

# ***Unisys Stealth Solution for Network***

## **Secure Business Operations for the Trusted Enterprise**

With more than 50 years of mission-critical enterprise experience, expertise, and passion, we offer unrivaled quality and a complete solution set from a trusted partner.

**UNISYS**

Thank you for this opportunity to speak about how Unisys can help you make your enterprise a Trusted Enterprise, one that protects its reputation, its ability to operate smoothly, and its enterprise data.

Let me tell you just a little about Unisys. Unisys offers more than 50 years of mission-critical enterprise experience, expertise, and passion. For you, this translates into unrivaled quality and a complete solution set from a trusted partner. We provide best-in-class enterprise solutions to enterprises like yours. We are a trusted partner, and we work very hard to make you a best-of-breed Trusted Enterprise.

**NOTE:** Additional industry-specific information on the experience and expertise of Unisys in building trusted enterprises is available on the last slide.

# Unisys Stealth Solution for Network

## Security Risks Distract Enterprises from Focusing on Business



- Promote sharing
- Extend the enterprise
- Strengthen agility
- Ensure trust

For many enterprises, the vision for long-term growth includes several prevailing IT goals:

1. An increased ability to share information
2. Greatly expanded sources and forms of information and related expertise to support rapid collaborative decision-making
3. Highly flexible, dynamic, and interoperable communications, computing, and information infrastructures that are responsive to rapidly changing operational needs

And 4. Assurance and trust that the right information to accomplish assigned tasks is available when and where needed, that the information is correct, and that the infrastructure is available and protected.

Achieving this vision is a challenge. Today, the risk of a security breach has everyone's attention. No one wants to be the subject of a special news report or pick up that phone call that your data has been stolen.

I'm sure you can relate to this: one of our customers reported 2.5 MILLION security events per hour. Already, five to seven percent of all IT spending is earmarked just for security.

And as you well know, the consequences of a breach are far-reaching. You not only face the immediate direct costs, but you also might lose the confidence of your customers and stakeholders. 60% of customers who get one of those "we lost your data" letters are likely to take their business elsewhere.\*

All of this day-to-day security firefighting is distracting us from focusing on our real job—the long-term growth of our business.

\* Source: "2006 Annual Study: Cost of a Data Breach", PGP Corporation. Based on a 2005 survey of 51,000 adult consumers by Ponemon Institute, LLC. Of the 9,000 respondents who had received a notification that their information had been lost, "almost 20% terminated their relationship with the company," and "a further 40% were considering terminating their relationship." Only 14% were "not concerned."

# Unisys Stealth Solution for Network

## Every IT Executive's Challenge Is to Manage and Protect Data



- Data fortresses
  - Always a taller ladder to breach the walls
- Encryption
  - Data is intact and vulnerable
  - Stymies sharing

It is your responsibility to ensure that network data is secure, safe, and private. You need to know where it is, where it goes, who is accessing it every minute of the day. If there's a data security breach, it's your responsibility. So you'll do whatever it takes to keep it safe—even if that means implementing separate networks, which has been the approach so far.

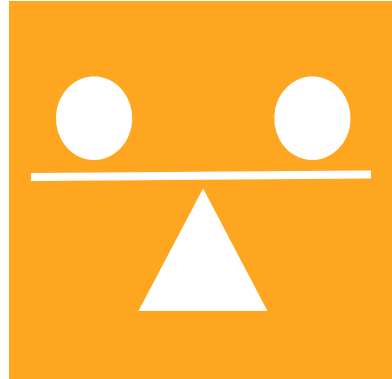
This is similar to building a data fortress around your network data. You have built walls around the data to keep it safe from harm or compromise. And as the data got tougher to protect, you built bigger and higher walls. Unfortunately, you just can't build security walls high enough. Someone will always make a taller ladder.

Another solution used to protect the data is to employ encryption. Unfortunately, traditional encryption is not the answer. It leaves the data intact and vulnerable, while stymieing the sharing of information.

# ***Unisys Stealth Solution for Network***

## **Balancing Security and Sharing Is Hard**

- Current security solutions
  - Ignore sharing
  - Make sharing too complex, costly, and time-consuming
- Multiple networks or silos inhibit agility



Keeping the data safe is simply not enough. Data must be shared so that decisions can be made and the enterprise can respond to market changes. As you well know, you've always faced tradeoffs between security and sharing. Enabling and controlling sharing in a secure way is quite a challenge.

Everyone wants to make services widely accessible and shareable. And new architectures—such as SOA-based systems—push to open rather than isolate data. But can you really open up sharing and keep network data safe?

Traditional network security solutions have not been able to address all four of those IT strategy goals simultaneously. Some only addressed security, leaving out sharing; others addressed both requirements, but are complex, costly, and time-consuming—certainly not the definition of agility.

Multiple networks have disadvantages: multiple sets of equipment, and significant cost for support, management, and administration. Having multiple networks is not an agile condition. It's cumbersome to manage and a pain for your users. If you have sharing requirements that cross different levels of security, it becomes even more complex.

# ***Unisys Stealth Solution for Network***

## **The Right Security Infrastructure Enhances Agility**

What if you could ...

Feel confident?

Share data?

Be agile?

What if security could unleash your full potential?

This shift in focus opens new possibilities and even makes the issue of security something positive—something that can enable and empower the business. So, what if there were a solution that could achieve all the IT strategy goals?

What if you could feel confident about data as it moves through your networks?

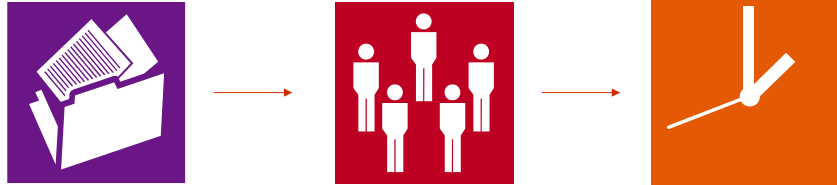
What if you could share throughout your enterprise and beyond without compromising security?

What if you could quickly respond to changing market conditions?

What if security could unleash your full potential?

# ***Unisys Stealth Solution for Network***

## **Stealth Delivers the Right Information to the Right People at the Right Time**



- Protects data-in-motion on LAN, WAN, and wireless networks
- Improves agility
- Provides value and cuts costs

With the Unisys Stealth Solution for Network, you can do all this and more. First and foremost, you'll have confidence in the day-to-day security of operations in your network. You won't have to worry about the safety and security of data as it moves through your network or about managing multiple networks. In fact, with Stealth, your network data is even safer than it is today. You can share the information that needs to be shared within or across communities of interest—a defined group of people who need to share common data—with confidence. With Stealth, you can be agile—responding quickly to opportunities and changing conditions. You can get the data **WHERE** it's needed and **WHEN** it's needed to those **WHO** need it.

The Unisys Stealth Solution is a transformational way to protect your network data. It starts by using certified encryption, then bit-splits data into multiple slices as it moves through the network. But more than that, Stealth allows multiple communities of interest to share the same network without fear of another group accessing their data or even their workstations and servers. The result is a much simpler network infrastructure, increased agility to react to new opportunities, and enhanced security of your network data.

Today, we'll cover the three primary benefits of Stealth:

- Stealth protects data-in-motion.
- Stealth improves agility.
- Stealth provides value and cuts costs.

# ***Unisys Stealth Solution for Network***

## **Stealth Keeps Data-in-Motion Secure**



Network data:

- Is dispersed across the network
- Is protected in-motion
- Is never whole in your network
- Can only be accessed by Stealth users
- Can be structured into controlled-sharing groups

First, let's address the ability of Stealth to keep your data-in-motion on LAN, WAN, and wireless networks safe—possibly even safer.

To do this, Stealth cryptographically transforms information using a data-splitting algorithm that weaves your data into the very fabric of the network. With Stealth, your network data:

... is dispersed across the network

... is protected in-motion

... is never whole in your network

... can only be accessed by Stealth users

and

... can be structured into controlled-sharing groups.

Stealth keeps your network data secure—but in a far simpler consolidated infrastructure. Your data is safe, and you're able to safely share the infrastructure across many communities of interest.

# *Unisys Stealth Solution for Network*

## **Stealth Enables Secure Information Sharing**



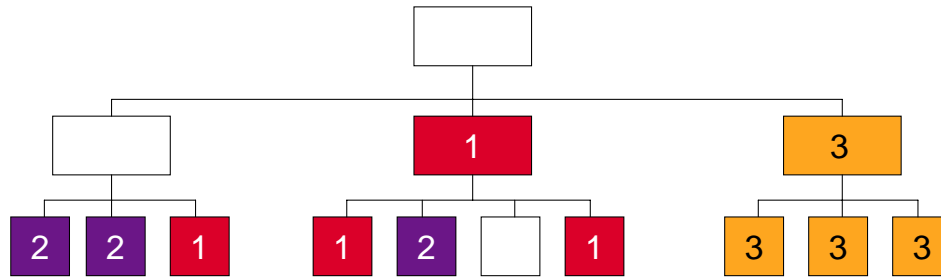
- Control how and what information is shared
- Define access rights based on the needs of the operation
- Other data remains completely safe and hidden

With the Unisys Stealth Solution, you can safely share across the Enterprise and beyond—even across different communities of interest. You control how and what information is shared. By defining communities of interest for users who need access to the same data, you define access rights based on the individual needs of your operation. Complicated access definitions and management do not drive these definitions—your specific domain sharing requirements drive access.

With Stealth, you don't need separate networks. Each user can easily access data authorized for that user, wherever the data is—but only that data. Other data remains completely safe and hidden.

