WatchGuard®

# THE GAP IN THE GOWN

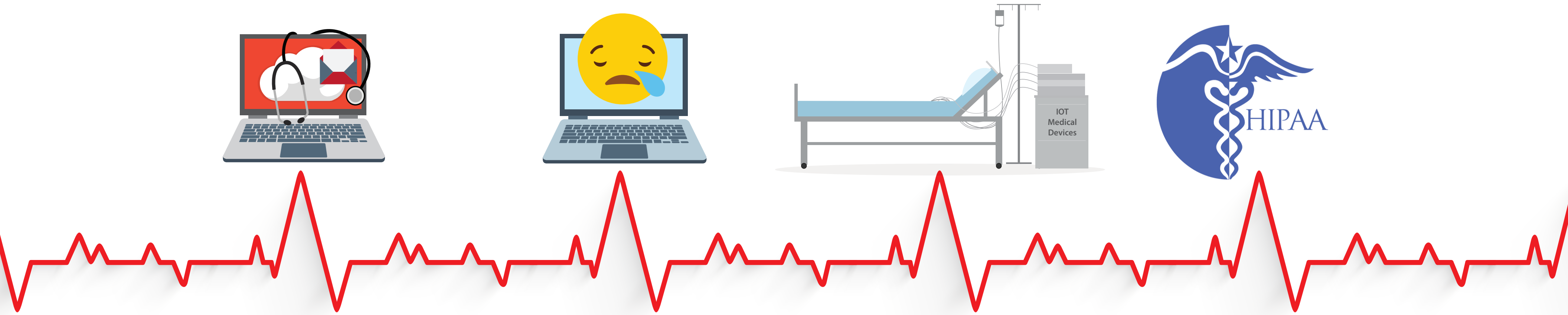
*How not to become over-exposed in healthcare cyber security*

# TABLE OF CONTENTS

# INTRODUCTION

As the healthcare sector continues its shift towards a value-based care model – driving lower costs and higher accountability, while placing patient satisfaction at the forefront – most facilities are looking for the right tools and technology to make it happen. With innovations in care delivery arriving on the market daily and opening the door to better treatment, productivity, and communication within medical facilities, it's difficult to not be hopeful about a bright new future.

But for all the promise, healthcare facilities cannot lose sight of the continuing effort to secure network resources and ensure privacy. Because a dose of cold, hard facts (twice a day – unless otherwise directed by a physician) should be taken with any new technology regimen, this eBook will explore key drivers and advancements in the healthcare sector today, the associated information security risks, and the solutions that support a healthy technology adoption plan.



**Proliferation of Telemedicine and Care Clinics**

**Evolving Threat Landscape**

**Securing the Internet of Medical Things**

**Maintaining Compliance and Accreditation**

# MARKET DRIVERS

## Proliferation of Medical IoT

**IoT business is booming**, and only getting bigger. With the need for more advanced and personalized treatment pushing the market, connected healthcare is forecasted to reach **$117 billion by 2020**.

*ACT, "State of the App Economy, 4th Edition"*

## Evolving Care Delivery

By making it easier to see a physician when the need mandates, without taking time off work or traveling to a clinic, Telemedine is winning over patients. In fact, **83% of patients who have participated in a telehealth visit** felt they'd **received quality care**.

*iSalus Healthcare, "20 Telemedicine Statistics Private Practices Should Know," April 5, 2017*

## Regulatory Compliance

The average number of days between a healthcare breach occurring and the incident being reported to OCR (Office of Civil Rights) was 174 days. It took an average of **123.5 days** for healthcare organizations to discover a breach had even occurred.

*HIPAA Journal, "Summary of January 2017 Healthcare Data Breaches," Released, Feb 14, 2017*

## Ransomware On the Rise

Healthcare data is unique, which makes the privacy and security of it so critical. While credit cards can be canceled if stolen, medical records can be compromised for years. With that said, it's estimated that **ransomware attacks** on **healthcare** organizations will **quadruple by 2020**.

*Cybersecurity Ventures, "Ransomware Damage Report," May 18, 2017*

# CHALLENGE

## Proliferation of Telemedicine and Care Clinics

Too many people and not enough seats, immersed in a cacophony of sneezes, coughs, sniffles, and the unsettling feeling you may walk out with a few more cold germs than you walked in with. The average waiting room experience is not one most patients look forward to – that is, assuming they're able to make an appointment in the first place. With a national doctor shortage fueled by population growth and aging baby boomers, patients are now waiting an average of 24 days[1] for a scheduled appointment with a doctor. The experience can be just as stressful for care providers; with waiting rooms often bursting at the seams, many doctors feel conflicted taking even short breaks between appointments.

