Case Study: MiStealth Data Security for Healthcare

Imagine a patented, NSA-certified, and hack-proof security solution that delivers unprecedented healthcare data protection by making communication end points undetectable on any network. Even better, make it an enterprise-wide solution that can be deployed and implemented incrementally and cost effectively, without disrupting current network operations.

AT A GLANCE:

- MiStealth creates Communities of Interest (COI) within a hospital network to tightly control which staff—doctors, administrators, and others—can access specific network assets.
- All COI can share the same physical infrastructure because MiStealth cloaks assets from non-COI members, rendering the assets undetectable.
- MiStealth allows you to save capital and operating expenses by simplifying a hospital network infrastructure and securely using any line—LAN, WAN, wireless, public or private.

Solution

Mitel MiStealth

Benefits

- Safeguards Protected Health Information (PHI)
- Facilitates compliance with HIPAA security rules and the Office of Civil Rights, enforcing HIPAA rules for data encryption
- Avoids costs associated with data breaches
- Saves capital and operating expenses by simplifying hospital network infrastructure
- Secures sensitive data across the hospital campus
- Protects data access for physicians, home care providers, and employees accessing information off-site

NORCOM

Protecting PHI Data in Motion

Problem

Ensuring sensitive information is secured while data is in motion across private and public networks

Information sharing is key to effective healthcare services. Health Information Exchanges (HIE) raise the bar providing information to consumers and sharing information across varying networks, providers, and jurisdictional borders, all while protecting patient privacy. Solutions deployed in HIEs must address the data protection requirements of HIPAA/HITECH and other data protection regulations and statutes.

Solution

Mitel MiStealth for Secure Virtual Terminal

- MiStealth uses military grade encryption and unique message-shredding technology to ensure data cannot be stolen and/or decoded by unauthorized users as it moves across networks.
- MiStealth creates COIs based on user credentials versus device location or physical topology, which control the ability to decode MiStealth formatted messages.
- MiStealth can add or remove users to COI or change access rights of COI members in just minutes.

Save Costs While Increasing Security

Problem

Saving money on IT while restricting access to sensitive data

HIPAA compliance requires secure controlled access to sensitive data to ensure patient privacy. Traditional methods to control access to information—separate physical networks for different departments—are expensive, complex, and increase management overhead. While flattening the network is more cost efficient, protecting access to private resources with passwords could easily result in a data breach.

Solution

Mitel MiStealth for Network

- MiStealth enables significant CapEx/OpEx savings by collapsing physical networks and reducing VLANs.
- Easy-to-manage user groups provide cryptographic separation to increase data security, facilitate compliance, and simplify security management.
- Only users with corresponding COI keys can access servers and applications. Non-COI users cannot see systems they are not authorized to access.

SSVT Solves the Leading Cause of HIPAA Data Breaches

Problem

Laptop theft is the leading cause of HIPAA data breaches

Senior clinical and business personnel use laptops to access huge numbers of patient records. If a laptop is lost or stolen, HIPAA-compliant practice management and Electronic Health Record (EHR) software packages with robust core IT systems are too often ineffective. In fact, more than half of all HIPAA security breaches are behavior-driven.

Solution

Mitel MiStealth for Secure Virtual Terminal (SSVT)

- SSVTs allow users to securely work anywhere without storing patient personal health information on laptops, desktops, or portable media, while remaining invisible on the open Internet.
- SSVTs safeguard patient data by neutralizing existing infections and malware, and protecting the data as it moves across the network.
- SSVTs leave no trace of user activity on the system and are configured to eliminate data loss at the end user's PC/laptop.
- If an SSVT is lost or stolen there is no risk of a third party gaining access to sensitive data—the SSVT will destroy its content when someone attempts to take it apart.

More Secure Telemedicine than Traditional VPN

Problem

Privacy and confidentiality requirements apply equally to conventional medical and telemedicine records

As with conventional medical records, a telemedicine clinician must safeguard a patient's electronic personal records and keep treatment information confidential. Transmitting sensitive information over communication lines can be vulnerable to hacks such as "man-in-the-middle" eavesdropping and "phishing" that employ hackers masquerading as trusted partners. Organizations must ensure that patient privacy is maintained and that data and image integrity is maintained at all times when being transmitted.

