Healthcare Security

Introduction

Protect your patients, your practice, your brand, and yourself

As the healthcare industry continues to adopt network applications and tools, patient data must remain secure and private. This technical guide is focused on securing deployments and describes:

- The security threats facing healthcare organizations
- The options that healthcare organizations must take to protect the network
- Secure deployment options
- Access for mobility and remote access
- Security Policy Guidelines

The material described in this document provides guidelines and options for security in your healthcare network. Each healthcare organization has different needs, and a different product solution set might be needed to handle your organization's traffic and service load. This needs to be taken into account as you plan your security strategy.

Table of Contents

SECTION I: Why Healthcare Providers Need to Protect the Network

Summary

Network-based applications have transformed virtually every industry, and healthcare is no exception. Solutions that allow access to electronic medical records (EMRs), medical management systems, imaging, biomedical information, material management, patient accounting, admitting information, and online claims submissions are becoming commonplace in wireless, wired, and mobile scenarios.

As healthcare providers adopt new technologies, they also face new security threats from hackers, ransomware, computer viruses, and disgruntled employees. Human error also presents real dangers to healthcare networks: http://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months

In the earliest implementations of Internet Protocol, there were not specific provisions for security in its design. As a result, healthcare providers also need to make sure that their IP implementations take into account network security best practices, services, and products that can mitigate the inherent risks associated with today's integrated healthcare.

Fortunately, most security breaches can be prevented, and there are numerous network security tools available that are easy to deploy and use. Cisco has a security suite that is best in class in its capability to provide complete defense for information, applications, and services.

Security must be considered a process and not a product-based point solution.

1. The first step in the process that an organization should take to establish a secure network infrastructure is to develop a formal security policy to define the roles, responsibilities, acceptable use, and security practices it will implement and enforce.

2. After developing the policy, the organization should then monitor and assess the implementation of said policy by using established best practices as a benchmark. Providers should closely examine and test their network infrastructure to identify potential vulnerabilities, including physical security, to establish a vulnerability/risk matrix.

3. As the implementation continues, providers must continually evaluate each area of the network, determine potential threats, and implement the appropriate security modules to mitigate them.

If the provider does not have a technical security expert, Cisco and its qualified partners can assist in developing an appropriate architecture that will meet the established security policies for your healthcare organization.

The Need For Network Security In Healthcare

While information security is a top priority for any organization, healthcare providers must be especially diligent in protecting confidential patient data. In addition to the evolving threat posed by hackers and other intruders, government regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), establish privacy requirements for Protected Health Information (PHI). Merely deploying a network firewall is insufficient. Instead, providers need to take a comprehensive approach to protecting patient information at every potential point of access, both inside and outside the network.

As healthcare organizations increasingly rely on networks for their core operations, they become vulnerable to nontraditional attacks. Compromised security can disrupt critical functions, interfere with a clinician's ability to treat patients, expose providers to substantial liabilities, risk the loss of lives, and ruin an organizations reputation.

Employee threats must also be considered. Though possibly unintentional, these threats can still cause significant damage and disrupt patient care. Intentional attacks by internal employees are the most common disruption, and are 10 times as costly as an external attack: http://www.isdecisions.com/insider-threat/statistics.htm

Network attacks vary by systems and location in the network. Some attacks are elaborately complex with specific motives, while others are malicious annoyances meant to disrupt your organizations network infrastructure and accessibility.

Common network threats include:

