MiStealth

Innovative security for mission-critical data and networks

Questions and Answers

1. What did Mitel and Unisys announce recently regarding Stealth and MiStealth?

On April 20, 1016, In partnership with Unisys, Mitel introduced MiStealth: A security technology to provide enterprises and service providers with secure mobile access to the cloud and to ensure they remain protected against security threats and data breaches. Combining Mitel's communications leadership with the security of Unisys Stealth™ identity-driven segmentation and encryption, MiStealth allows businesses to control who can access enterprise networks based on users' identities–whether within the enterprise or on the cloud–while reducing the attack surface and providing the elevated levels of security typically associated with private cloud deployments. MiStealth additionally simplifies security management, as users can access public networks (such as the Internet) without threat of exposure to their real-time communications. The solution also integrates with Mitel's RCS/VoLTE/VoWiFi clients to provide a seamless experience.

2. Who is Unisys?

Unisys (NYSE: UIS) is a global information technology company that works with many of the world's largest companies and government organizations to solve their most pressing IT and business challenges.

Unisys specializes in providing integrated, leading-edge solutions to clients in the government, financial services and commercial markets.

With more than 20,000 employees serving clients around the world, Unisys offerings include cloud and infrastructure services, application services, security solutions, and high-end server technology.

Key facts about Unisys

- *Formed in 1986 with the merger of Sperry and Rand.*
- *Technology leader for more than 130 years*
- *23,000 employees in over 100 countries*
- *FY 2012 revenue: $3.7 billion*
- *Only service provider with all global centers certified ISO 20000, 27001, 9001*
- *Hold more than 1,500 patents world-wide*

3. What is Stealth or MiStealth?

MiStealth is Mitel's exclusive version of Stealth(mobile)™. Stealth(mobile) enables authenticated and secure access to application processing environments in the data center from mobile applications. It leverages application wrapping software that encrypts data-in-motion from the mobile app across the Internet–securing it from hackers and evesdroppers. Stealth(mobile) secures the entire data path by protecting critical servers and virtual machines with micro-segmentation, connecting authenticated mobile users into secure Communities of Interest (COIs), and wrapping applications on the mobile device.

4. How long has Stealth been a product?

The crypto module of Stealth dates back to 2005. Stealth was first released as a product in 2007, and is now in version 3.0.

NORCOM

5. How does Stealth work?

Stealth is a software-defined security portfolio that delivers consistent, inimitable security for global enterprises focused on protecting data in their data center, cloud, and mobile infrastructures. Stealth was designed to deal with advanced threats in a completely new way; by substituting traditional hardware topology for software-based cryptography, Stealth's micro-segmentation solutions prevent unauthorized access to sensitive information and reduce the attack surface, thereby making endpoints invisible to unauthorized users.

Stealth operates between layers two and three in the protocol stack, transparently accepting and decrypting packets from authorized users, and silently discarding everything else. Thus if offers virtually no attack surfaces: It doesn't respond to pings or any other ICMP-based protocol. It doesn't reveal ports, and it doesn't offer any information to outside entities.

6. What is micro-segmentation?

Unisys takes the approach that Instead of building higher walls and monitoring massive volumes of security events, it's better to accept the inevitable truth: Malware will get in. But once it does, immediately contain the attack before any damage can be done. This way when malware does eventually get in, it's locked in a tiny micro segment, and can't get out.

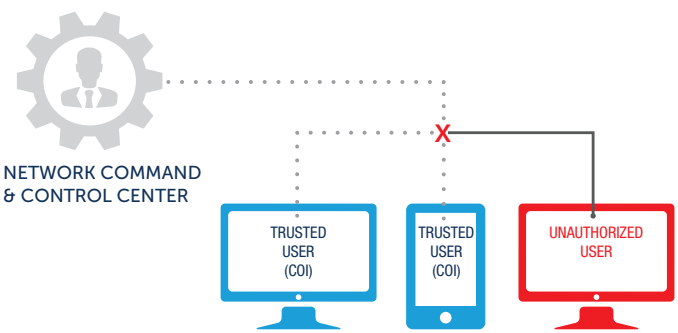
Unisys' implementation of micro-segmentation is very straightforward. It cryptographically isolates valuable endpoints down to the smallest levels at the packet level. And it organizes them into functional communities so that only the right people can do the right things. It works across enterprises and ecosystems. It works in challenging security environments. And it works in data centers with old and new systems, clouds, ICS/SCADA, and global mobile.

7. Can you provide some examples of "use cases" for a prospect who has end of life or older technology that is more apt to be hacked?

Unisys recognizes that many industries are faced with a difficult decision regarding outdated legacy systems, such as those running on Windows XP or Microsoft Server 2003. Very often these OS's are not running on traditional computers, but industrial control systems, or automated remote devices. Even ATMs. Very often, the OS is embedded in firmware, and cannot be upgraded. These IT managers are faced with three decisions: Abandon that hardware, and upgrade to newer ones; accept the risk imposed by a wildly unsecure OS; pay for custom support to the OS manufacturer.

Stealth offers a fourth, more economical solution: Isolate those legacy devices behind a Stealth Secure Virtual Gateway (SVG). The SVG can operate on public networks and securely communicate with other devices within its secure COI, while the legacy devices are able to communicate only with each other, and the SVG. They are cryptographically darkened to anyone outside the COI.

You Can't Hack What You Can't See



Go Invisible

You control who can access—or even see—systems.

8. What is Stealth(cloud)?

Stealth(cloud) allows IT managers to extend their secure data center into cloud-based systems such as AWS or Azure, using the same cryptographic keys and protocols, and preventing east-west breaches on cloud servers.

For details, see http://www.unisys.com/offerings/security-solutions/unisys-stealth/stealth(cloud)

9. What is Stealth(mobile)?

For details, please visit http://www.unisys.com/offerings/security-solutions/unisys-stealth/stealth(mobile)

10. What is Stealth(core)?

Stealth(core) is the heart of all Stealth solutions. It consists of various modules, including the Enterprise Manager system, which is a GUI-based console for administering all aspects of a Stealth environment.

http://www.unisys.com/offerings/security-solutions/unisys-stealth/stealth(core)

11. Does a client need to buy all three Stealth products, or can they use just one if that is their requirement?

Stealth(core) includes the administration, licensing, and crypto modules, and is required for all Stealth solutions. Mobile, cloud, analytics and identity are optional add-ons.

12. Is there a website that contains marketing information or white papers?

Yes. See http://www.unisyssecurity.com

13. Does Unisys provide professional services for implementation?

Yes. See http://www.unisys.com/offerings/security-solutions/professional-services for details

14. Does Unisys provide PS for security assessments if a client has that requirement?

Yes. Unisys Security Professional Services does vulnerability and threat assessments along with eDiscovery forensic data analysis, traffic flow analysis for network slowdowns, old legacy application security, and EDRM for litigious events–for both incident and non-incident related security.

NORCOM
TELEPHONY SOLUTIONS
Hosted • Premise • Virtualization

877-NORCOM1
norcomsolutions.com/mistealth