EBOOK

Ransomware:

What every healthcare organization needs to know

Cisco Umbrella

In the healthcare industry, information security is critical. It's also a tremendous challenge, now more than ever before. Changes in government regulations, a massive revolution in medical device and mobile technology, and a transformation in the way care is delivered and consumed have come together to form a perfect storm of complexity and vulnerability.

In this ebook

Medical devices: A new crisis in healthcare security

Monitoring devices, wearables, patient portals, tele-medicine, and mobile health apps are just a few examples of the revolutionary technologies impacting healthcare, all of which introduce a new realm of potentially vulnerable endpoints for cyber attack.

And with onsite Wi-Fi, any staff, patient or guest device connecting to the Internet on the organization's network has the potential to spread infection. Compounded with the high stakes that accompany protected health information (PHI) or Personally identifiable information (PII), the healthcare industry presents a veritable greenfield for cyberattackers.

A 20 percent growth in medical devices is seen each year,[1] for which there are no common security standards. A medical device might seem different from a computer, but anything connected to a network – including fetal monitors, pacemakers, infusion pumps, and ventilators – poses a security risk.

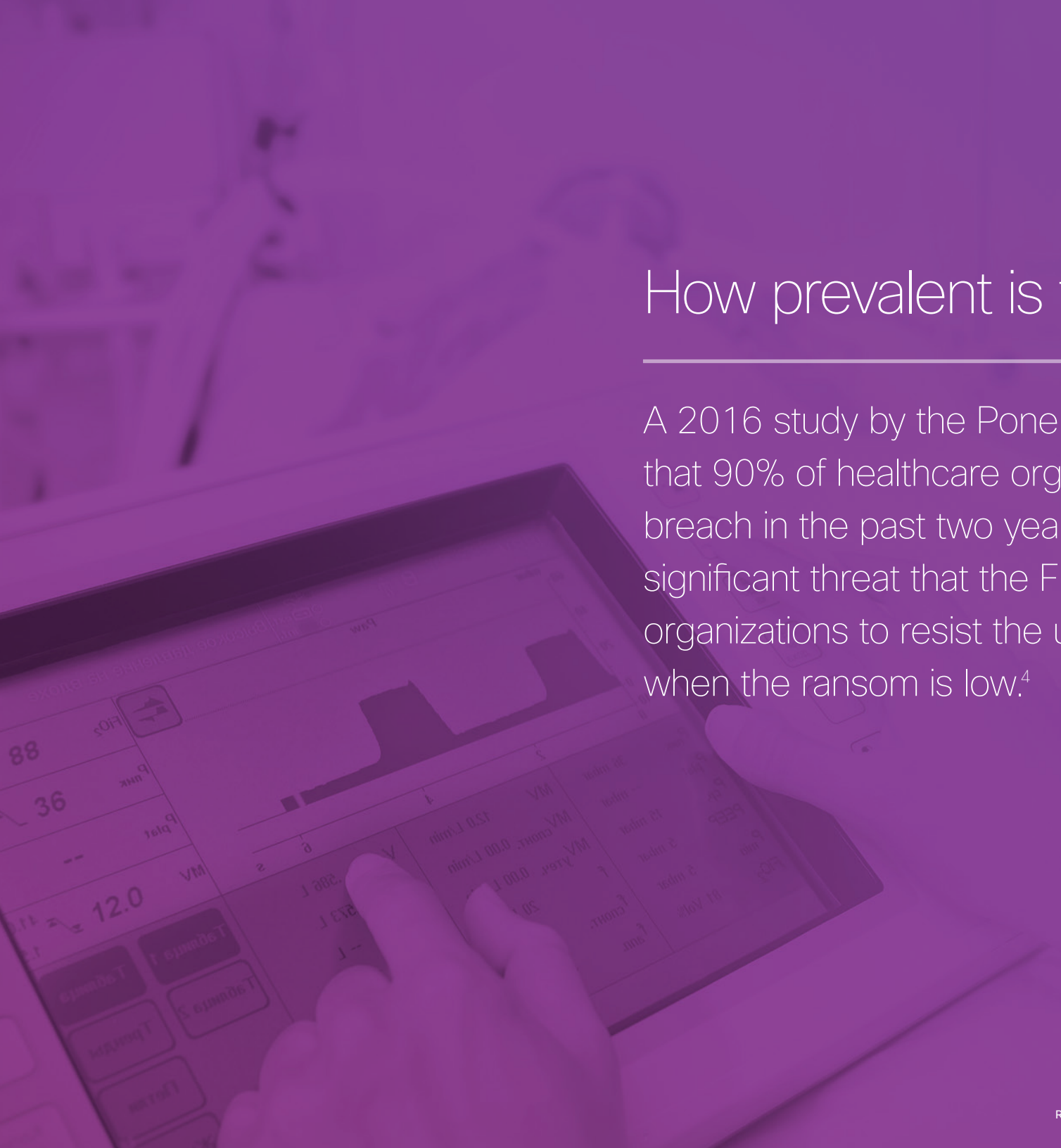
What is ransomware?