- **Packet Sniffers:** Hackers can abuse this legitimate management tool to capture data that is transmitted over a network, such as usernames and passwords.
- **IP Spoofing:** This occurs when a hacker inside or outside a network impersonates a trusted computer to gain access to network information.
- **Defacing:** For healthcare practices with a web presence, defacing (the changing of files on a web server) can damage patient and partner confidence in an organization's ability to protect sensitive data.
- **Denial of Service (DoS):** Perhaps the most widely publicized form of attack, a DoS can be initiated using programs that are available on the Internet. It focuses on making a service unavailable for normal use, often by exhausting a resource on the network, operating system, or application.
- **Spam:** Another growing threat to network operations is spam (unsolicited mass email), which slows mail servers, overruns storage space, and reduces user productivity by clogging mailboxes.
- **Man-in-the-Middle Attack**: Hackers who have access to packets that move across a wired or wireless network can initiate a man-in-the-middle attack. During this attack, hackers hijack a network session to gain access to private network resources, steal information, or analyze traffic to learn about a network and its users.
- **Viruses, Trojan Horses, and Worms:** End-user PCs and workstations are especially vulnerable to viruses and Trojan horse attacks. A virus is malicious software code that is attached to another program to execute an unwanted function on a user's PC. Trojan horse attacks are similar to viruses, but they disguise the application to look like something else. Worms are malicious replicating programs.
- **HTTP Exploits:** HTTP attacks use a web server application to perform malicious activities by exploiting the relatively insecure access to an organization's Web servers. If attackers can take control of a web server, they can access resources that would otherwise be unavailable.
- **Application Layer Attacks**: Hackers can initiate application layer attacks using several different methods. One of the most common is to exploit well-known software weaknesses commonly found on servers—such as send-mail, HTTP, and FTP—to gain high-level administrative access to a computer.
- **Ransomware:** The rise of ransomware over the past year is an ever growing problem. Business often believe that paying the ransom is the most cost-effective way of getting their data back – and this may also be the reality. The problem we face is that every single business that pays to recover their files, is directly funding the development of the next generation of ransomware. As a result of this we're seeing ransomware evolve at an alarming rate:
  http://www.cisco.com/c/en/us/solutions/enterprise-networks/ransomware-defense/index.html

Costs of Poor Security Network

Security breaches can result in fines, legal liability, personal liability, lost productivity for clinical and administrative staff, and the devastating loss of partner and patient confidence. The worst-case scenario would be punitive damages resulting in patient identity theft or changing of EMRs resulting in patient death. In addition to the cost of repairing the network itself, the impact on a provider can include:

- **Disruption of clinical and administrative processes:** Network downtime and loss of critical server and application operations are common immediate effects of poor security. The more that providers rely on networks, EMR, practice management systems, and clinical information systems, the more an unavailable network can interfere with a provider's ability to treat patients.

- **Loss of patient and partner confidence:** A practice that has been victimized by hackers may find it difficult to earn back trust and loyalty. Patients, insurers, and clinical partners are understandably reluctant to share private information with a practice that cannot protect it. Under HIPAA, business associate agreements prohibit the sharing of PHI to organizations that cannot ensure its confidentiality.

- **Financial costs:** Under regulatory requirements like HIPAA, providers that fail to protect confidential patient data can face stiff penalties and liability from litigation. To combat these threats, providers need a consistent, scalable, enterprise-wide security solution that continually safeguards their networks.

Benefits of Maintaining a Secure Healthcare Environment

Providers that employ strong security do more than just protect patient data. They establish new capabilities for improving patient care and business operations. A secure healthcare network can enable:

- **Access to information at the point of care**: A secure wired or wireless network allows clinicians to access and update clinical records directly from an examination room or lab, providing a more up-to-date, comprehensive view of the patient where caregivers need it most.

- **Increased mobility:** Secure wireless networks and VPNs allow clinicians to access patient information, lab results, and medical libraries from notebook computers, PDAs, handheld devices, and portable phones, as well as from remote and home offices.

- **Enhanced productivity and reduced costs:** Once a secure, reliable network is in place, healthcare providers can deploy applications that streamline resource intensive back-office processes. Solutions can include business management applications, claims processing systems, and systems for finance and human resources management.

- **Improved patient care and safety:** Digital clinical applications and real-time information sharing enabled by a secure network provide a more unified, up-to-date view of the patient, which results in faster, more accurate, less redundant care. When clinicians can securely update records and digitally write orders and prescriptions at the point of care, they can substantially reduce errors associated with handwritten, paper-based systems.

SECTION II: How Healthcare Providers Can Protect the Network

Threat-Centric Security Model

Networks are ever changing and they continuously evolve. New devices, mobile devices, and cloud offerings make it impossible to have a static network. With all the change happening, so are the threats to healthcare networks.

It is no longer individuals that are just trying to get in, but now there are teams and groups of individuals that are well organized, educated, and they have made a business for themselves stealing and leveraging information they can gather. They are financially motivated. They are always evolving on how they attack. This leads to the complexity of security solutions because of various point products that people use to mitigate risks.

A threat-centric security model allows customers to provide protection before, during and after an attack.