# Unisys Stealth Solution for Network

## Security Group, Domain, or Community of Interest Defines Data Access



- Community of Interest 1: HR Department
- Community of Interest 2: Project Team A
- Community of Interest 3: Project Team B

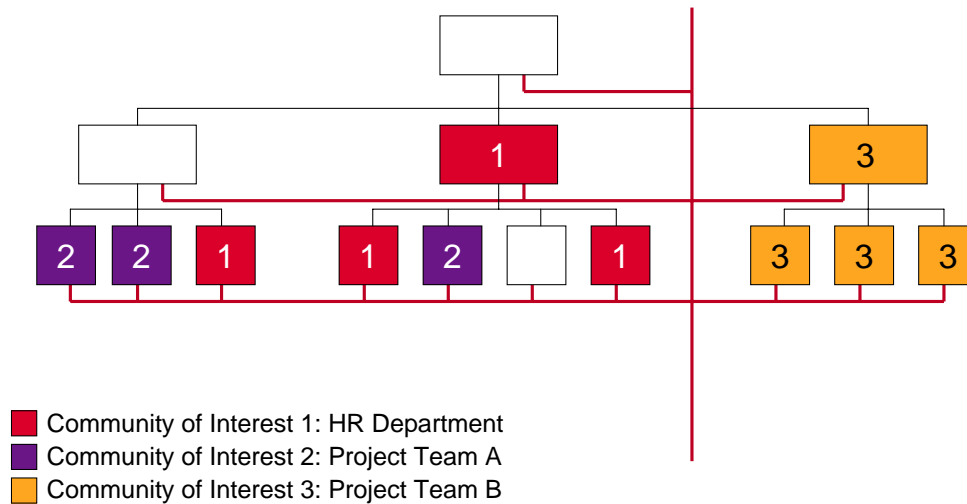
Let's talk about access rights. With Stealth, you define access rights by defining communities of interest. A community of interest can be people within the same department or people from different departments working together on a special project—anything you require.

The Stealth communities of interest remain secure. Each community of interest is given a workgroup key that defines access and security level. Without the correct workgroup key, network packets are just ignored.

The workgroup key construct provides a stronger way to control access to your data.

# Unisys Stealth Solution for Network

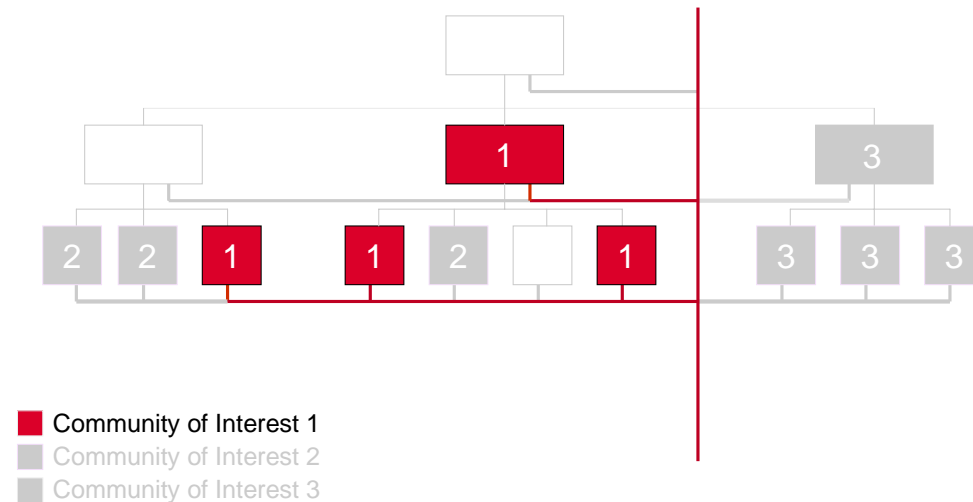
## Multiple Communities or Domains Can Safely Share Data



What's truly unique about the Stealth architecture is that you can intermix data from multiple communities of interest, multiple domains, and multiple workgroups on the same network with confidence. Individuals in different departments, in different organizations, or on different projects—your communities of interest—can work securely on the same network.

# Unisys Stealth Solution for Network

## The Rest of the Devices Remain Cloaked from Unauthorized Eyes



The Stealth workgroup keys secure your network. Without the correct workgroup key, the rest of the devices on the network are cloaked and invisible to unauthorized eyes. Without the correct key, users can't ask for the data from the server or send data to the server or workstation. They can't even ping the server or workstation. It's like they are not even there at all.

It's simple. How can you attack what you can't see?

# ***Unisys Stealth Solution for Network***

## **Network Data Is Even Safer**



- Certified AES-256 encryption
- Bit-level data splitting
- Optional virtualization
- Optional resiliency

As we discussed a few minutes ago, your job is simple: get the right information to the right people at the right time. . . But you better make sure every bit of that information remains secure. You cannot compromise on security. You must protect all network data and eradicate threats to data-in-motion across your network.

Remember, Stealth protects your data-in-motion by cryptographically transforming it. So with Stealth, you don't need to worry about the confidentiality, integrity, and availability of data on your networks. You achieve Secure Network Operations.

To give you even greater security than you have today, Stealth uses four methods that together ensure your data is protected:

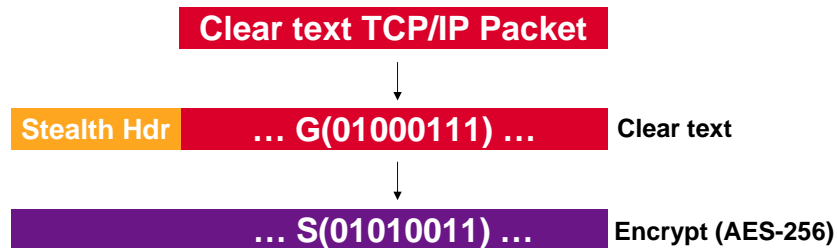
- Certified AES-256 encryption
- bit-level data splitting
- an optional innovative virtualization methodology that sends your data on separate paths through the network

and

- an optional resiliency feature for data recovery

# Unisys Stealth Solution for Network

## Stealth Delivers Defense-Level Encryption



Let's look at how Stealth provides AES-256 security for your data-in-motion. The next few slides provide a simplified view of the internal process; there is a lot more actually going on within Stealth than we can show here. At the end of this presentation, I'll give you a link to a Technical Brochure and White Paper that provide additional information on how Stealth works.

When transmitting network data between two points, Stealth generates two session keys: an encryption session key and a split session key.

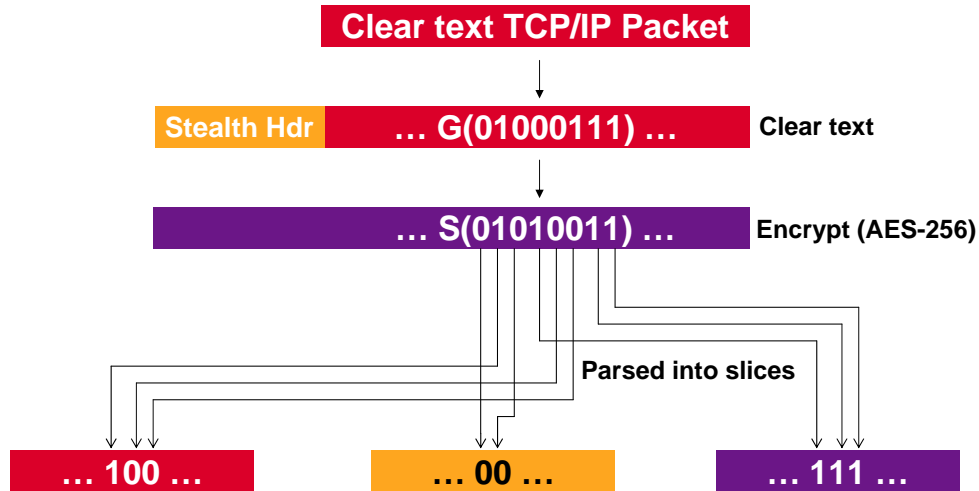
Stealth creates these session keys when the transmission tunnel is opened, with a separate pair of keys for each transmission direction. The session keys are encrypted with the workgroup key and sent to the other side of the tunnel at tunnel-open time using Perfect Secret Sharing, a mechanism that has never been broken.

The Stealth Solution employs a unique, patented way to protect your data throughout the network. First, it adds a Stealth header to your clear text. Then the data is encrypted with the encryption session key. By default we use AES-256, but Stealth can use other encryption algorithms.

Just for this example, let's assume that the clear text "G" is encrypted to an "S", although AES-256 is obviously much more complicated than a simple character substitution.

# Unisys Stealth Solution for Network

## Data Is Split at the Bit Level



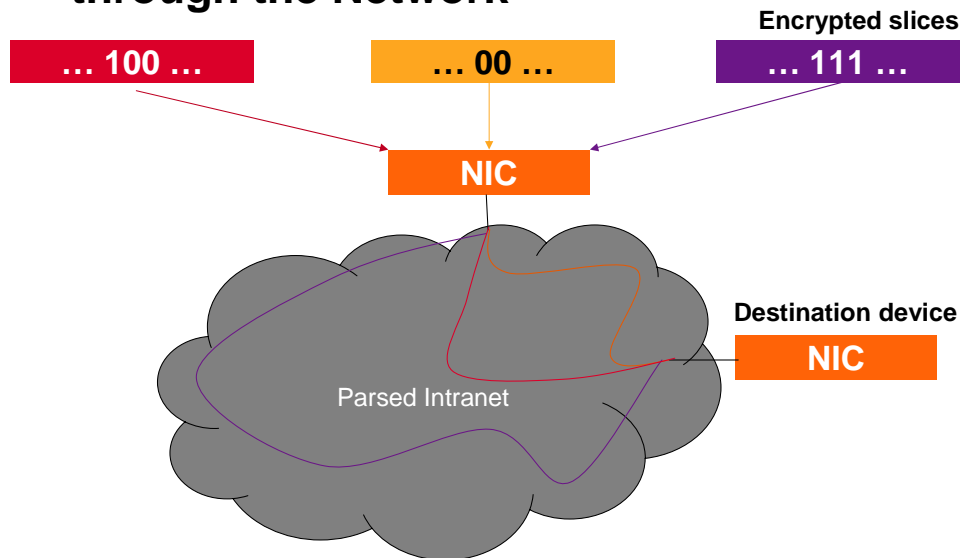
Next, Stealth employs its unique data-splitting methodology. The encrypted record is parsed at the bit level into multiple pieces called slices. Note how the individual bits in the “S” (which was originally a “G”) are split across the different slices.

