage were virtualized to make data centers more effective and easier to manage, and to improve the environmental footprint. To further drive down operational costs, the management of the data center may have been outsourced and automated.



Today, the explosion in consumerization of IT, cloud computing and increasingly sophisticated breach attempts are driving more change and innovation to address new challenges in protecting high value corporate IP and assets. Enter the era of Data Center Segmentation: the latest evolutionary phase to properly manage the impact and leverage the potential of new computing while tightly controlling access to corporate servers, data, and applications.

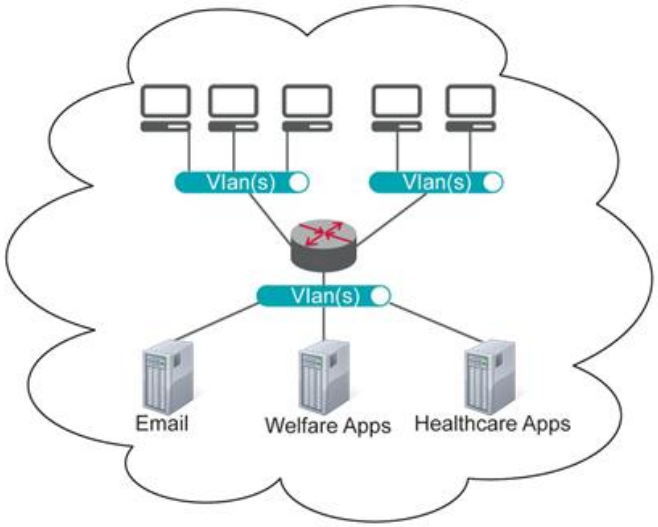
.

Unisys Stealth Securely Segments Data Centers

Unisys Stealth™ is designed to protect business data and systems by creating a communications tunnel that is cloaked to any users or devices except those who are pre-identified as part of the “secure community” referred to as a Community of Interest (COI). This is unlike traditional solutions, which use physical topology to cordon off and protect high value servers, virtual workloads and applications.

In a traditional tiered network, security is accomplished by physical segmentation. This requires additional network equipment and is subject to the risks of VLANs and firewalls. For example, if a configuration element is incorrect, VLANs “fail open” and a communication path is established.

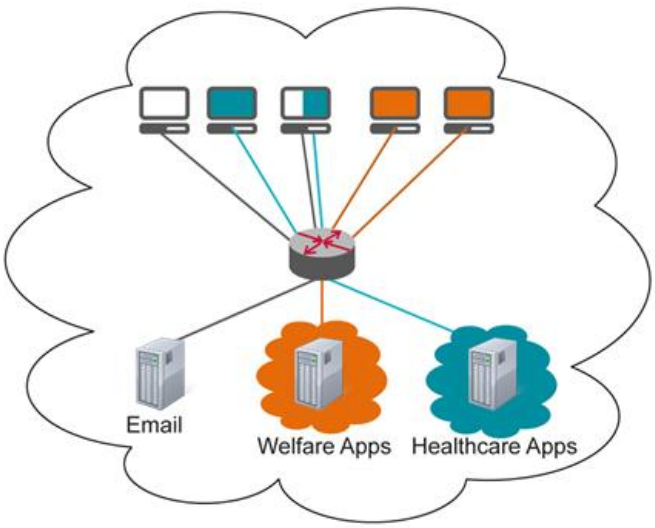
Traditional Data Center Segmentation



Maintaining multiple physical networks is expensive and complex, and managing user privileges which change as business requirements evolve can force physical network reconfigurations.

In contrast, Stealth enables security by using COIs, allowing the network to be simplified while protecting visibility and access to different servers and applications.

Stealth Data Center Segmentation



If the Welfare Applications in this example are strategic programs, only the users who dynamically receive the matching COI key information based on their user credentials will be able to see and access the servers housing those applications.

If an endpoint tries to connect to Welfare Apps and does not have the correct COI key configuration, which means that the endpoint is not a recognized member of the COI, Stealth "fails closed" and no communication path is established.

Stealth encrypts data moving between Stealth secured endpoints with FIPS140-2 certified AES 256 encryption. In addition, the Stealth message is formatted with specific COI key information which does not allow the message to be reassembled by any software other than another Stealth endpoint with matching COI keys. At the endpoints, Stealth can be configured to communicate via Stealth-secure channels and non-Stealth paths concurrently.

Stealth safeguards each endpoint by not interacting with any non-matching COI traffic. Stealth does not respond to any inquiring "pings" on the network or to any messages directed to it from a non-COI member. The communications and the endpoints themselves are dark, keeping them from discovery by hackers. You can't hack what you can't see.

Unisys Stealth is Easy to Integrate

In the case of flat network configurations, user access to servers and applications is often managed at a higher level, not at the network level. Enforcing security is a challenge because once on the network, users can find other systems even if they cannot access them directly, therefore setting the stage for exploiting vulnerabilities. Unisys Stealth is easy to integrate into environments configured as flat networks, all while offering superior security with no application changes.

Regardless of the starting point, Unisys Stealth can be deployed on top of the existing infrastructure. At the endpoints, Unisys Stealth can be configured to communicate via Stealth-secure channels and non-Stealth paths concurrently.

Managing Stealth devices and users is simple. Unisys Stealth integrates with Microsoft Active Directory and other identity management systems so that you can quickly set up and manage COIs. Users and systems are assigned to COIs based on their identity, not by physical location, so as these resources move between projects, a simple Active Directory change is all that is required.

The Stealth Solution results in equipment cost savings, simplified administration, and significantly higher data and application protection.

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.

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 www.unisys.com/stealth

Printed in the United States of America January 2014