> **Before:** Think of this as your baseline or your perimeter to allow and disallow traffic. It helps identify what is on your network by identity and access control. In this arena, firewalls are the initial line of defense. However, what goes through still needs to be inspected at a deeper level.
>
> **During:** Think of it as inspecting at a single point in time and looking at traffic as it comes across the wire to determine if it is good or bad. But this is not always 100% effective. Files can change after traversing the network. They can appear good at first but act negatively later.
>
> **After:** This is the after or the attacks that are successful. You need the ability to analyze data traversing the network and use the information to determine what has changed, and go back and change your policies about files and pull them out memory and put them in quarantine and begin to stop the threat, you need to be able change the access policies of users themselves if they are hacked, and change the access policies to start blocking traffic. Cisco can do this because we are sharing information amongst our architecture and communicating across all our products.

Threat-centric blueprints are based on years of experience developing security solutions for organizations of all sizes around the world. Organizations that use these blueprints can benefit from proven best practices for creating robust security solutions that protect both patients and healthcare organizations.

Cisco has helped develop a threat-centric security model to help protect your intellectual property, and to safeguard their patients' information, therefore protecting your brand. This model helps you safeguard before, during, and after an attack. The Cisco® security portfolio works together during all events and allows for automation to detect, protect, and isolate threats before they affect and impact your network, data, and patients information.

There are three major categories of creating a threat-centric security model for a healthcare provider network:

1. Setting up a security policy
2. Ongoing monitoring and revising the organization's security policy
3. Implementing new security modules as indicated by your security policy and network needs

Creating a Security Policy

The first step in helping to ensure a secure healthcare environment is to develop a sound security policy that addresses all the requirements to protect people, processes, data, and technology. A security policy is a formal, publishable document that defines roles, responsibilities, acceptable use, and security practices for the organization. It is an essential component of a complete security framework, and it should be used to guide investment in security defenses.

Considerations for Implementation Security Policy

Challenges are continually evolving, and deploying technology alone is not enough to combat them. Healthcare organizations must develop end-to-end strategies for combating security threats, including robust technologies, a comprehensive security policy, and in-depth evaluation of potential vulnerabilities. A sample analysis, such as that shown below, can be applied to determine where resources should be applied to mitigate the threat in any network location.

Threats (Targets)

- Type A: Targets Critical Infrastructures
- Type B: Targets Near-Critical Infrastructures
- Type C: Insignificant Targets, Minimal Impact

Vulnerabilities (Damage Potential)

- Type 1: Catastrophic Loss of Life and Money
- Type 2: Significant Loss
- Type 3: Everything Else

Risk = Threat x Vulnerability

Effective Security If and Only If:
Prevention + (Detection + Response) > Acceptable Risk
T t

T = Development/Deployment Time ~ Days, Months, Years
t = Reaction Time ~ Seconds, Minutes, Hours

The Elements of a Security Policy

Since a security policy affects all aspects of a healthcare ecosystem, it should be created through a collaborative process that includes representatives of clinical, administrative, legal, and technology staff. A cross-functional team will help ensure that all interests of the provider are met while delivering a secure system. Developing a policy can take weeks, depending on the size of the organization.

The elements of a security policy include:

- **Policy Statement:** A concise statement of the document's purpose, a policy statement should be specific to the individual organization or department and be auditable, controllable, and enforceable.
- **Scope:** The policy should include the type of information and resources covered by the policy (for example, whether it applies only to electronic resources or incorporates paper-based physical security or other forms of intellectual property).
- **Roles and Responsibilities:** Policies must define the roles and duties of those managing security and information systems, as well as the responsibilities of clinical and administrative staff.

- **Security Directives:** The policy should offer detailed security directives that must be followed. Directives should cover the types of hardware and software that employees can use, any third parties that will have access to the network, remote access, name and password management, IDSs, and other requirements.

- **Acceptable Use Policy (AUP):** The AUP addresses issues such as personal use of the Internet and prohibitions against accessing Internet sites that offer inappropriate content.

- **Incident Response Procedures:** Among the most important aspects of a security policy, incident response procedures define how notification will occur for various threats and the specific actions that are required for response.

- **Document Control Factors:** Organizations should define how updates to the security policy will occur and how often they should be reviewed and validated.

Providers may want to begin with a simplified, high-level security policy and refine it over time. Sample policies can be found at www.sans.org. Cisco recommends that organizations postpone making any major security purchase decisions until a policy is in place.

Administrative and clinical processes will likely change over time. Practices should create guidelines for continuous review of the security policy to incorporate new threats and organizational changes.

A Modular Blueprint Based on Best Practices

Each security blueprint uses a modular approach that offers two main advantages.