The mapping of those bits from the encrypted record to the slices is controlled by the split session key, which I mentioned on the last slide.

Stealth calculates an authentication code for each slice, and stores all of these authentication codes in every slice. By verifying these authentication codes at the other end, Stealth can detect accidental or deliberate corruption in a slice, and ensure the integrity of the data.

# Unisys Stealth Solution for Network

## Stealth Sends Data on Different Paths through the Network



These data slices are sent through your network. The Stealth Solution employs a Unisys-developed information management architecture that fundamentally alters the approach to data protection by turning your network into a parsed network. With Stealth, all IP traffic (except some basic management functions such as DHCP) is parsed.

If unauthorized people capture some of these data slices, they can never put it all back together. Even if they get all of the slices, they won't be able to capture the original data. They need the split session key to unscramble the bits, and the encryption session key to decrypt the message. It's like we took a book and put all the "A"s in one file, all the "B"s in another file, and so on. Each file is useless by itself. Only by knowing the original mapping can you put the book back together.

If your network support VLANs, you can optionally specify that Stealth is to use separate VLAN paths for each slice. Each of these paths has a different spanning tree, thus you now have different data paths through the network. These multiple network pathways are nearly impossible to detect or jam.

Now that we've talked a bit about how it works, let's put it all together in a movie. Let me set the scene first: In this example, the Stealth network includes a workstation and a server. The user at the workstation needs a map.

# ***Unisys Stealth Solution for Network***

## **How It Works**

Let's take a high-level view of how Stealth works <start movie>.

**Start** In this example, the Stealth network includes a workstation and a server. The user at the workstation needs a map.

So he requests the map from the server, ...

... and transmits that request to the server.

The server retrieves the map from a database and initiates the maps' return to the workstation. This is where Stealth takes over, deep in the TCP/IP stack.

It first adds a Stealth header ...

... then using AES 256 and an encryption key Stealth generated just for this session, Stealth encrypts the data.

Next, Stealth parses the encrypted data at the bit-level into a site-specified number of slices. Here, there are 3 slices. The exact way the bits are parsed depends on another 256-bit key Stealth generated just for this session.

**Transfer the slices** For added security, Stealth can send these slices over separate VLANs, actually weaving the data into the very fabric of the network, or as shown here, can send them through any network.

At the receiving end, the process is reversed. The slices representing the original data are collected, and the individual bits are reassembled into a single record.

The data is decrypted.

Then, the Stealth header is removed, restoring the original data. Again, this is all happening deep in the TCP/IP stack, below the OS and all applications.

And before he knows it, the user receives the map.

USS-L1

# ***Unisys Stealth Solution for Network***

## **Network Data Remains Safe from Threats**



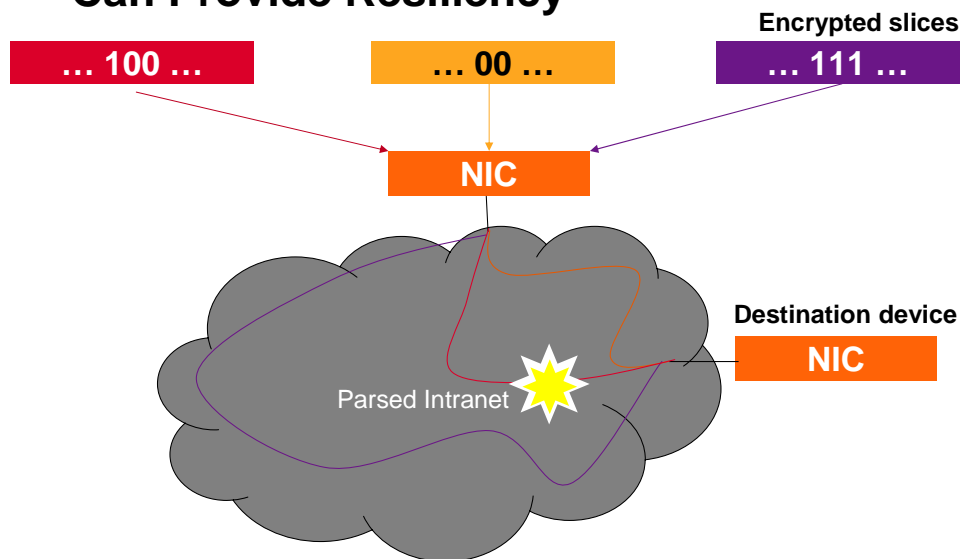
- External
  - Packets safe from interception
- Internal
  - Intentional threats
  - Accidental threats

With the Unisys Stealth Solution, you're actively assured of the security of data-in-motion on your network. Stealth protects your data-in-motion from external and internal threats—whether intentional or accidental.

Internally, Stealth automatically detects corrupted data and can provide resiliency. To protect from external threats, packets can't be intercepted. Only pieces of packets can be intercepted. And these pieces are useless.

# Unisys Stealth Solution for Network

## Stealth Detects Data Corruption and Can Provide Resiliency



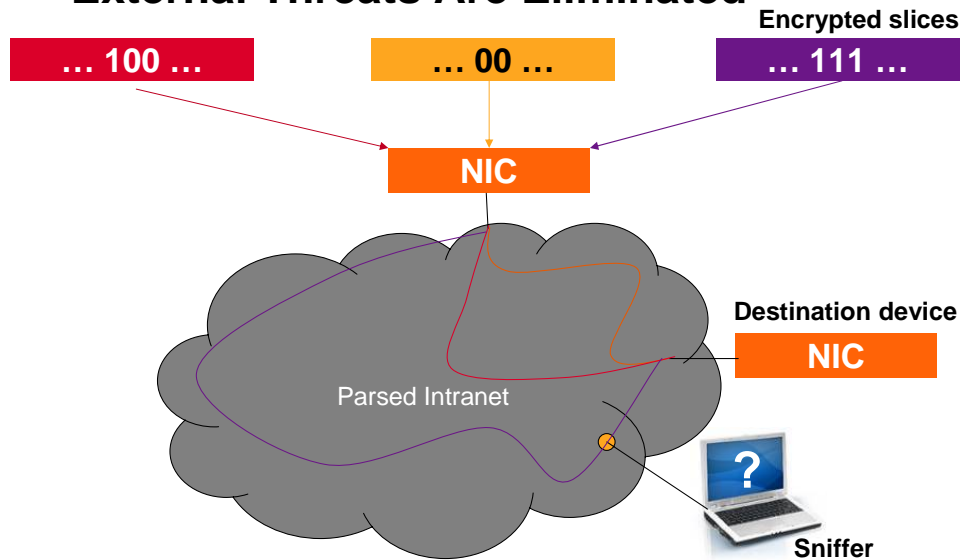
Integrity is further enhanced through Stealth's ability to detect corruption and through the resiliency option that enables data reconstruction with fewer than the original number of slices.

Because each data slice includes a thumbprint of all slices, Stealth detects slice corruption or tampering. If one or more slices are damaged, corrupted, or lost, the problem is detected, and the slice is retransmitted.

For less reliable networks, Stealth can provide resiliency. Stealth can optionally add fault tolerance so that the original data can be reconstructed from less than the total number of slices. For example, Stealth can be configured to require only some of the slices ( $m$  of  $n$ ) to reconstruct all of the data. So let's say you specify 3-of-4 redundancy. Here, Stealth creates four slices, but only needs any three of them to reconstruct the original data.

# Unisys Stealth Solution for Network

## External Threats Are Eliminated



With Stealth's level of security, you don't need to worry about the latest targeted threat to your network data. The hackers simply cannot break through. Even someone logically inside your network cannot capture your data because they cannot find all the slices on their disparate pathways through your network. They couldn't decode the data anyway because they can't reassemble the original encrypted record, and they can't break the encryption.

The cryptology is FIPS 140-2 certified, and the solution is in process for Common Criteria EAL4+ certification.

# ***Unisys Stealth Solution for Network***

## **Be Secure, Not Just Compliant**

“It’s easier to say you’re compliant than to say you’re secure, except when there is an incident.”

Consulting company INPUT, March, 2007

Whether you’re dealing with Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, or other state and local acts, you must comply with privacy regulations. These regulations require you to both limit access and become all-seeing and all-knowing when it comes to who is accessing what data on your network. But laws and regulations can have two major problems: they can lead to different interpretations, and they don’t cover everything.

Once you have taken care of all the regulatory requirements, you’re compliant. But are you truly safe? It is far easier to say you are compliant than it is to say you are secure. You can be compliant and still have a data security breach.

So it’s time to take your security architecture to the next level, one that allows you to meet regulatory requirements and feel confident that you’ve protected the integrity of your data and the security of your network. The Unisys Stealth Solution makes you secure, not just compliant.