Enter telemedicine. Enabling healthcare professionals to evaluate, diagnose, and treat patients at virtually any distance using telecommunications technology, telemedicine drives more flexible office hours, fewer patients in waiting rooms, and less patient non-compliance with treatment plans, as more consistent follow-up is possible through video calls in lieu of clinic visits. Additionally, telemedicine provides a new revenue stream for doctors; in fact, with the addition of five telehealth calls a day, five days a week, a doctor can potentially add $3,500 in monthly revenue.*

However, as with all digital communication, telemedicine carries considerable cyber security and privacy concerns. Medical identity theft has exploded in recent years, and while most practices require patients to have insurance cards and picture IDs on hand, telemedicine patients are remote, making it all too easy to obtain treatment with a stolen identity. Telemedicine also produces a sea of new data that must be accounted for, traveling from the patient's device to the provider, and onward to its final home in the patient's EMR (Electronic Medical Record.) All stages of the data's journey – from transmission to storage – must be done so with data security at the forefront.

With the addition of **five** telehealth calls a day, **five** days a week, a doctor can potentially add **$3,500 in monthly revenue.**

[1] Merritt Hawkins, "2017 Survey of Physician Appointment Wait Times"

# SOLUTION

## For: Proliferation of Telemedicine and Care Clinics

Rx

### Identity Verification

Requiring images of a remote patient's medical ID card and state-issued ID during the medical "visit" goes a long way towards preventing identity theft in telemedicine environments. Likewise, multi-factor authentication and complex passwords help ensure that only authorized users can access healthcare systems to undertake consultations.

### Secure Remote Access

A secure connection between physicians and remote patients is a non-negotiable. WatchGuard's Firebox® UTM solutions feature drag-and-drop VPN creation, securing the path from patient to EMR by encrypting data communications.

### Performance

It would be horrible for the system to go down mid-exam or diagnosis, so in order to maintain telemed operations, firewall appliances must support high speeds, VoIP, and high bandwidth with Quality of Service (QoS) settings and clustering for highest possible uptime.

### Appointment Privacy

Patients should be counseled to attend telemedicine appointments from a private location, if possible, and not to share logins, passwords, or other access information with others.

– WatchGuard

# CHALLENGE

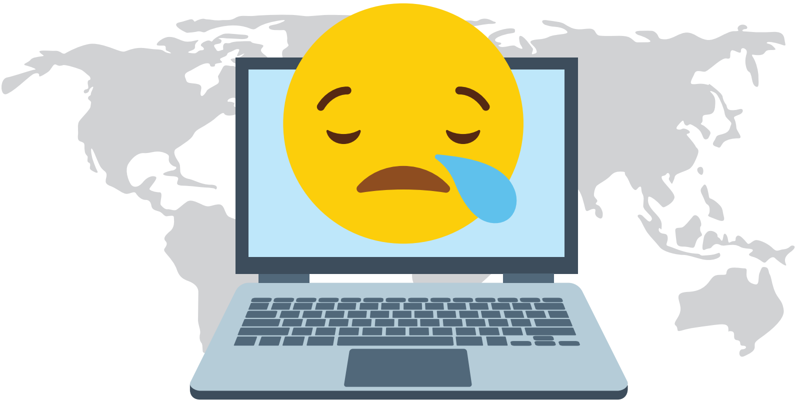
## An Evolving Threat Landscape

With consequences running the gamut from costly inconvenience to catastrophe, ransomware has lurched out of the dark web and onto front page news around the world. First gaining attention around 2005 in Eastern Europe, the malware variant works by infecting a computer, locking users out of the system (usually by encrypting the data on the hard drive), and then holding the decryption or other release key hostage until the victim pays a fee, typically in Bitcoin.