Solution

Mitel MiStealth for Network

- MiStealth creates a communications tunnel invisible to everyone except those who are pre-authorized as COI members.
- MiStealth is more secure than VPNs. MiStealth formatted messages are only decodable by a MiStealth endpoint with matching COI keys.
- MiStealth is not vulnerable to "man-in-the-middle" attacks. MiStealth secure tunnels eliminate a hacker's ability to insert him/herself between MiStealth endpoints.
- MiStealth prevents phishing. All MiStealth traffic flows between endpoints that share the same COI key, eliminating any opportunity for traffic to be maliciously redirected.

Emergency Preparedness

Problem

When disaster strikes, medical personnel must still access patient data

Your hospital data center has a disaster recovery "failover" plan, but if medical personnel cannot get to a facility, patient outcomes could suffer. Physicians must be able to triage remotely to advise onsite staff. Viewing patient test results and diagnoses over the Internet is not secure and may violate privacy regulations.

Solution

MiStealth for Secure Virtual Terminal

- SSVTs allow users to securely work anywhere, while remaining invisible on the open Internet.
- SSVTs safeguard patient data by not storing information on the device hosting the SSVT.
- SSVTs protect the data as it moves across the network.
- SSVTs are password protected and require user credentials to open a MiStealth connection, thereby eliminating the risk of misuse in case of loss or theft

MiStealth for Secure Virtual Terminal

SSVTs tightly secure and control information access and transmission over the Internet from anywhere by locking the communications channel to targeted endpoints.

SSVTs are deployed via locked down secure USB-based devices running MiStealth network security software. This virus-free, trusted environment is verified at each boot.

SSVTs can be deployed without making changes to your organization's current infrastructure or web enabled applications.

SSVTs enable healthcare workers to securely access:

- *Their own desktop located in the healthcare facility via a remote desktop (RDP) session*
- *Microsoft Remote Desktop Services or other virtual desktop infrastructure (VDI)*
- *Web enabled applications*

Save Money While Making Your Network More Secure

Mitel MiStealth offers unprecedented security and value. Key benefits include:

- *Protection of private healthcare data*
- *Facilitates HIPAA compliance*
- *Significant cost reduction*
- *Quick and easy deployment*
- *Incremental implementation*
- *Identity-based management*
- *No application changes*
- *Highest security performance*

MiStealth Security for the Cloud

MiStealth in the public or private cloud secures and isolates communication between virtual resources in a multi-tenant environment.

- *Mitigates threats*
  - » *Mitigates theft or misuse of IP within a tenant and between tenants*
  - » *Eliminates vulnerability from unauthorized access inside or outside the cloud*
- *Benefits*
  - » *Protection follows the workload, regardless of where it is physically executing*
  - » *Provides secure resource sharing within COI*
  - » *Isolates workloads between different COI*
  - » *Allows IT managers to extend their secure data center into cloud-based systems such as AWS or Azure*

Key Features

- FIPS 140-2 certified AES-256 bit encryption
- Information Dispersal Algorithm (IDA) provides a two-tiered level of network data protection and obfuscation
- Utilizes encryption and IDA keys that are separate from the user session keys and unique to each user or device
- Automatically drops endpoint connections after a defined period of non-use
- Determines secure access rights based on the identity credentials of users and devices as defined by the site's identity management system
- Supports multi-factor user authentication methods, such as Smartcards and One Time Passwords
- Operates over legacy switches, routers, and cable plants
- Provides the same level of data segmentation on wired and wireless networks
- Provides endpoint-to-endpoint encryption, such as user personal computer to application server, without the need for other data encryption devices in the network
- Fully compatible with standard TCP/IP networks
- Requires no changes to existing applications on personal computers or servers

Learn How MiStealth Can Protect Your Critical Information

Talk to an expert at Mitel.com or call 877-NORCOM1 to learn more.

NORCOM
TELEPHONY SOLUTIONS
Hosted • Premise • Virtualization

877-NORCOM1
norcomsolutions.com/mistealth