{Link to quote:

[http://www.input.com/corp/events\\_conference/presentations/PRES\\_20070327\\_Prabhat%20Agarwal.ppt#274](http://www.input.com/corp/events_conference/presentations/PRES_20070327_Prabhat%20Agarwal.ppt#274)}

## ***Unisys Stealth Solution for Network***

### **Internal Threats Are Eliminated**



With Stealth's workgroup keys, encryption, bit-level splitting, and multiple data paths, your data-in-motion is secure. You have superior data integrity. Confidential data remains confidential. And your data is available when you need it to be.

Your data is not only protected from unauthorized access, theft, or misuse, but also from corruption or loss.

# ***Unisys Stealth Solution for Network***

## **Stealth Strengthens Enterprise Agility**

**Respond quickly  
Deploy quickly  
Share quickly**

***Information drives business.***

Our next key element of Stealth is its ability to improve agility.

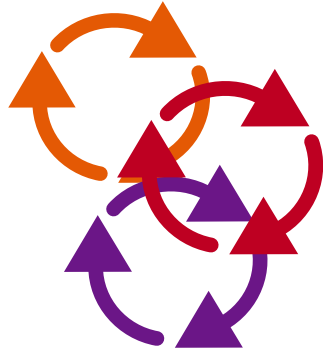
In today's fast-paced and sometimes turbulent competitive environment, you simply must maintain the ability to respond and ramp up quickly.

With the Unisys Stealth Solution, you not only are assured of security of the data in your network operation, but you also have enabled new capabilities. You can deploy far more quickly, and your network itself is far simpler. You can share information more quickly. Essentially, you can better use information to grow the business. And with Stealth, you have one familiar place to manage access rights, communities of interest, and workgroup keys.

Active Directory and the Stealth workgroup key are the enablers of access and sharing, agility, and security.

# Unisys Stealth Solution for Network

## Sharing Is Simpler



- Access policies and governance enhanced
- Password rules remain as defined
- Users restricted to only applications and services in assigned workgroup

Given that agility is enabled through simplicity, we've made sharing data amongst different communities of interest easier than ever. You can simply configure your network for all your communities of interest, no matter where or who they are. You just assign new users into the appropriate community of interest—or more than one—and you're ready to go. You don't have to change your physical network.

And while you are sharing, your access policies and governance have been enhanced. Password rules remain as defined, yet all users are now restricted one more level to only those applications and servers in their assigned workgroups.

You assign a workgroup key to each community of interest. This workgroup key is the secret to secure sharing. Without the right key, unauthorized users cannot access the data—the data remains visible only to members of that community of interest. There's no more risk of users probing servers in other non-authorized areas.

# Unisys Stealth Solution for Network

## Defining Communities and Workgroups Is a Snap



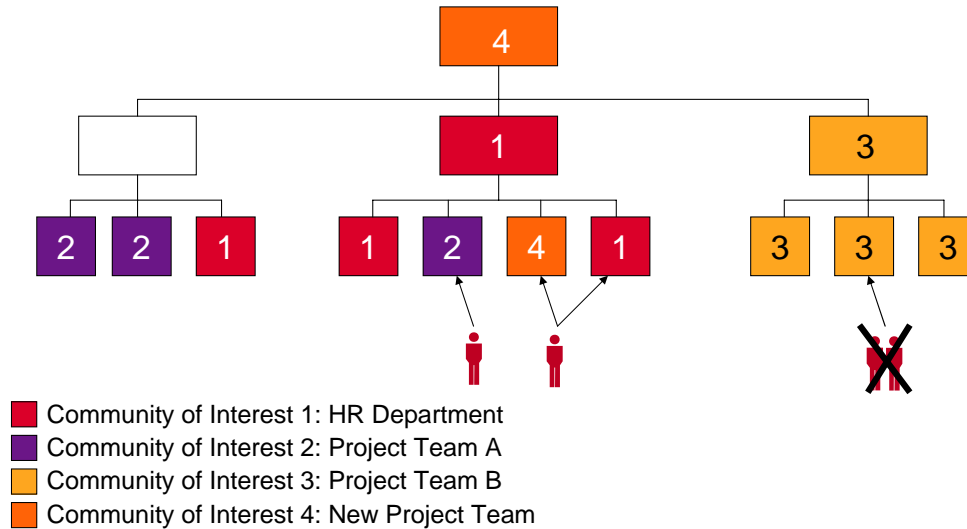
- Define
- Change
- Expand
- Reduce
- Add
- Delete

With the Unisys Stealth Solution, initiating sharing and user management is very easy. A few slides ago, we talked about defining your communities of interest—based on your security and sharing requirements. Once you start to set up these communities, you'll find it's easy to configure Stealth using tools you use every day like Active Directory (or whatever you're using to manage user identity). You can define, change, and expand communities and workgroups by whatever scheme you need.

And adding new communities (and remove obsolete ones) is easy too. You're able to quickly respond to unanticipated partners and events.

# Unisys Stealth Solution for Network

## It's Easy to Add or Remove People



It's also simple to add new people or remove people as needed.

You easily configure for new individuals, partners, and new organizations. No matter who your users are—internal or external, long-term or transitory—you can easily add them to a community of interest, and your access configuration is done. You don't need to reconfigure a network, change firewall rules, or the like.

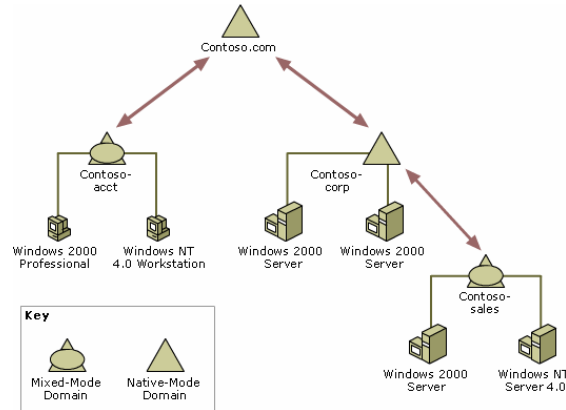
And it is just as easy to remove individuals from communities of interest.

It's doubtful that your organization is so tightly defined that each person is isolated in one community of interest. You'll have many people who cross domains and project lines and need to be placed in multiple communities of interest. With the Stealth Solution, you can add people to as many communities as you need.

And what's more, because you defined your communities of interest and you're using workgroup keys for access control, your physical network can be simplified and does not have to match your user groups. You can build the network you need—and no more—and still provide the access your users require.

# Unisys Stealth Solution for Network

## Active Directory Manages Communities of Interest



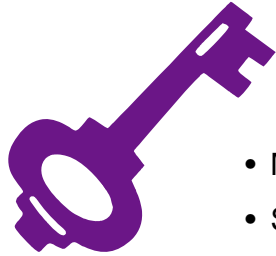
I've mentioned using Active Directory a couple of times—let me explain why this is important. The Unisys Stealth Solution uses Microsoft's Active Directory (again, or whatever system you're using for identity management) to define and manage communities of interest. This allows you to centralize authentication and authorization with a single well-known administration tool.

The power of Stealth and communities of interest (and their corresponding workgroup keys) is that when something changes, you just make the change one time in one place. Using Active Directory, it's quick and easy to shift a person's or group's access as their responsibilities change or to add additional new people or groups to communities. You update Active Directory to reflect the new person, the new assignment, the new community of interest. And you're done. It's as if Stealth instantly and automatically reconfigured your network infrastructure to match your organizational structure.

For those few organizations that aren't using Active Directory, you can use any other equivalent mechanism to provide the workgroup key.

# ***Unisys Stealth Solution for Network***

## **Stealth Keys Improve Agility**

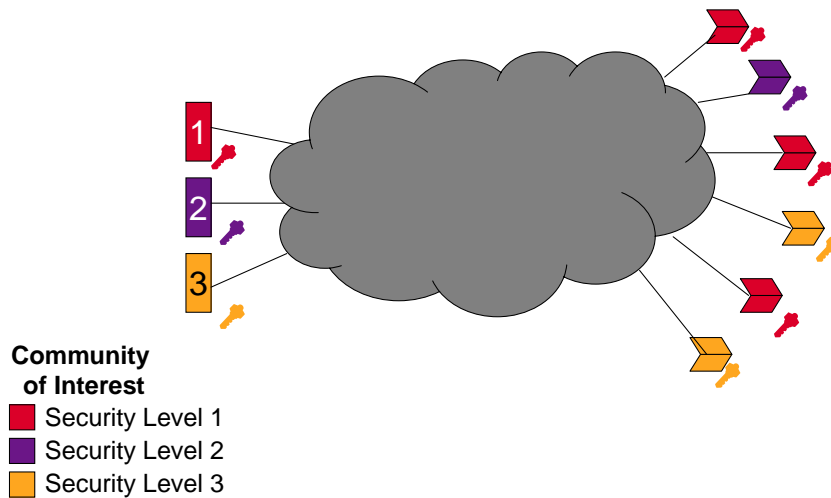


- Manage workgroup keys in Active Directory
- Stealth manages session keys

Sometimes when we start talking about keys, red flags go up. Managing keys is often complicated and time-consuming. This is definitely not an indicator of an agile organization. But with Stealth, key management is simple. As I've mentioned, it's done in the well-known and commonly used Active Directory when you set up your communities of interest. And split session keys—those keys generated to protect each unique active session—are completely managed by Stealth. You don't need to do a thing.

