WHITE PAPER

How healthcare benefits from cloud-delivered security

Healthcare IT professionals are swimming upstream to overcome security challenges. Cloud-delivered solutions may represent a life preserver in their efforts to reduce risk, simplify management and control costs.

The day in the life of a healthcare IT professional can be a whirlwind of activity – some of it built around exciting opportunities, but seemingly much more of it centered on conflict resolution and problem solving.

When you're not dealing with escalating security threats, tight budgets and inadequate in-house security expertise, you're trying to make doctors, nurses, researchers and administrators happy with support for more devices, applications and services. Managing and securing a dizzying array of endpoints – from traditional desktops and notebooks to personal mobile devices and even Internet of Things (IoT)-based equipment such as smart medical devices – is itself enough to make an IT executive's head spin.

Risk management, in particular, is a huge issue for healthcare IT. And that all starts with dealing with malware, ransomware and other threats that impact regulatory compliance, legal exposure, corporate governance and the very essence of the healthcare mission – improved patient outcomes.

How in the world can you keep up with the expanding security threat landscape, let alone get ahead of the game?

cisco Cisco Umbrella

TechTarget Custom Media

A TECHTARGET WHITE PAPER

For more healthcare IT professionals, cloud-delivered security solutions are the way to go. This is a big development, considering how long it took for the healthcare industry to embrace cloud and how stretched-out the adoption process has been. That's changed dramatically, however: Healthcare industry expenditures on cloud computing will experience a compound annual growth rate of more than 20% by 2020.[1] The industry has quickly transitioned from being hesitant – in some cases, simply afraid – to move to the cloud to wrapping both arms around the technology in order to leverage its many benefits.

And, a big driving force for using cloud-delivered security as a way to turn chaos into a cohesive, comprehensive security framework is the emergence of new solutions that combine faster deployment, easier management, greater functionality and improved cost efficiency.

This paper looks at how a day in the life of a healthcare IT professional can be transformed from firefighting and pain avoidance to strategic, confident actions that make everyone's work lives better. You'll read about specific steps you can take in order to actively reduce the number of ransomware infections across the organization, as well as how to spot, block and remediate other threats before they do real harm to the enterprise and your patients.

Turning problems into opportunities

Although security is obviously an important issue in all industries, healthcare presents a number of unique and particularly problematic challenges. These concerns cover a gamut of factors, from regulatory to technological, as well as unique workflows and business processes.

In fact, research by the healthcare industry's leading association for technology indicates that 81% of survey respondents believe they need "more innovative and advanced tools" in order to confront and overcome security threats.[2]

1 "Healthcare Cloud Computing Market Worth $9.48 Billion by 2020," Markets and Markets, June 2015, http://www.marketsandmarkets.com/PressReleases/cloud-computing-healthcare.asp

2 "2015 HIMSS Cybersecurity Survey," Health Information and Management Systems Society, June 2015, http://www.himss.org/2015-cybersecurity-survey

Why using DNS can protect PHI

Command & control (C2) callbacks use any port:

15% C2 bypass web ports 80 & 443[1]

91% C2 initiated by DNS requests[2]

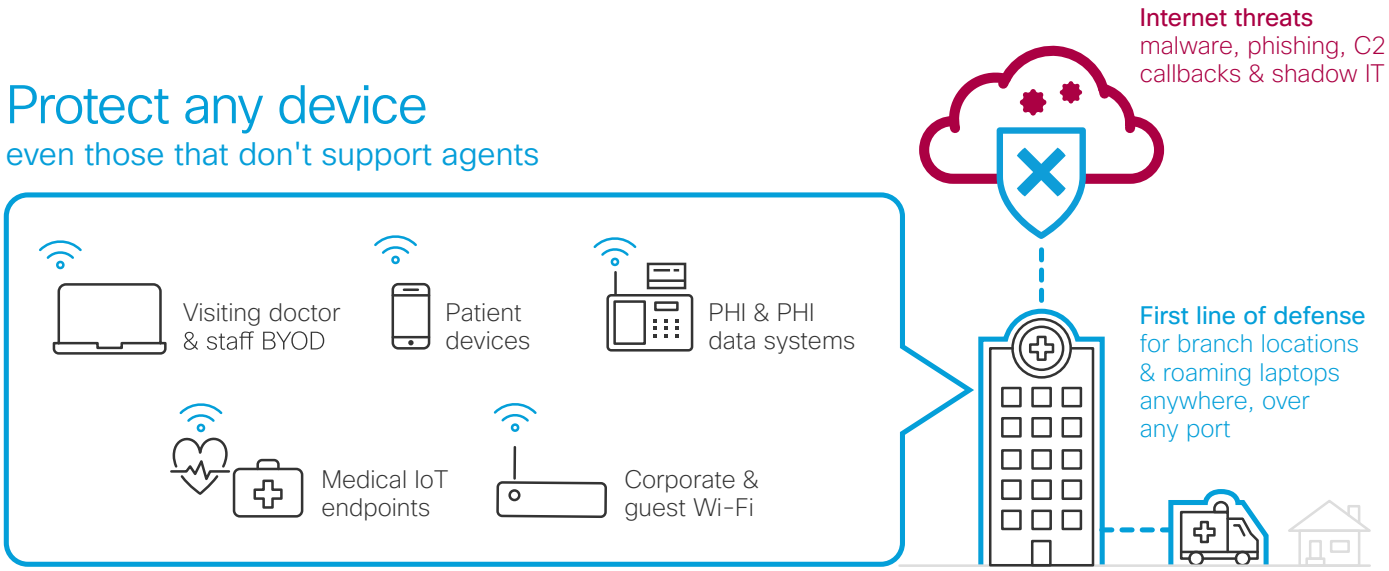
[1] cs.co/lancope-c2-stat, [2] cs.co/dns-c2-stat