1. First, it allows network planners to address the security relationship between the functional blocks of the network.

2. Secondly, it enables planners to evaluate and implement security on a module-by-module basis, instead of attempting the complete architecture in a single phase.

Cisco has developed blueprints for small, midsize, and large networks that incorporate wired and wireless infrastructures, satellite locations, and remote connectivity.

As healthcare customers continue to embrace technology, security is top of mind. They recognize the opportunity to be hacked, and they also realize the responsibility they have to protect and represent their brand, their intellectual property, and to safeguard their patients' information. Every day we see the devastation hacking bring to companies around the globe. Healthcare customers are realizing they are a primary target (https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/) and need intelligent security solutions.

Cisco continues to make wise investments in our security products and solutions. We have a strong architecture strategy, powerful technology, comprehensive portfolio, and the largest security team of engineers in the industry. We also provide the capability to have the network be a part of the defense. Based upon policies created, the network can react to prevent threat and attacks from infiltrating other portions of your network and devices.

In today's world, everything is connected with more and more devices being plugged in. With that in mind, you have to consider all healthcare devices and public access might create security vulnerabilities. In addition, threats are more persistent today than ever before. This makes cybersecurity as important as local network security. Today, it's not about if you will be compromised, but when.

Healthcare customers must ask themselves, if you knew you were going to be compromised, how would you prepare? Do you have a defense strategy? Do you have a combination of products that work well together or disparate systems that are cumbersome and make it hard to isolate vulnerabilities? Do point products create vulnerabilities? If we were hacked, how long would it take to realize it has happened?

Today people watching screens do not work effectively to counteract security threats, healthcare organizations need a seamless arch that detects and reacts to anomalies. Reducing remediation time helps protect data integrity. Having a security infrastructure that is pervasive, integrated, continuous and open helps you reach your security goals.

The Components of a Healthcare Security Solution Blueprint

While the threats to healthcare networks are real, protecting against those threats can be relatively easy and straightforward—even for smaller organizations without a large IT staff. Network security tools include:

- Policy Access and Control Solutions
- Next Generation Firewalls
- Next Generation Intrusion Detection Systems
- Advanced Malware Protection
- Web Security
- Email Security
- Cisco Umbrella
- Security Advisory, Managed and Implementation Services

Cisco leverages these products and solutions to help healthcare organizations protect their networks and stop before, during and after threats. The following section will highlight the products you can use to improve the security of your architecture.

Policy and Access Control Solutions

Healthcare customers are trying to manage a more complex IT ecosystem. By complex – we refer to remote users, IoT devices, and mobile devices, along with wireless and VPN networks. This leads to a complex set of rules and architectures that determines who and what can go where. Believe it or not, complexity is the enemy of security.

The Cisco Identity Service Engine (ISE) helps simplify things. One of its unique features is its ability to distinguish between different types of devices (corporate laptops vs. mobile devices). This type of visibility is what we call contextual awareness. It is a vast improvement over what most organizations have today. You can use this awareness to drive one policy across the entire network.

Many organizations have a multiple policies today. They use different policies for wired, wireless, and VPN networks. Now you have the ability to create a single network policy. By having policies that are easy to manage and simplifying the network architecture, we improve security and reduce cost. We do this by segmenting the network properly, which prevents threats from moving around the network and going anywhere they choose. Many threats move around the network until they find valuable information. If a vendor or patient brought in a threat, the threat should never get near a credit card database or patient data.

Another way we protect is profiling the devices as they access the network using Cisco's Identity Services Engine (ISE). If a vulnerable or noncompliant device accesses the network, ISE limits its access to what is deemed necessary and it is not allowed near classified information. Finally – if a

healthy device becomes infected while on the network, ISE can exchange his information with other security devices using pxGrid and instantly quarantine it in order to stop the infection from spreading.

For more information concerning ISE:
http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

Cisco Firepower Next-Generation Firewall

A firewall provides basic but a necessary level of security for access control. As security threats have evolved, we have improved firewall capabilities from access control to threat control. You can do this by licensing firepower services for the ASA to get a higher level of protection, which is a key benefit. You can leverage existing investments in your ASA products. To get this level of protection in the past, customers would have to purchase multiple devices adding cost and complexity. Now, everything can run on a single platform. Most healthcare organizations have a base firewall. Cisco Firepower® solution gives them greater visibility into devices and applications. This helps save money and improves security through automation. With Cisco Firepower solution you get Cisco Application Visibility and Control (AVC), URL filtering, and Advanced Malware protection (AMP). This transforms the basic firewall into a -centric security device that provides protection across the entire attack continuum. This is before, during, and after an attack scenarios mentioned earlier. This provides contextual awareness of all users, applications and devices on the network.