# Unisys Stealth Solution for Network

## Workgroup Keys are Easy to Store and Manage



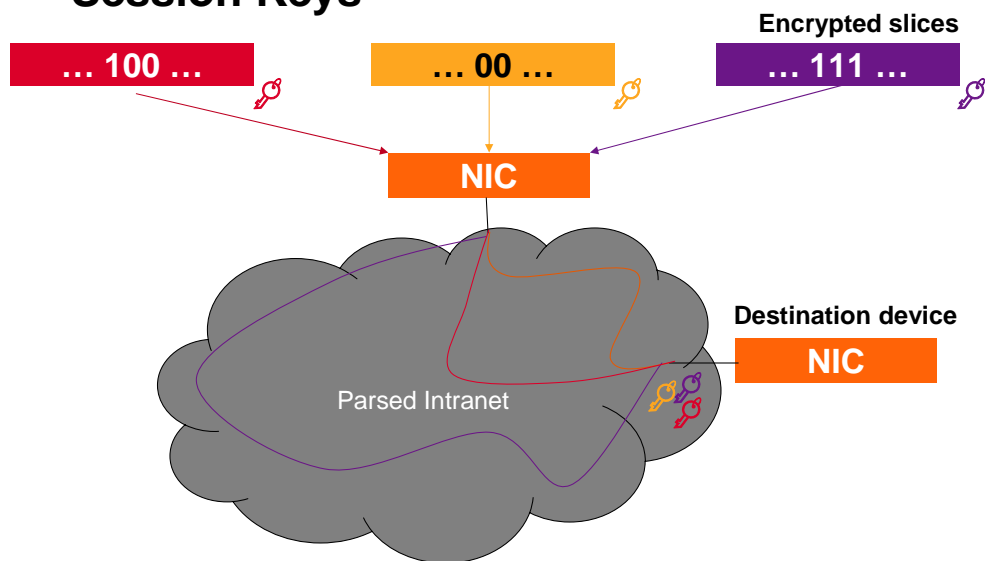
We've engineered Stealth specifically to be easy to manage. No additional overhead or complication is necessary. The same is true for management of the Stealth workgroup keys, which determine who in your organization is allowed to communicate with whom.

The workgroup keys control the communities of interest—users that need to share information. Information can only be retrieved by members of the designated community of interest, as long as they have the appropriate workgroup key. If there's a match, the data is shared.

And with using Active Directory to manage the Stealth workgroup keys, it's simple and familiar with no additional overhead.

# Unisys Stealth Solution for Network

## Stealth Generates and Manages Session Keys

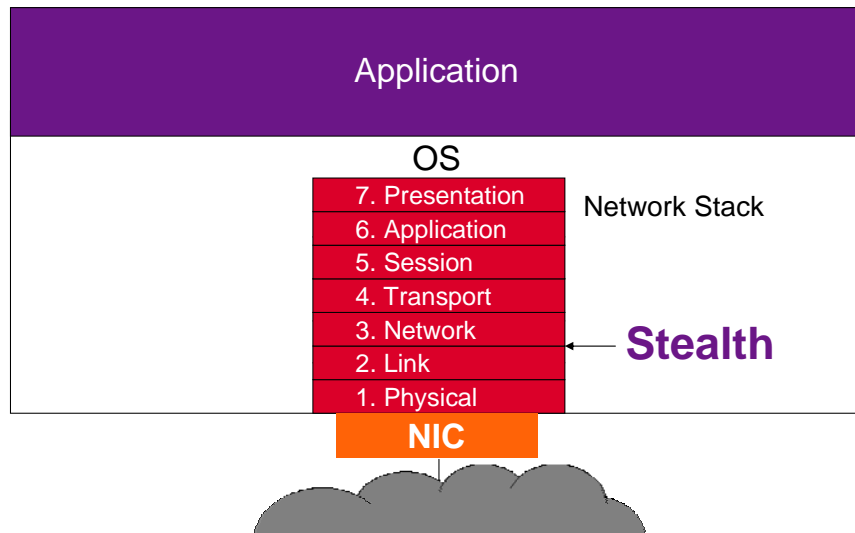


The second type of key that Stealth employs are session keys: encryption session keys and split session keys. These keys are short-lived: they are generated only for a single, unique session when a network pathway is opened. The split session key determines how the packets are split into slices, and how those slices will be put back together on the other end. Stealth uses the encryption session key to encrypt the slices.

These keys are completely handled by Stealth. They are generated by a cryptographically secure pseudo-random number generator, never written to any non-volatile memory or other media, and are destroyed after the session ends. They are secure and require no additional overhead of storage or management.

# Unisys Stealth Solution for Network

## Simpler Provisioning Translates to Rapid Deployment

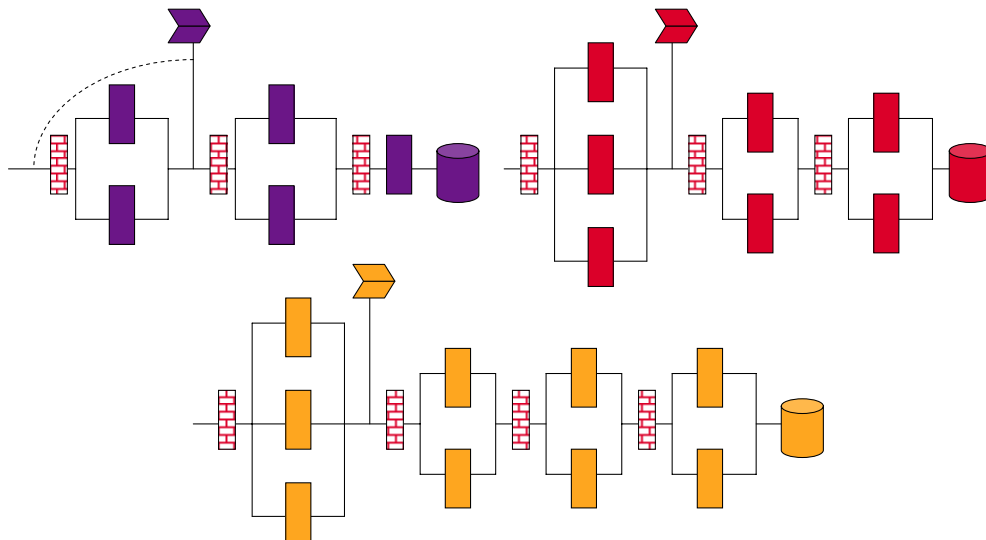


Stealth works at exactly the right point in the network—integrated into the network infrastructure and below the applications. When you need to make a change, you don't need to touch routers, firewalls, or applications. Simply put, you don't have to change your infrastructure to implement a Stealth network. Because Stealth sits in the Network stack, it will run on the network infrastructure you have today and give you enhanced security of your data-in-motion within your LAN.

With Stealth, your physical network is simpler. Stealth employs simpler provisioning, allowing you to ramp up quickly. First, your network is more compact—less to procure and less to support and manage. You can quickly add new workstations, servers, and applications to the network in far less time than you're probably spending now to do the same thing.

# Unisys Stealth Solution for Network

## Your Current Infrastructure Is Complex to Support

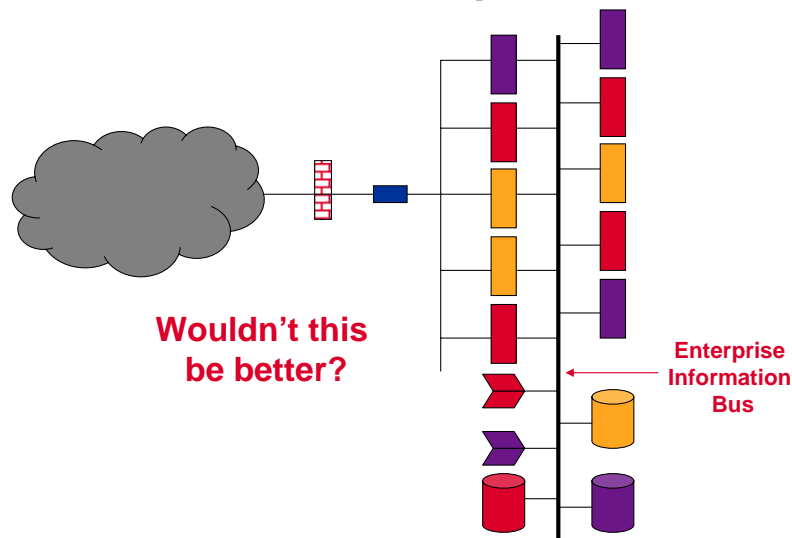


Does your network look like this? Separate physical networks for different communities of interest, and those networks further divided to protect tier-3 servers from tier-2 servers from tier-1 servers and vice versa? These separate networks isolate the information and transactions of individual applications—or sometimes even subsets of a single application. Each is surrounded by its own set of firewalls, switches, routers, security requirements, and access rights.

For this type of infrastructure, you need lots of equipment and the corresponding people required to install, maintain, and manage those devices. When things change, and they do, you often need to adjust your network. Periodically, you need to also replace a class of your infrastructure products or add a new set to provide additional protection. Every time that happens it is a real event, requiring detailed planning and exacting execution, usually at significant cost in time and money.