Ransomware is covertly installed, malicious software that holds users' files for ransom by encrypting the data and then demanding the user pay a fee in exchange for the encryption key. Hackers using ransomware usually give the victim a limited period to pay the fee; if the victim doesn't pay, the hackers threaten to destroy the encryption key entirely – in which case, unless there are uninfected backups, access to the files will be lost forever.

Ransom is usually paid in the form of bitcoin, a secure, anonymized, and untraceable e-currency, which makes it possible for criminals to get away with extorting payment online. Hackers often intentionally set prices low so that it's more convenient to pay than to seek help.

Beyond locking files at user endpoints and workstations, the software travels across your network and encrypts medical endpoints, equipment, and sensitive data stores like healthcare records.

Most recent ransomware infections of healthcare workstations...could be traced to clinical staff web browsing from a workstation that was missing Flash player patches.[2]



How prevalent is the threat?

A 2016 study by the Ponemon Institute found that 90% of healthcare organizations have had a breach in the past two years[3] and poses such a significant threat that the FBI has publicly urged organizations to resist the urge to pay, even when the ransom is low.[4]

Why is healthcare being targeted?

It's lucrative

Hackers go after personal information, which they can sell and, ransomware can elicit $50 per medical record[5] – 10 times more than credit cards on the black market.[6]

Opportunity abounds

The healthcare industry is massive, and its recent digitization has only expanded the available attack surface. Likewise, when it comes to security, healthcare is one of the biggest laggards.

The stakes are high

The critical care that's provided is often dependent on the availability of electronic medical records (EMRs), PHI or the operation of networked medical devices, which makes healthcare providers more likely to pay up.

A recent Politico report states:

"Healthcare companies should be spending at least 10% of their information technology budgets on security.[7]", however the industry-wide average is only about 3%[8]. With staffing and maintenance of existing on-premises security technology consuming half of most healthcare organizations' security budgets[9], healthcare organizations become a target.

How does infection happen?

Ransomware can infiltrate a computer or device in a number of ways:

Phishing emails
Legitimate-looking emails with malicious attachments or links to compromised websites are sent to employees. When clicked or opened, ransomware downloads and calls out to its command and control server.

Unpatched programs/drive-by downloads
Users with vulnerable programs (an outdated browser, software that's missing a plug-in, or an unpatched third-party app) visit a compromised website, allowing an exploit kit to download and install.

Compromised websites
A user visits a legitimate website whose security has been compromised, hiding malicious scripts. Those scripts redirect the user to an exploit kit, which installs on the user's computer.[10]

Malvertising
Infected banner ads on legitimate sites can initiate an exploit kit that checks for vulnerabilities in the user's system – without even being clicked – allowing malicious scripts to infect their workstation in seconds.[11]

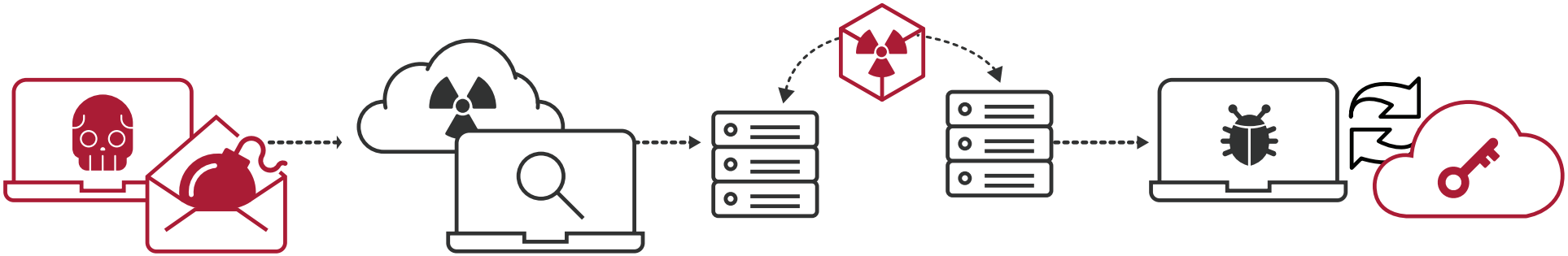
Free software downloads
When a user willingly downloads a file, that file bypasses firewalls and email filters, and goes straight to the user's hard drive.