For more information on the Next Generation Firewall, visit
http://www.cisco.com/c/en/us/products/security/firewalls/index.html

Next Generation Intrusion Detection System

Healthcare customers can have comfort in knowing that Cisco goes a step further when it comes to intrusion detection. Cisco not only detects intrusions, but also dissects the traffic for context. We examine applications, operating systems, user names, physical locations, URLs, files, etc., on the network. We not only identify the threat but the context about the threat, and how the threat relates to your people, processes and things. We use this visibility to simplify and automate management operations. Because we can see what is on the network, we can tell the next generation intrusion protection system (NGIPS) to look for attacks against assets. Then, when we see the attack against a device, we can understand if it is a valid attack or random noise then prioritize events accordingly. This saves time and money, and increases security.

Additional security measures offered within IPS are application control, URL filtering, and Advanced Malware Protection (AMP). AMP functionality is very unique to Cisco. Threat intelligence and research keeps the device up to date against the latest threats. The Cisco Talos Group of researchers has vast and unique resources of information to pull from. They are able to share and correlate threat information with other cisco security products. We can offer the solution as a security appliance, also available as a virtual deployment such as a license upgrade to an ASA firewall known as FirePOWER™ Services for ASA.

For more information on the Next Generation Intrusion Detection System, visit
http://www.cisco.com/c/en/us/products/security/ngips/index.html

Advanced Malware Protection

Malware is made up of two words – *malicious* and *software*. Any software used for malicious intent can be malware. It starts with threats and Cisco takes a threat-centric approach to threat protection. Hackers are clever and are always working on ways and strategies to circumvent security devices and avoid detection. Cisco Advanced Malware Protection (AMP) helps identify threats even after they get through and pass initial inspection. We do that with continual analysis. While most technologies are point in time, make a decision, and then move on. Cisco remembers that decision and continues to gather information about files. If a file is initially thought to be good, we continue to watch it to see if it starts acting badly. If it does, we can change network policies to stop it. Remembering our decision gives us a tremendous amount of visibility into where files came from, where they went, and what machines they are on. If you know this, you can help clean up issues much faster. This saves time and money, improves your security, and increases uptime.

AMP is available as endpoint software, for networks as a stand-alone appliance, and can be licensed in most of our security devices like the ASA firewall, web, and email security appliances. Each can work alone or together. These all share information to a centralized repository at the Talos Group. Once a threat is determined to be bad, all the products and customers using AMP are protected from it going forward. Today, can you act on threats that have gotten into your network? Can you determine how a threat was introduced to your environment, and where it went? How fast can you determine that a threat got in, and how many tools do you use for incident response? The centralized nature of this solution allows us to share data across multiple technologies to reduce threat quickly, efficiently and effectively.

To find out more about our Advanced Malware protection, visit
http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

Web Security

Why should hospitals be concerned with web security? Why have web security? Often times the web is one of the first attack vectors for hackers. The other being email. But for the web, HTTP and HTTPS are most common. Web security can protect companies against their own users. Look at the Cisco 2016 annual security report (http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html) – the third aspect in Cisco web security is uniquely suited to protect networks that are global and highly distributed. What is the solution? It comprises two different products – web security appliance and cloud web security.

Cloud web security is a software-as-a-service offering – The appliance is an on-premises solution in a centralized, highly concentrated customer environment. The cloud-based solution is helpful for customers that have global networks. Because it is a cloud service, it is uniquely able to protect the networks that are global in nature and highly distributed.

Another aspect of web security is what it allows customers to do. An administrator with web security can set policy and controls against two things in the network: inappropriate browsing and malicious content while browsing online. The administrator can also pull reports in order to see the internet usage occurring within the company network.

So how does Cisco protect against that malicious web attack vector? First, Cisco web security is integrated with AMP to look at malicious files and to provide retrospective security for those files that turn bad after a certain amount of time. So we can go back in time and find out where those files are and remediate. The next important integration to mention is with cognitive threat analytics, or CTA. With CTA we are looking at behavior in the form of command and control traffic or web requests.