# Unisys Stealth Solution for Network

## The Stealth Network Infrastructure Is Consolidated and Simplified

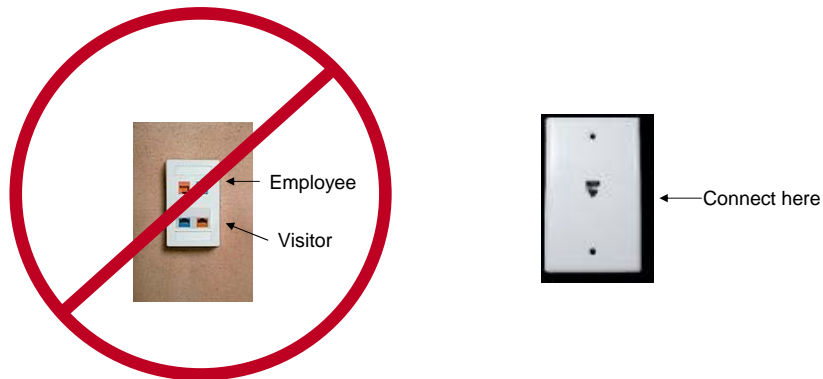


With Stealth, you no longer need to physically separate devices, applications, and data to control access. You have a simpler network infrastructure. Stealth offers a more consolidated infrastructure, and your physical network is independent of your user group structure. Stealth lets you create a single enterprise information bus, an infrastructure and architecture that demonstrates loose coupling and flexibility. And do it while maintaining, or even enhancing, your control over the data in your network.

You still have to protect your network from the outside world, but with Stealth it is as if you could completely trust everybody inside your network to never accidentally, or deliberately, look at anything they aren't supposed to see. You are still protected, with Stealth acting like the firewalls, switches, and routers you need to keep Harry's team from seeing what Mary's team is doing. Just as if you had a perfect network infrastructure around every project, there is no way to get or send data outside of a workgroup.

## ***Unisys Stealth Solution for Network***

### **Set Access by User, Wherever the User Chooses to Connect**



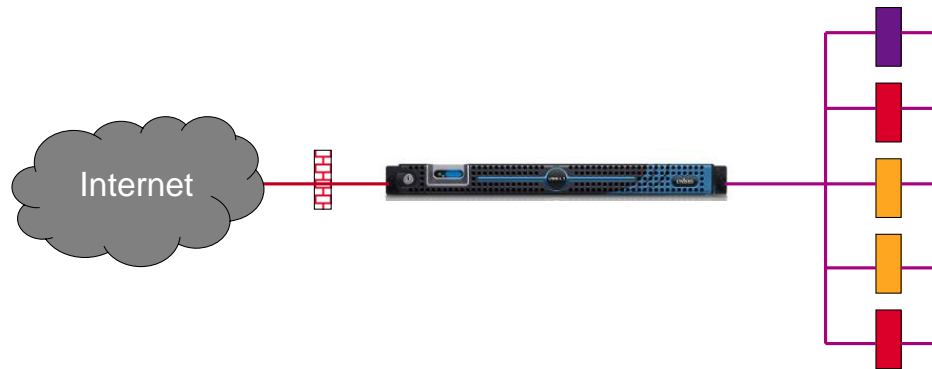
Because the Stealth Solution network is secured, you define access by user, not by location. It doesn't matter where the user is or what connection is used: you don't have to change your network at all.

With Stealth, location doesn't matter to you because security is assured by employing the workgroup keys, not by drilling holes in the firewall to physical devices.

Separate non-Stealth VLANs carry visitors to the Internet or some other landing zone that you define with no risk that the visitor can even see a Stealth network or its application devices.

## *Unisys Stealth Solution for Network*

### **The Stealth Appliance Is Your Gateway to the Non-Stealth World**



When you need to communicate outside of your Stealth protected network, you use the Stealth appliance for LAN. The appliance acts as a gateway between the Stealth LAN (the purple network on the right) and a non-protected network like the Internet. You can also use the appliance to connect legacy systems or other large servers to your Stealth network. We plan to show you in 2008 how to expand Stealth protection out to units or partners, no matter where they are.

# ***Unisys Stealth Solution for Network***

## **Stealth Delivers Significant Economic Value**



- Protects from network breach
- Strong ROI
- Long-term value

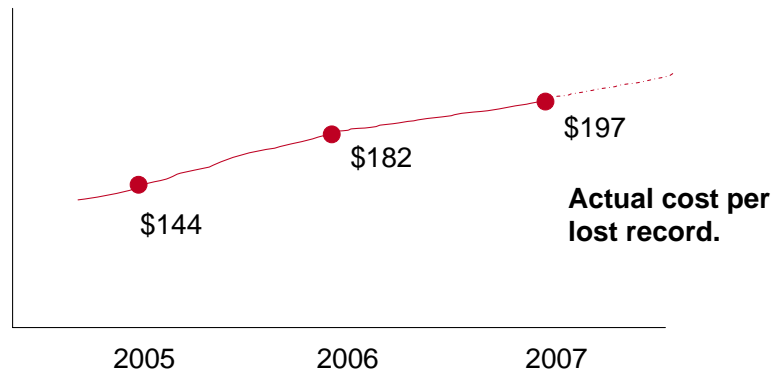
The third key benefit of Stealth is the economics—both in terms of lower costs and in long-term value. Imagine: the ability to extend the network while being agile *and* lower costs.

Typically, we only discuss the economics of a security solution implementation in terms of having the lowest costs; the subject of savings is not broached. With Stealth, however, you can achieve both short- and long-term value.

First, let's address the obvious. The Unisys Stealth Solution, of course, vastly reduces your risk of facing a security breach and the associated costs. But Stealth goes way beyond that. It offers you short-term economic advantage in terms of a strong return on your investment in your more consolidated network and the enduring strategic value to your stakeholders from being a Trusted Enterprise.

## ***Unisys Stealth Solution for Network***

### **You Are Protected from the High Costs of a Network Breach**



Ponemon Institute. 2007.

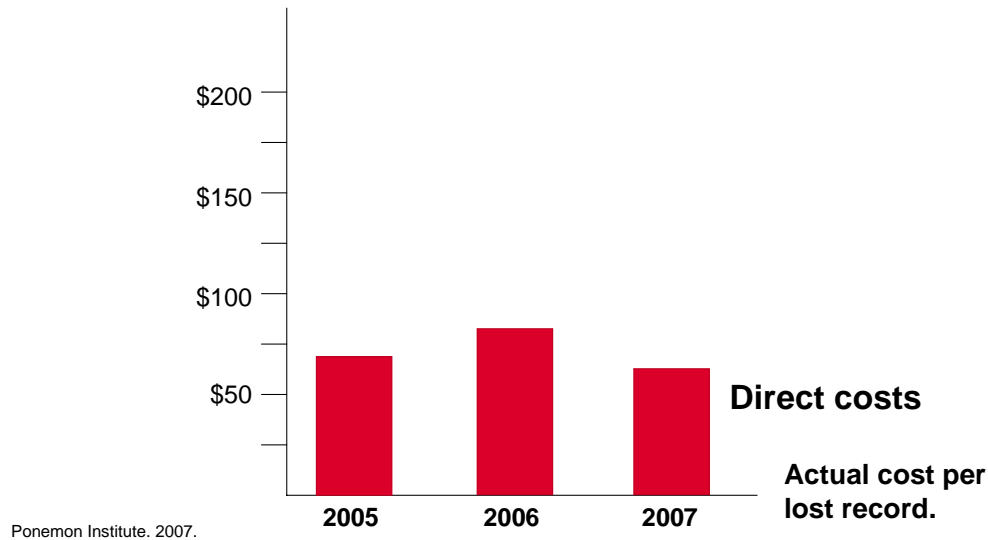
A network breach is expensive. Think of some recent examples in your industry.

In fact, industry analysts are predicting that some large, well-known company will face Chapter 11 due to a security breach in the next 12 months. They don't know who it will be, but they are confident it is a sure bet.

And as you can see, that cost of a network breach is rising, from \$144 per lost record in 2005 to \$197 per record last year. Analysts expect this increase to continue.

# Unisys Stealth Solution for Network

## A Privacy Breach Is Expensive



The Ponemon Institute conducts annual studies to determine what a data security breach really costs. They actually measure it.

They start with the first element of a breach—the direct costs. This includes those unbudgeted, out-of-pocket expenses covering notification, legal and accounting services, call centers, and public and investor relations.

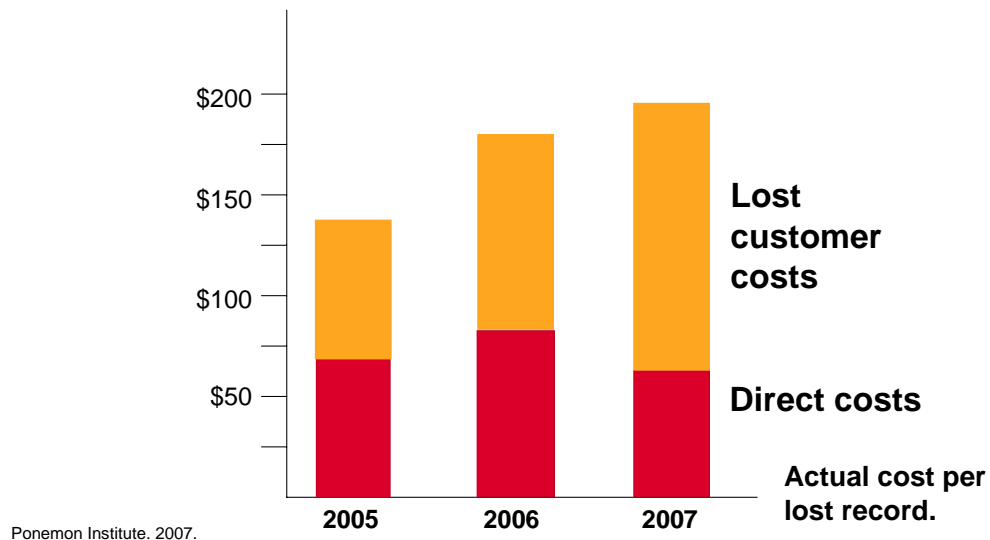
It also includes the lost productivity. As I'm sure you know, a data security breach initiates those internal fire drills that affect a large proportion of the organization. It's basically an all-hands-on-deck call to patch the hole and deal with the consequences. You need your employees and contractors to concentrate on the crisis, diverting attention from other tasks.