Regardless of the infection route, almost every type of ransomeware follows a series of steps – often repeated steps – to attack users.

How does a ransomware attack work?

There are two ways that hackers execute ransonware attacks: via email and via the web. In an email attack, the user clicks a link in, or opens an attachment from, a phishing email. In a web attack, the user visits a compromised website or a site displaying malvertising.

From there, the following occurs:



1. Launch

That initial action triggers the download and installation of an exploit kit. On its own, the exploit kit is not harmful to the user's computer. But it opens the door to step 2.

2. Exploit

The exploit kit identifies any vulnerabilities in the user's system and makes a "callback" to the malicious infrastructure to communicate these vulnerabilities.

3. Install

The infrastructure sends a targeted payload (that is, a payload that can exploit the vulnerabilities identified) to the user's computer.

4. Callback

The payload makes another callback to the malicious infrastructure to retrieve a private encryption key. Once the key is received, the data at the endpoint (in this case, the files on the user's computer) is encrypted.

Health check: How can you protect your organization before an attack?

To stop ransomware before it can do damage, prevent attacks before they start: Attackers have to stage servers and register domains before they can send payloads, and they often re-use attack infrastructure. If you can detect that infrastructure, you can block the callbacks – which is exactly what a DNS-based defense does. In that way, it protects your healthcare organization proactively, regardless of how stealthy a cybercriminal's ransomware attack may be.

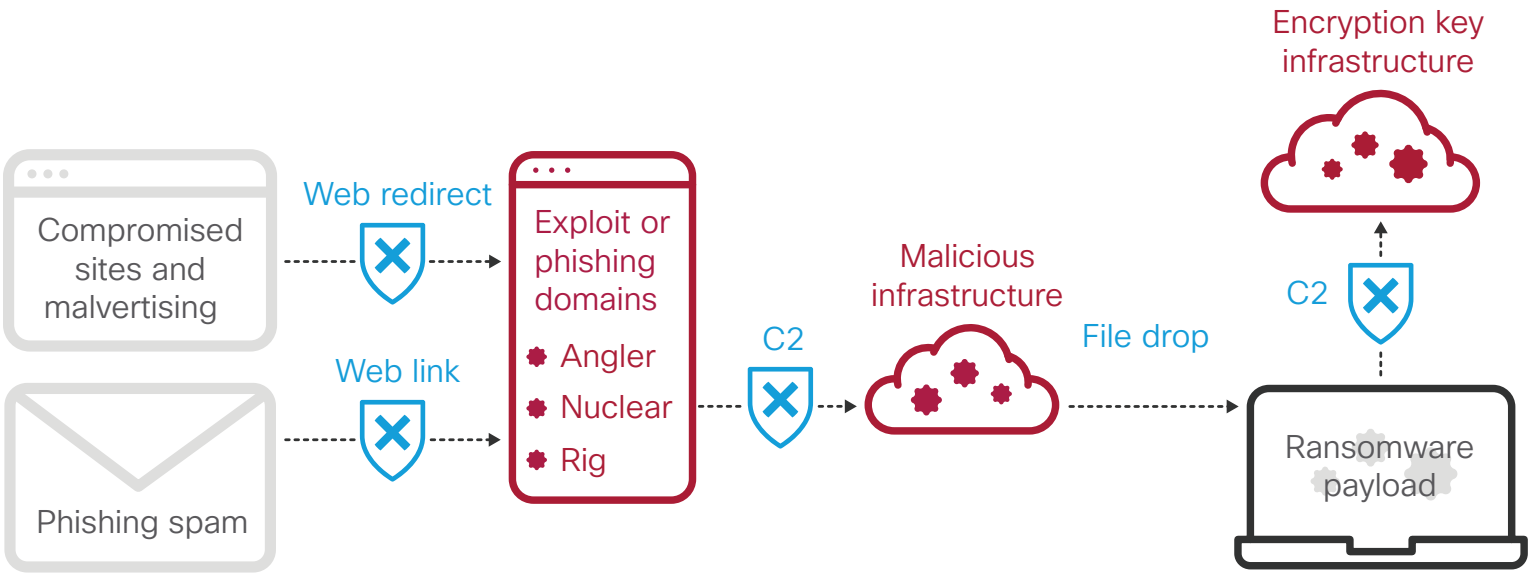
What you should do:	Cisco Umbrella enables you to:
Monitor global cybercriminal activities for insight into where hackers are staging infrastructure for future attacks.	Automatically uncover attacker infrastructure staged for current and emerging threats. Gain visibility needed to protect internet access across all devices on your network, all office locations and roaming users.
Protect patient devices, medical IoT endpoints, PHI and PII Data systems, even those that don't support agents.	Prevent malware from infiltrating all devices on your network icluding: infusion pumps, heart monitors, corporate systems.
Discover and block domains and IPs that are likely malicious.	Proactively block requests to malicious destinations before a connection is even established without adding latency. Stop threats over any port before they reach your network and endpoints.
Feed contextual threat intelligence into your security management or incident response environment to identify which incidents require attention.	Integrate with your existing security stack and local intelligence. Leverage open APIs to programmatically extend protection for devices and locations beyond your perimeter, and enrich your incident response data.
Know how unmanaged mobile and IoT devices connect to your network to prevent exfiltration of patient data.	Provide a layer of PHI/PII breach protection.