Lastly, Cisco web security leverages Talos global threat intelligence like all of our Cisco products do so that we can actually share information and threat information across multiple products and take advantage of the large amount of traffic that Talos is able to see.

For more information on Web Security:
http://www.cisco.com/c/en/us/products/security/web-security/index.html

Email Security

Many of the attacks that affect a healthcare organization pass security measures by coming in through email. Healthcare organizations need an email security system to protect their email gateway. Cisco has two Cisco IronPort® solutions for email security. We offer it as an Email Security Appliance (ESA), or as a cloud solution, Cloud Email Security (CES). These solutions provide industry-leading cloud-, virtual-, and appliance-based email security. We provide multilayer defense against spam and virus attacks, and we protect against phishing and malicious malware attacks. We use multiple spam and virus engines to ensure the highest catch rate and also the lowest false positives.

As another part of our solution, we also provide email encryption to protect sensitive transmissions as they traverse the Internet. We have also integrated AMP to protect healthcare customers from more sophisticated attacks. How does email security fit directly into the Cisco security strategy? Cisco Talos provides global threat intelligence across our security portfolio. Cisco's email security also leverages Talos to provide dynamic attack information to protect customers before and during an attack. With the AMP add-on license, we also protect healthcare customers during and after an attack with file retrospection where we can look back and see if a file has changed after it entered the network.

What differentiates Cisco is that we offer an email security solution, not just a point product. When added to our other solution offerings, you have additional protection. Solutions like Talos global threat intelligence provides real time information from outbreaks around the world. Another benefit is AMP and Threat Grid® technology, as well as Zix Encryption for email security. Cisco is able to provide customers not just a point solution, but also an architectural solution that surpasses most offering today. You can get this protection from either the cloud or our on premise appliance.

For more information on email security, visit
http://www.cisco.com/c/en/us/products/security/email-security/index.html

Cisco Umbrella

Cisco Umbrella prevents system compromise and data exfiltration by blocking connections to malicious sites and containing command and control callback. We provide visibility into the infrastructure that attackers set up and leverage for an attack. We show the relationships and connections between domains, IPs and autonomous systems across the Internet, which makes it easy for Cisco to uncover malicious sites and find related attacker infrastructure. With Cisco intelligence you can speed up Internet investigation and even uncover domains and IPs that may be using future attacks. We are also able to help enforce acceptable use policies for Internet browsing, and provide insight into cloud services and IoT devices in use across customer's environments. As a result of using Cisco Umbrella products, there are a number of measureable benefits that healthcare customers see.

Two key products to Cisco Umbrella are Umbrella and Investigate. With Cisco Umbrella Investigate, our live global threat intelligence can easily be incorporated into the customer's existing Internet response process to give them more context during investigations.

With Cisco Umbrella, you have a cloud-based solution that is very simple to deploy. Most healthcare customers can be up and running within 30 minutes. We are able to detect more, and healthcare customers are ultimately able to see a reduction in the number of security information and event management (SIEM) alerts because we are able to stop malware phishing attempts before they can compromise a system. That means your security team is freed up to focus on more important tasks.

Cisco Umbrella is for enforcement, and Investigate gives you access to all out threat intelligence. Umbrella provides protection against malware, phishing, and command and control callbacks. Key points to know about Umbrella: threat prevention at the DNS layer. We are able to see requests from malicious domains or IPs and actually block it before a connection is ever made. We can also detect command and control callbacks from already infected machines and stop possible data infiltrations. Umbrella can protect healthcare users easily whether they are on or off the network. So even if users are working at their home or a remote clinic, users still have the same protection without the need for VPN. Since it is cloud delivered, Umbrella is always up to date and administrators do not have to worry about applying updates. Because we work at the DNS layer, it does not matter what port or protocol or app is being used. We see all of the requests and block connections to malicious domains and IPs. We have a number of turnkey and API-based integrations. So healthcare customers can easily integrate and extend protection with our product. In addition, no professional services are needed.

Cisco Umbrella Investigate gives you access to all of our intelligence about domains and IPs across the Internet. This intelligence is also what is empowering Umbrella and enforcement. It provides access to a large graphical database of all the DNS requests and other contextual data from across our global network. With that data we are able to automatically discover and predict malicious domains and IPs. With this information customers can enrich their existing security data with our global intelligence. And they can access it through our web user interface or an API. It provides healthcare customers a single source of data they can use to research any domain or IP across the Internet.