As you can see, although the direct costs are coming down due to better systems and processes for handling breaches, a breach remains expensive: it costs \$69 per lost record.

But wait, there's more.

## ***Unisys Stealth Solution for Network***

### **A Privacy Breach Is Even More Expensive**



They also measure the biggest cost of all, which grew tremendously in 2007.

You know the drill. The effect of a breach snowballs. One scared customer walks away, but makes sure to tell other customers on the way out. Following a breach, customer turnover averages a little more than 2% and can range as high as 8%. And acquiring new customers becomes increasingly difficult and expensive.

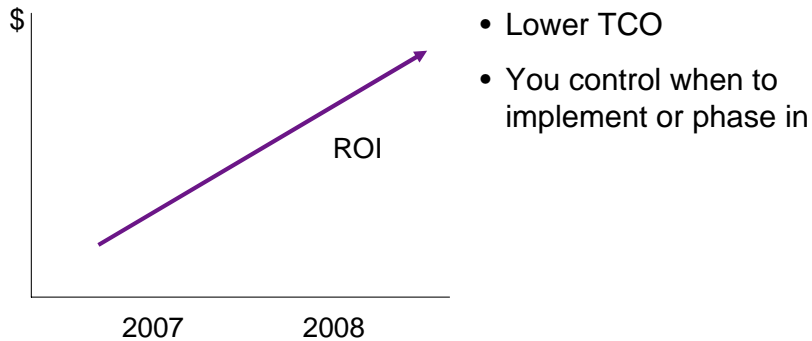
Today, breach costs you an additional \$128 in lost customer loyalty per record lost. That's a lot of lost good will. All in all, that's \$197 per lost record.

Yes, the cost of a breach is extremely expensive, and as I mentioned, it's increasing. Already, Ponemon's research shows that it's up by 37% over 2005 costs.

And how many records do you have? Do the math.

# Unisys Stealth Solution for Network

## Stealth Improves ROI



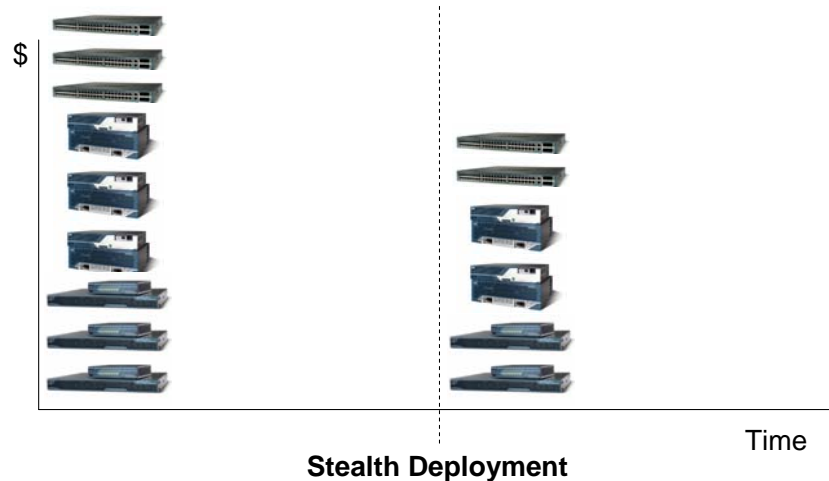
Simply put, Stealth offers a solid ROI.

The Unisys Stealth Solution consolidates and simplifies the network, which offers lower TCO and a better return on investment. In fact, your return on your Stealth implementation will be measured not only through reduced expenses for equipment but also through reduced staff and support costs. In addition, with a consolidated Stealth network, the amount of space, weight, and power required is drastically reduced—critical in many remote environments.

Stealth gives you the ability to control your ROI. As we mentioned before, with Stealth, you don't have to change anything. You can leave your infrastructure as it is, or phase in the changes over time, when it's convenient.

# Unisys Stealth Solution for Network

## Stealth Lowers Acquisition Costs



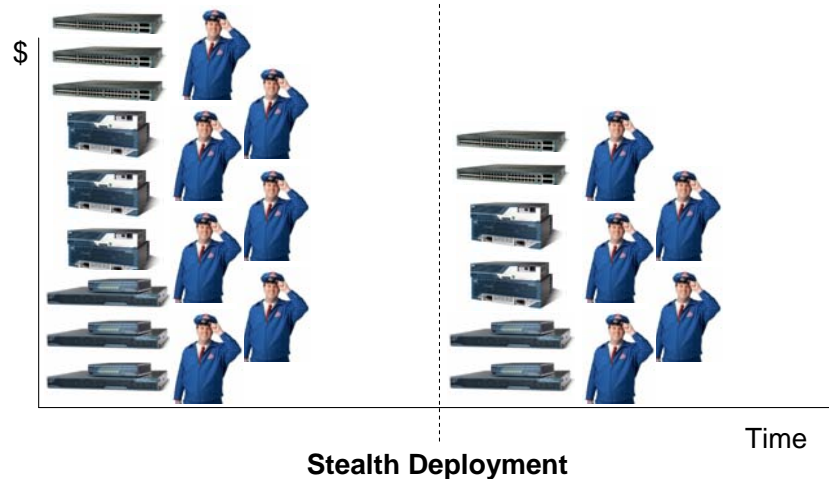
First, Stealth gives you the opportunity to lower your vendor costs for procurement. You no longer need as many routers, switches, or firewalls. With a Stealth infrastructure, we expect you will reduce your capital expenditures on network hardware substantially.

In addition, the Stealth Solution provides VPN-like capability for each workgroup without the need for the expense of other VPN technologies.

Having heard Stealth's story, how many routers, switches, and firewalls (and their support costs) do you think you could eliminate in your network?

# Unisys Stealth Solution for Network

## Stealth Lowers Implementation and Support Costs

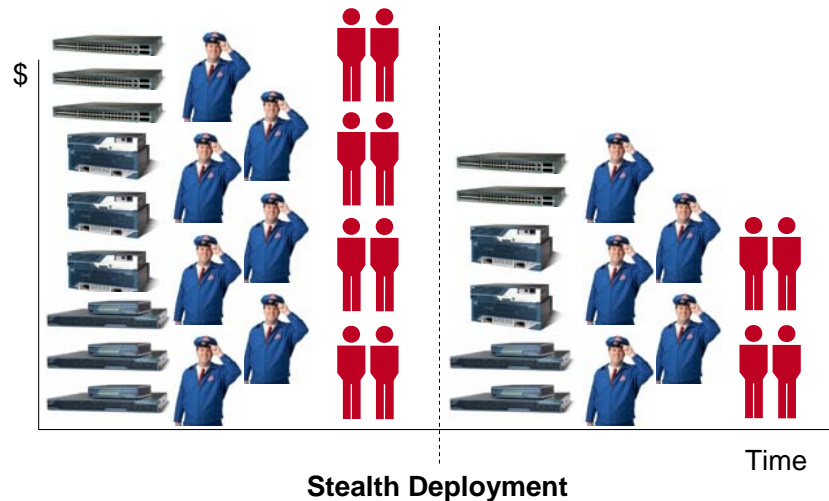


Secondly, Stealth can reduce your support costs along with acquisition costs. How much do you pay to all of your infrastructure vendors? 15%? 20%? More? As you reduce the number of components in your network, you should expect a corresponding reduction in your vendor support costs.

You're beginning to see significant benefits of a Stealth Solution network. How much of your budget is spent on network infrastructure vendors? As you reduce the number of components in your network, you should expect a corresponding reduction in your vendor support costs.

# Unisys Stealth Solution for Network

## Stealth Lowers Implementation and Support Costs



And because Stealth offers a less complicated network environment, it is far easier to manage and administer. This means lower management and administration costs for your network.

For instance, with Stealth, you see a reduction of 20 to 50% in firewall rules maintenance. Of course, this will depend on the complexity of your security objects in Active Directory and their maintenance. Reduced support complexity for firewalls, reduced outage risk from firewall rules changes, and fast additions of qualified users to Active Director security groups all translate into greater agility.

# ***Unisys Stealth Solution for Network***

## **Stealth Lowers Environmental Costs**



### **Tough Environments**

- Branch offices
- Remote locations
- Historic buildings

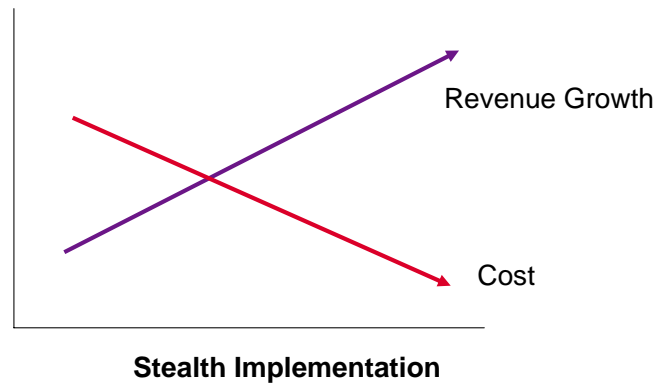
### **Stealth Conserves**

- Space
- Weight
- Power
- Heat Generation

Enterprises often need to place networks in tough locations, like branch offices, remote locations, and historic buildings. Conserving space, weight, power consumption, and heat generation is critical. With Stealth, a consolidated network and reduced infrastructure can dramatically lower these factors.