Triage: Blocking an attack after a breach

While you can't always block an initial infiltration, in a vast number of cases, you do have the power to prevent ransomware from successfully completing its install cycle.

Where Umbrella can help

1. View real-time security activity to see the relationships between malware, domains, IPs, and networks across the internet.
2. Search up-to-the-minute threat info as well as historical context about all domains on the Internet, and respond quickly to critical incidents via Cisco Umbrella Investigate.
3. Pinpoint devices infected or users targeted by advanced attacks to reduce the time to remediation.



Get well: What to do after you've been attacked

After you've remediated a ransomware attack, it's a good time to take a step back and assess what happened:

- Identify the root cause
- Develop a proactive security plan that leverages a multi-layer defense
- Use predictive intelligence to understand how and where attacks are staged on the internet
- Internally segment networks to contain a breach
- Restore data from backups
- Educate employees about security best practices

Deploy a first line of defense that will stop opportunities for lateral movement of ransomware within your network, eliminate its propagation, and reduce the amount of time any attack has to operate within your network.

By leveraging open APIs Umbrella extends protection to the cloud, enforcing policy or acting on intelligence across endpoints on or off the network before an attack, and enriches incident response data after an attack.

Your first line of defense: The DNS layer

As with healthcare itself, the best medicine is prevention. The most effective anti-ransomware strategy will detect and arrest threats before they breach the perimeter. And, with 91% of malware using DNS to gain command and control, exfiltrate data or redirect web traffic, DNS-layer security is the most effective first line of defense against ransomware.

Simple, open, automated, and effective security

Cisco Umbrella provides PHI breach protection critical to addressing the marked increase of ransomware attacks on healthcare organizations.

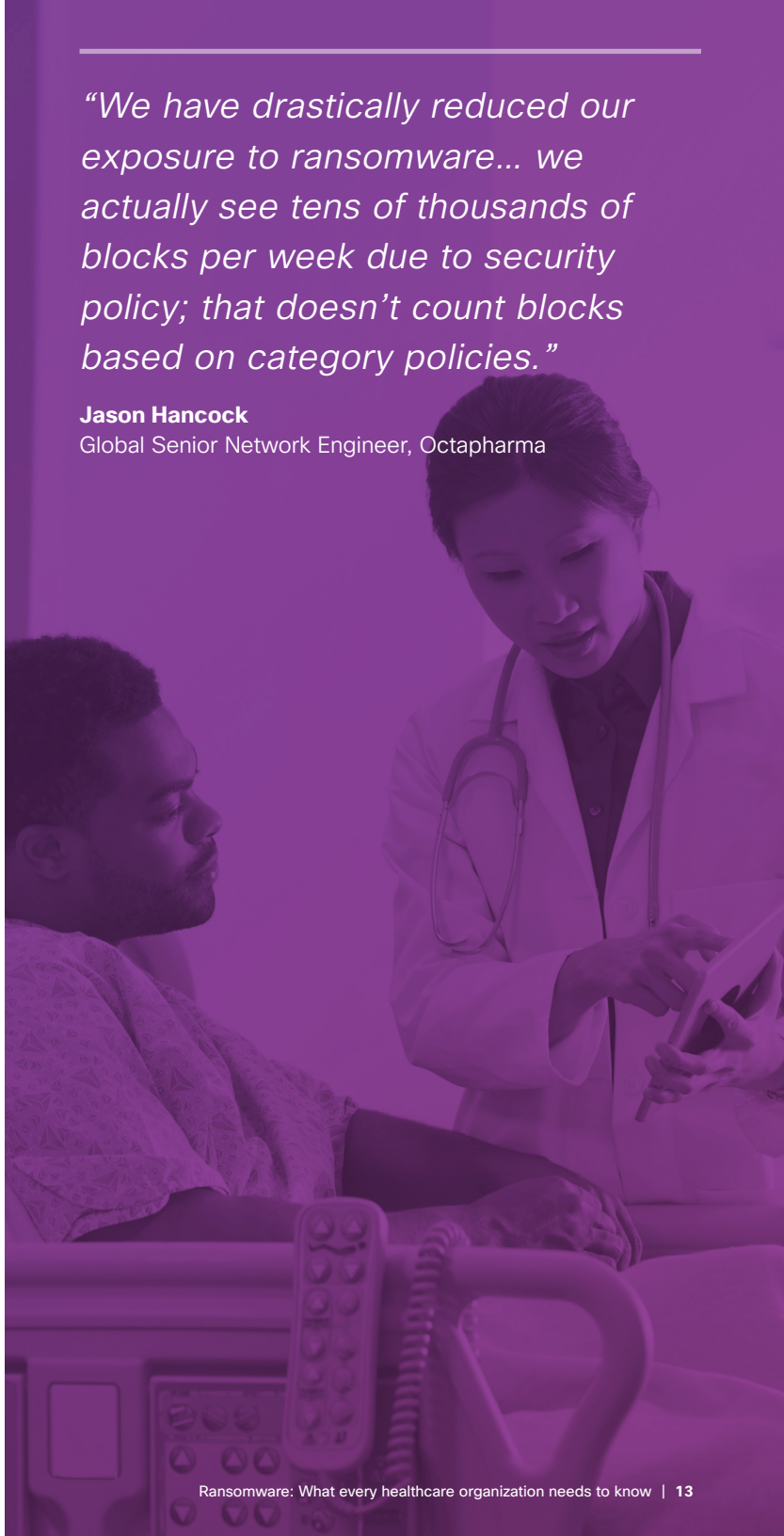
First line of defense against threats
Umbrella is built into the foundation of the internet and blocks requests to malicious destinations before a connection is even established — without adding any latency. Stop threats over any port before they reach your network and endpoints.