How do we get our intelligence – we ingest a massive amount of diverse data from our global network in real time into this graph database. Then we continuously run statistical models against it. Our security research team constantly analyzes this information as well. And using this combination of human intelligence and machine learning, we identify current and future areas of concern on the Internet.

Cisco Umbrella maps across your before, during, and after framework mentioned earlier. Before the attack, customers can use Investigate to do threat research and uncover a potential attacker infrastructure. Umbrella can proactively protect users from connecting to malicious sites and does it at the DNS layer before a connection is ever made. During an attack, Umbrella can contain and control callbacks, which stops data infiltration from already infected devices. After the attack, Investigate can provide live threat intelligence about all domains and IPs during an event investigation.

To learn more about Cisco Umbrella, visit
https://learn-umbrella.cisco.com/solution-briefs
https://umbrella.cisco.com/

Security Advisory, Managed and Implementation Services

Security is top of mind, or should be within your healthcare organization. Healthcare providers are struggling with a very real and dynamic threat landscape. They are more concerned about patient health and day-to-day business, rather than running a security operations program.

Cisco can help you manage both.

It can be done more efficiently and cost-effectively. We offer managed and cloud delivered solutions with the main goal to identify, prioritize and respond to potential threats. We take the security event data into our correlation platform, analyze it, and then determine what incidents our customers need to engage on. That allows the customer to focus their primary resources on business tasks.

Before security decisions are made, many healthcare customers like to speak to companies with strategic security programs so they can help develop the metrics to run their security program and strategies for their organization. This could also help with governance risk and compliance, identity and access management.

Cisco has the expertise and programs in place to conduct this type of a strategic review with a product-agnostic point of view. We can help you in a variety of ways:

- Manage boardroom discussions around risk and what the financial impacts to the risks are at a higher level.
- Conduct compliance assessments to examine where healthcare customers are and provide roadmaps to improve risk over time.
- Conduct additional assessments to include penetration testing to assess applications, cloud plans and the management of real threats.
- Help build incident response programs or be there when a breach occurs and assist with remediation.

The outcome would be to deliver an increased level of risk posture, helping the customer to understand their risk, and how to reduce it over time.

We have the expertise and intelligence based upon information, gathered from around the world, to support existing security teams. In addition, we offer the best in breed products and solutions to support customer needs.

By allowing Cisco to be part of your team, we can work together and deliver value by focusing on these three key metrics:

- **Speed** – improve speed to identify and report on incidents over time.
- **Accuracy** – when we provide an incident to our customers, they realize it has value and it is not a false positive.
- **Focus** – recommend what the next steps are – segment off a piece of network, remediate a machine or quarantine a solution.

Cisco integration services can also help implement your firewall, IPS, and ISE, and manage migration from legacy to new Cisco products, helping complete deployments vs. long deployment cycles. Cisco services can help healthcare organizations realize the benefits of their security solution sooner and reduce your risk faster.

For more information visit
http://www.cisco.com/c/en/us/products/security/service-listing.html

None of the components just mentioned on its own can fully protect healthcare systems, but when integrated, they are highly effective in keeping a network safe from attacks and other security threats.

SECTION III: How Healthcare Providers Connect and Manage as Secure Network

Access for Mobility and Remote Access

Today, clinicians are more mobile than in the past. They move from room to room and facility to facility to deliver the best patient care. This leads to the need for secure mobile access that determines who and what can go where. Healthcare providers need to provide secure access for mobility including: IoT devices and mobile devices; along with wireless and VPN networks.

WLANs

Perhaps no industry has benefited more from wireless networking than healthcare. Clinicians can now use wireless-enabled handheld devices to access clinical information systems, medical records, imaging systems, and other resources—right from the patient's bedside. However, WLANs also present unique security considerations.

Since overall network security is only as strong as its weakest link, providers need to be as certain as possible that WLANs are providing the same level of access control and privacy as wired LANs. In contrast to a wired LAN, in which a physical connection controls access to the network, WLANs broadcast data through the air. Any wireless-enabled device in the area—such as a patient's laptop in a waiting room or a wireless PDA in a neighboring office—presents a potential security threat

Deploying WLAN Security

The two primary components of WLAN security are authentication and encryption. Authentication helps ensure that the user and the access point are who and what they say they are. Encryption helps ensure that data remains uncorrupted throughout transmission, and that anyone who might intercept data will be unable to read it.