The many unique and daunting challenges for healthcare security include:

- The introduction of an avalanche of unmanaged consumer endpoints, such as tablets and smartphones used for clinical purposes by doctors and other practitioners.
- The ever-changing regulatory landscape marked by the Health Insurance Portability and Accountability Act (HIPAA) and a number of other privacy initiatives.
- The dramatic uptick in smart medical devices that are conspicuous elements in the IoT movement in healthcare, creating both new endpoints and a host of new incursion points for threats and bad actors.
- Increased use of Wi-Fi networks in hospitals and other healthcare facilities for use by patients, visitors and contractors, putting new strains on healthcare leaders to protect vital data assets when devices often lack sufficient and updated security.
- The highly collaborative nature of healthcare service delivery, requiring open sharing of data among doctors, nurses and other clinicians for applications ranging from electronic health records to clinical documentation standards such as ICD-10.

Ransomware, in particular, has emerged as a potentially huge problem for healthcare organizations, given the stark reality that healthcare records are the most sought-after and threatened data assets by hackers and cyber attacks. Healthcare industry experts estimate that the value of healthcare records is far greater to hackers than stolen credit cards. Just how much more is a subject of great debate: Global information service Experian says healthcare records are worth 10 times more than credit cards on the black market, while James Scott,

Cover healthcare security gaps



co-founder and senior fellow of the Institute for Critical Infrastructure Technology, said electronic health records are as much as 100 times more valuable.[3]

Ransomware has become so prevalent in healthcare that FBI officials have taken the unusual step of publicly urging organizations to resist the urge to pay ransomware demands, even when the monetary amounts are relatively small.[4]

Fortunately, against this backdrop of increased volume and sophistication of threats, new solutions have emerged to help healthcare organizations devise better defenses against security threats. The increased use of cloud computing for everything from securely storing medical images to utilizing software-as-a-service applications has given healthcare IT executives and their business counterparts a high level of confidence in the utility, cost effectiveness and, in particular, security of using the cloud.

Delivering security from the cloud can relieve the mounting pressures on healthcare organizations to devote enough staff and budget resources for on-premises-managed security. This is particularly important given the increased incidence of zero-day threats that emerge without warning, as well as sophisticated advanced targeted attacks through malware and social engineering.

Using a cloud-delivered security framework can help healthcare organizations stay in front of emerging threats more reliably and efficiently than your overworked in-house staff, which often lacks the necessary expertise.

This is a vital element to the benefit of using a partner with cloud-delivered security because **staffing represents 26% of healthcare IT security budgets, while maintenance costs account for another 23%** – that's essentially half of all healthcare IT security budgets just for staffing and maintenance.[5]

3 "Has Health Care Hacking Become an Epidemic?" PBS, March 2016, http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/

4 "FBI Cyber Division Chief Advises Companies Not to Pay Ransom For Release of Data," The Wall Street Journal, May 2016, http://blogs.wsj.com/cio/2016/05/04/fbi-cyber-division-chief-advises-companies-not-to-pay-ransom-for-release-of-data/

5 "Industry Spotlight: US Healthcare Security Budgets, Priorities, And Challenges," Forrester Research, February 2014, https://www.forrester.com/report/Industry+Spotlight+US+Healthcare+Security+Budgets+Priorities+And+Challenges/-/E-RES109443

Defining the cloud-delivered security solution

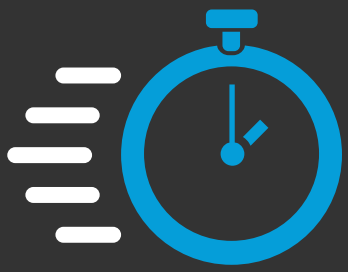
Once you determine that a cloud-delivered security framework meets your organization's needs, the next step is to scope out the key functionality and capabilities you must have. While every organization's needs have at least some level of uniqueness, it is possible – and, in fact, necessary – to create a functionality checklist.

This will help you and/or your colleagues when evaluating solutions options from many different tools suppliers and service providers that are vying for your business. Naturally, each of their solutions proposals will have their own distinct twist, often based more on what they can supply rather than on what you actually need. So, finding a way to equalize each solution in some way so you are comparing apples to apples is essential.