Visibility and protection everywhere
Your users and apps have left the perimeter. Umbrella provides the visibility needed to protect internet access across all medical devices on your network, all office locations, and roaming users.

Simple to deploy and easy to manage
Umbrella is simple to deploy — there's no hardware to install and no software to maintain. A cloud-delivered solution with 100% uptime, Umbrella protects users across your organization in just minutes. It's powerful, effective security without the typical operational complexity.

Intelligence to detect attacks before they launch
Umbrella monitors relationships between malware, domains, IPs, and networks across the internet, learning from activity patterns to automatically identify where attacker infrastructure is being staged for future threats.

Integrations to amplify existing investments
Easily integrate Umbrella with your existing security stack and local intelligence. Leveraging open APIs, you can programmatically extend protection for devices and locations beyond your perimeter, and enrich your incident response data.



"We have drastically reduced our exposure to ransomware... we actually see tens of thousands of blocks per week due to security policy; that doesn't count blocks based on category policies."

Jason Hancock
Global Senior Network Engineer, Octapharma

"We actually had a ransomware incident where a device did get infected, but it was easily contained by Umbrella...Deploying Umbrella was fast and we experienced immediate time-to-value."

Henry Duong
Infrastructure Security Manager
The University of Kansas Hospital

Try Cisco Umbrella now. Get started in as little as 30 minutes.

START YOUR FREE TRIAL

cisco Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go.

SC Magazine has recognized Cisco as the Best Security Company for 2016.

Source: 1 http://emergogroup.com/resources/research/outlook-medical-device-industry **2** http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html **3** Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data (May 2016) Ponemon Institute© Research Report **4** http://blogs.wsj.com/cio/2016/05/04/fbi-cyber-division-chief-advises-companies-not-to-pay-ransom-for-release-of-data/ **5** http://www.politico.com/story/2015/06/health-care-spending-billions-to-protect-the-records-it-spent-billions-to-install-118432 **6** http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf **7** http://www.politico.com/story/2015/06/health-care-spending-billions-to-protect-the-records-it-spent-billions-to-install-118432 **8** http://www.healthcareitnews.com/news/cybersecurity-special-report-ransomware-will-get-worse-hackers-targeting-whales-medical-devices. **9** https://www.forrester.com/report/Industry+Spotlight+US+Healthcare+Security+Budgets +Priorities+And+Challenges/-/E-RES109443?objectid=RES109443 **10** http://www.welivesecurity.com/2016/06/28/malicious-scripts-compromised-websites-protect/ **11** https://blog.knowbe4.com/scam-of-the-week-massive-webad-poisoning