Teleworking and Remote Access

Many providers have adopted remote connectivity solutions that give clinicians remote access to necessary applications. Using VPNs, clinicians can now use highly secure connections to access patient and clinical information from any remote location, including satellite facilities—and even their homes. As remote connectivity becomes a standard healthcare tool, practices need to provide remote connectivity solutions that are as highly secure and reliable as the wired and wireless office network. Any solution must account for the sensitivity of the information as well as the access method. Access may be denied based on any number of parameters in order to enforce security policies and maintain patient confidentiality.

Providers should implement remote connectivity solutions that support several options. For example, although DSL may be the practice's broadband technology of choice, some physicians may have access only to a dialup Internet service. Regardless of the access method, the provider network must help ensure proper routing, encryption, and access control.

Today, VPNs are the most popular and versatile remote-access solution. VPNs enable users to securely connect to provider resources over a public network, using any access method. Providers can use extranet VPNs to connect to their suppliers and partners, providing limited access to specific portions of the network for collaboration and coordination.

A healthcare VPN solution must include all of the security features needed to keep VPN traffic private and secure. VPNs use a tunneled connection to carry encrypted data between the remote user and the provider network. Providers should make sure that their VPN solutions support primary tunneling protocols, including IP Security (IPSec), Layer 2 Tunneling Protocol, and generic routing encapsulation.

VPN hardware and software client remote clinicians can use software or hardware VPN clients to connect with the provider. They can take advantage of Secure Sockets Layer (SSL) VPNs or clientless VPNs that require only a web browser. For clinicians who use the solution while traveling or working from a remote location, the software client or SSL VPN makes the most sense. However, when using a software client, information on the clinician's PC is protected only while connected to the VPN tunnel. Information on the laptop is not inherently protected while a clinician is surfing the Internet if he or she is not connected to the VPN tunnel.

For a clinician's home office, a hardware client, such as a firewall appliance or a broadband router with firewall features, provides a more secure connectivity solution. In a small satellite location with more than one user, the office router or firewall can also act as a VPN client, providing highly secure remote access for all users behind it and eliminating the need for each user to launch a VPN software client. In addition to day-zero threat protection, Cisco Security Agent has firewall capabilities and complements any type of remote-access VPN.

Satellite Locations

A healthcare provider's satellite locations function as independent, autonomous networks with their own local servers and user workstations or may rely on central processing resources. The satellite office should include the same components, design principles, and considerations as the security solutions discussed above.

Providers have two options for connecting the satellite locations—private WAN links and public links.

Private WANs: Private WANs such as Frame Relay, ISDN, T1, and Fractional T1—enable greater control of network traffic, including quality-of-service (QoS) support and traffic prioritization. Dedicated WAN links are more private, in that they are not shared connections; however, private WANs do not provide inherent security, since the traffic is not encrypted. This alternative typically costs more, with increased operating and ownership expenses.

Public Links: Public shared links, such as cable and DSL, are less expensive but less secure. To address this, IPSec VPNs use encrypted VPN connections over a service provider network or the Internet to support WAN connectivity. A provider should take HIPAA into account when making WAN choices; encrypted IPSec VPNs offer considerably more privacy protection.

Management Tools for a Secure Network

Strong healthcare security requires more than just the right network design, hardware, and software. System administrators must also be able to effectively monitor and manage the network with its integrated security system. The correct management tools allow administrators to view and control activity on the network at any time, and to access all network devices through a single interface. Healthcare organizations can determine the best management tools for their network by meeting with their Cisco account manager and partner team.

Conclusion

As the risks and security concerns for healthcare networks grow, providers should take a systematic, multitier approach to planning and deploying a highly secure network infrastructure. This approach should include a careful evaluation of each area of the network, identification of potential threats, development of a practice security policy, and implementation of network security technologies.

The Cisco security suite of products provides a comprehensive, modular approach to security—one that can evolve, as a provider's needs change. This approach encompasses every aspect of the data infrastructure, from the desktop to the WLAN to the network perimeter and the teleworker—and all areas in between.

While security measures must be comprehensive, they need not be difficult to deploy and manage. Cisco offers numerous security solutions designed specifically for small and midsize locations with limited IT staff and expertise. With so much at stake, healthcare organizations cannot risk compromising the trust of patients and partners.

Cisco offers hands-on experience and intimate knowledge of best practices gained from working with healthcare organizations around the world, and can help providers deploy highly secure network services with confidence.