At the end of the day, you'll want a cloud-delivered security solution that has each of the following capabilities:

- **Simple and fast to deploy.** You want to make sure the solution doesn't necessitate the expansion of on-premises infrastructure, or the addition of new software on endpoints, which takes time to implement. You'll also want to avoid the need for expensive technical experts to properly deploy or configure the service.
- **Support for all types of endpoint devices, including IoT.** Ensuring security at traditional nexus points, such as servers and desktops, is far from enough. Your partner must support the full array of endpoint devices, including smart medical devices like blood infusion machines and heart monitors. This is another argument in favor of working with a cloud-based security framework: the cloud's infinite ability for expansion to accommodate more and more unstructured data without adding expensive on-premises storage and software licenses.
- **Avoiding the need to purchase multiple on-premises appliances.** Next-generation firewall, secure web gateway and sandbox appliances have become popular in some healthcare organizations. They're fine – up to a point. As security threats expand, including zero-day attacks and advanced threats, it becomes impractical and expensive to keep adding more and more purpose-built security appliances.
- **Locally sourced, API-based threat intelligence.** Every healthcare organization should be using some form of threat intelligence. But it is essential to use locally sourced threat intelligence, then globally enforce it by using application programming interfaces (APIs), in order to get it into the cloud-delivered security layer.

DNS-layer network security should simply always work



Deploy in minutes

Fewer alerts

Integrate and block quickly

- **Performance and availability.** Of course, everyone wants security defenses that spot and remediate threats as quickly as possible. But you should be pushing for important metrics such as the lowest possible latency, as well as validated 100% uptime.
- **Analytics.** In today's fast-moving, ever-changing environment, you need real-time, deep analytics on network and application behavior, event logging, security information and event management (SIEM) and other predictive analytics to have clear, actionable views on what's happening and possible security anomalies. Hint: Look closely at your supplier's dashboards and visualization tools so your less-technical personnel can understand what's happening too.

Why Cisco Umbrella

One security partner with extensive experience in helping healthcare organizations manage their increasingly complex security requirements with a cloud-based solution is Cisco. The Cisco Umbrella cloud security platform centers on the concept of gaining visibility into where attackers build and stage incursions because of domain name system (DNS) requests resolved by Cisco's Umbrella global network.

Umbrella also provides protected health information (PHI) breach protection and internet-wide visibility both on and off the healthcare organization's backbone network.

This capability is a must-have to address the mounting problem of ransomware, because addressing that challenge through remediation is too late. When threats have already encrypted or exfiltrated health data records, the options are to pay the ransom, restore data from a secure backup or, in some cases, risk release of the patient data. These outcomes can be prevented only by spotting and blocking ransomware threats before infection or encryption takes place.

Umbrella also addresses the bring your own device (BYOD) challenges that are commonplace in healthcare organizations by providing a lightweight endpoint agent for Windows and Mac OSX devices that enforces security at the DNS and IP layers entirely in the cloud. Additionally, organizations can integrate their local threat detection defenses into Umbrella's API-based cloud service; this is typically a turnkey integration done in a matter of minutes.

As more and more practitioners use their own notebooks and tablets as part of their duties, Umbrella helps healthcare organizations mitigate security risks typically associated with roaming workers – without having to resort to expensive on-premises infrastructure expansion.

Another common problem with many security defenses is the proliferation of unwarranted alerts, based on rigid business rules and policy management. Umbrella ensures that a flood of alert noise doesn't hide dangerous alerts from the incident response team add period after team. Plus, Umbrella prevents threats before an IP connection is established or a file is downloaded, resulting in fewer alerts to examine and prioritize.

Conclusion

As healthcare security threats mount, the stakes rise exponentially for IT departments that need to protect information vital to the welfare of their organizations and their patients. With threat vectors expanding and still-unknown threats just around the corner, it is essential to lock down security in the data center, at the endpoints and at every nexus point on the network.

Unfortunately, most healthcare organizations lack the necessary budgets and manpower to adequately guard against this broadening array of threats and bad actors. That's why more healthcare IT and business professionals are finding common ground in turning to the cloud to enhance security today, while ensuring the ability to scale up defenses quickly as new threats emerge.

Cloud-delivered security is a cost-efficient and agile approach to dealing with healthcare security threats, while also improving the organization's ability to meet expanding and evolving compliance mandates. In order to more sufficiently cover potential security gaps, you should look for a solution that blankets the full range of systems and requirements in a typical healthcare organization, such as Wi-Fi access points, practitioners' and patients' mobile devices, PHI systems, smart medical systems and application servers.

Cisco Umbrella is a proven, reputable and innovative cloud security platform that provides the first line of defense against threats on the internet wherever users go. Its global network enforces security at the DNS and IP layers over any port or protocol, and the company's Cisco Umbrella upgrades traditional PHI/personally identifiable information (PII) breach protection.

For more information on how Cisco Umbrella can help your healthcare organization secure data cost efficiently with a simple, open, automated and effective security solution, please go to https://resources.umbrella.com/security-health/