## ***Unisys Stealth Solution for Network***

### **With Secure Network Operations, You Deliver Long-Term Value and Trust**

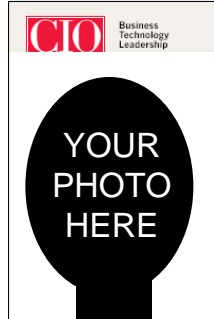


The real long-term value lies in your reputation. Your ability to protect your network data and your customers' privacy translates into lasting value for your organization. Some people call this the ROI of trust.

When you are a Trusted Enterprise, you have the confidence of your customers, partners, shareholders, and other stakeholders. And you can use that confidence to drive your market positioning, your revenue streams, and shareholder value.

# ***Unisys Stealth Solution for Network***

## **Security Becomes a Marketable Differentiator**



**Protection of data**  
=  
**Customer recognition**  
**Customer value**  
**Customer reward**

Being a Trusted Enterprise is a marketable differentiator to customers. With the Unisys Stealth Solution, you can stand out from the crowded marketplace because your security and the protection of your customers' privacy is assured.

As a Trusted Enterprise, you become best-in-breed, and customers recognize, value, and reward your ability to protect their privacy.

# ***Unisys Stealth Solution for Network***

## **Protection of Data Equals Protection of Revenue Streams**

“The ROI of Trust: Treat security and privacy spending not as something you have to do but as something you want to do.”

CIO Magazine, July 15, 2007  
John C. Reece, Chairman & CEO of John C. Reece & Associates

Because your network and network data are secure, your revenue streams are protected. Customer loyalty remains strong, and you shift your focus on day-to-day worries about a data security breach to focusing on building revenue and growing your business.

First, Stealth lowers your acquisition costs. You no longer need as many routers, switches, or firewalls. With a Stealth infrastructure, you can expect to reduce substantially your capital expenditures on network hardware.

## ***Unisys Stealth Solution for Network***

### **Security Drives Stakeholder Loyalty and Value Recognition**



When you demonstrate that your organization is secure, the effects are truly far reaching. It drives the trust and confidence of your customers and stakeholders. This trust has long-term effects. It drives your stakeholder loyalty and value recognition.

# ***Unisys Stealth Solution for Network***

## **What If Security Empowered Your Business?**

- Confident about data
- Share securely
- Respond quickly
- Unleash your full potential



We began talking today about a series of “What if” questions. Current security solutions cannot address all those questions. But Stealth is more than a simple security solution. With its ability to expand sharing and keep network data safe—maybe even safer—it becomes an empowering solution. The Unisys Stealth Solution can position your organization as a Trusted Enterprise.

With Stealth:

You could feel confident about data as it moves through your networks.

You could enable sharing with multiple networks without compromising security.

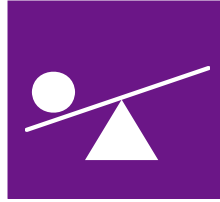
You could quickly respond to changing market conditions.

and

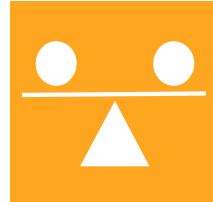
Security could unleash your full potential.

# *Unisys Stealth Solution for Network*

## **The Battle Between Security and Sharing Threatens Success**



- Current security solutions ignore sharing
- Multiple networks or silos inhibit agility



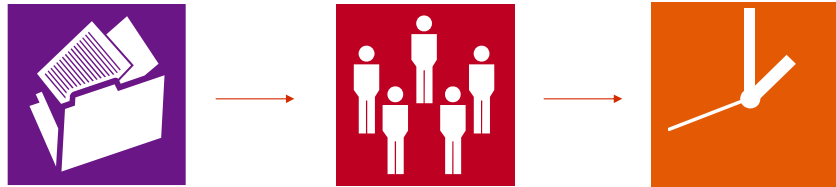
- Stealth balances sharing and security

For too long, enterprises have been stunted by the complexity of opening their business—and the network—to partners, consultants, customers and other stakeholders while remaining compliant and secure. This complexity, combined with complexity and cost of ensuring secure access even from those outside the organization, has been a distraction to the business.

The current trend of reactive security measures has made it difficult for enterprises to get the information to who needs it where they need it and when they need it without compromising security and where you can respond quickly to unexpected opportunities.

## ***Unisys Stealth Solution for Network***

### **Stealth Delivers the Right Information to the Right People at the Right Time**



- Protects data-in-motion
- Improves agility
- Provides value and cuts costs

The bottom line? With the Unisys Stealth Solution for data-in-motion, security and sharing can peacefully co-exist. You can be confident about withstanding the next major network attack. At the same time, you sharply reduce the complexity of managing so many network users across multiple networks.

As you can see, the Unisys Stealth Solution for Network gives you the ability to achieve your vision: to use information to drive your business. In doing so, Stealth delivers three powerful benefits.

-It secures your network data.

-It improves agility, allowing you to be responsive to changing market conditions.

-And it provides value and lowers costs through a simplified, consolidated network.

# ***Unisys Stealth Solution for Network***

## **Stealth Unleashes Your Full Potential**



- Promote sharing
- Extend the enterprise
- Strengthen agility
- Ensure trust

By establishing Secure Network Operations:

You can increase sharing of information.

You can extend the enterprise to support rapid collaborative decision-making.

You can strengthen agility to respond to rapidly changing operational needs.

And

You can ensure trust that data is available, correct, and protected.

# Unisys Stealth Solution for Network

The Unisys Stealth Solution

Security Unleashed

Questions?

[UnisysStealthSolution.com](http://UnisysStealthSolution.com)

**UNISYS**  
Imagine it. done.

**UNISYS**

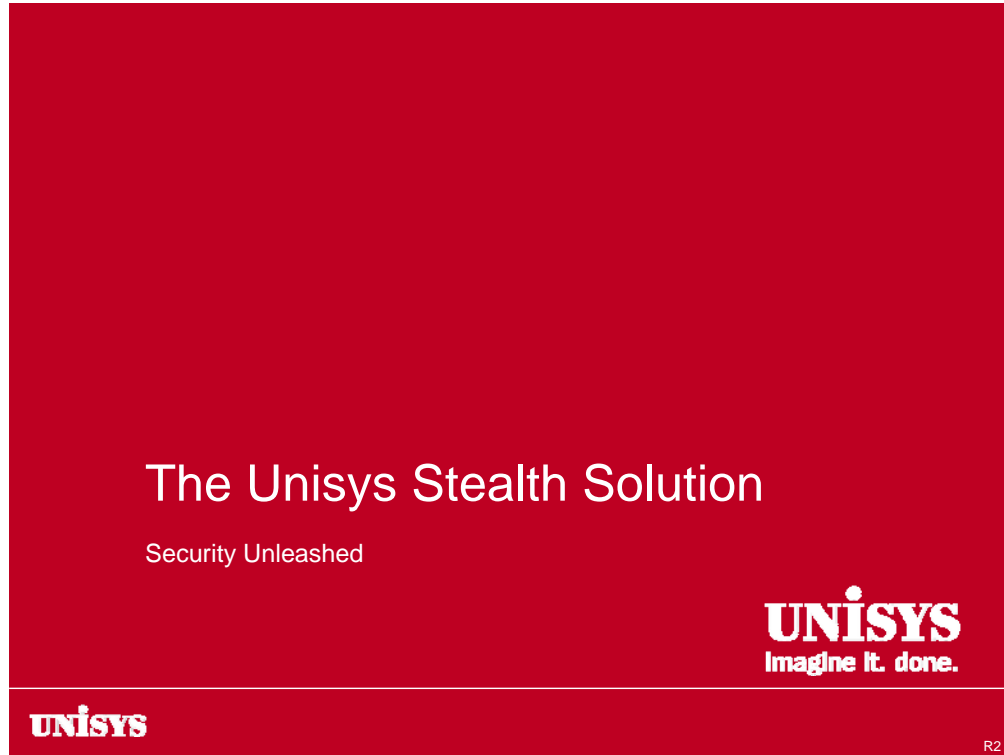
With Unisys as your partner, security doesn't hold you back. It empowers your operations. The Unisys Stealth Solution—security unleashed to create Secure Network Operations.

For more information, including a White Paper with a lot more detail on how Stealth works, visit the Unisys eCommunity. It's free and full of information about Unisys products and services, including:

- one stop destination for information
- browser based access to live Webcasts
- direct line to people who can help
- answers by Unisys experts to your questions, and
- collaboration with others who have shared interests

You will need to register, and will have the option to opt-in to receive email updates in areas of your interest.

# Unisys Stealth Solution for Network



**NOTE:** Unisys has vast experience in building trusted enterprises in many industries.

#### Supporting Facts

##### Financial

- 88 percent of the world's banks rely on Unisys
- 8 of the top 10 global life and pension insurers are Unisys clients
- 7.5 million bank accounts are protected by Unisys Managed Security Services
- 250 million income tax returns are processed annually using Unisys systems
- 50 percent of the world's checks are processed by Unisys solutions

##### Public Sector

- 1,500 government organizations are Unisys clients
- 115 million Brazilians vote electronically with Unisys solutions
- 58 million citizens worldwide use Unisys smart cards
- 300 justice agencies worldwide partner with Unisys

##### Transportation

- 600 airports worldwide use Unisys solutions
- 20 US airports use Unisys biometric solutions
- 29 percent of all air passengers are served using Unisys solutions
- 1 billion airline bags are cleared annually using Unisys solutions
- 35 percent of the world's air cargo is processed by Unisys solutions
- Unisys operates the world's largest RFID network across 25 countries

##### Communications

- 100 carriers in 40 countries rely on Unisys solutions
- 150 million voicemail subscribers worldwide rely on Unisys solutions
- 100 million FT Orange voicemail transactions daily use Unisys solutions