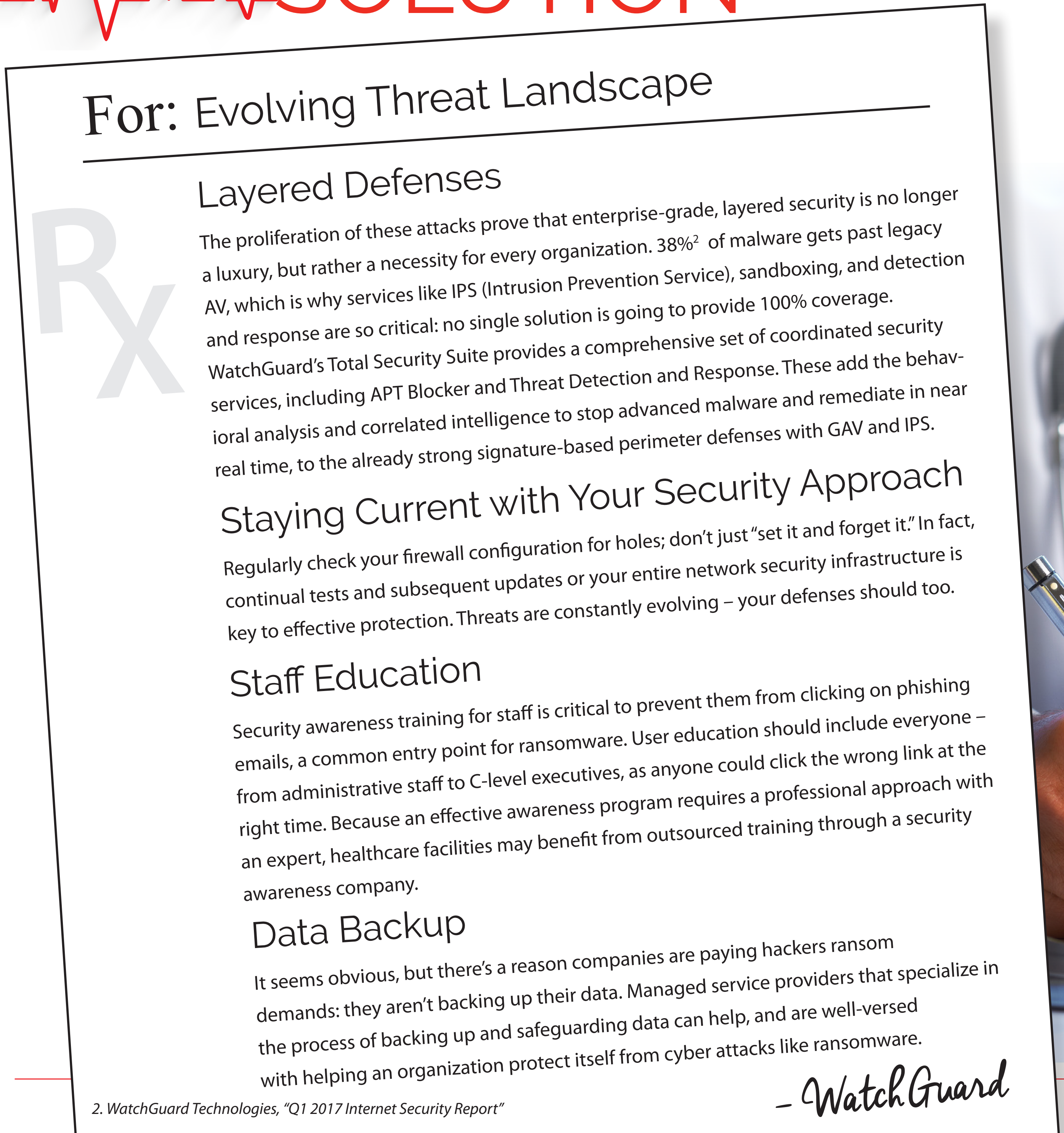
Relying on access to accurate information from EMRs in order to provide critical care, the healthcare industry has emerged as a popular target for ransomware extortion largely because the stakes are so high. With an urgent need to restore service for their patients, hospitals are more likely to pay criminals in order to reinstate critical systems.

When a hacker took control of their network – and refused to release it without payout – Hollywood Presbyterian Medical Center paid no less than $17,000 in Bitcoin in order to resume normal operations. Not far on the heels of that cautionary tale, WannaCry – the now notorious ransomware variant that leveraged a vulnerability found on older versions of Windows OS – left a multitude of infected computers in its wake: around 200,000 across 150 countries. The healthcare sector was hit hard, causing a state of crisis in hospitals and clinics around the globe. National Health Service (NHS) facilities in England experienced computer and phone system disruption, system failures, and ultimately a wave of surgery delays, cancelled appointments, and confusion after hospital computers began displaying a ransom message demanding Bitcoin. One of the industry's largest drug manufacturers, Merck, confirmed they had also fallen prey to the forceful variant, with attacks extending throughout their global offices. Not only can these incidents have horrible short-term impact to patient outcomes, they also affect a facility's ability to compete over the long term if their reputation is tarnished.

**WannaCry** – the ransomware variant that leveraged a vulnerability found on older versions of Windows OS – left a multitude of infected computers in its wake: around **200,000** across **150 countries.**



# SOLUTION



## For: Evolving Threat Landscape

Rx

### Layered Defenses

The proliferation of these attacks prove that enterprise-grade, layered security is no longer a luxury, but rather a necessity for every organization. 38%[2] of malware gets past legacy AV, which is why services like IPS (Intrusion Prevention Service), sandboxing, and detection and response are so critical: no single solution is going to provide 100% coverage. WatchGuard's Total Security Suite provides a comprehensive set of coordinated security services, including APT Blocker and Threat Detection and Response. These add the behavioral analysis and correlated intelligence to stop advanced malware and remediate in near real time, to the already strong signature-based perimeter defenses with GAV and IPS.

### Staying Current with Your Security Approach

Regularly check your firewall configuration for holes; don't just "set it and forget it." In fact, continual tests and subsequent updates or your entire network security infrastructure is key to effective protection. Threats are constantly evolving – your defenses should too.

### Staff Education

Security awareness training for staff is critical to prevent them from clicking on phishing emails, a common entry point for ransomware. User education should include everyone – from administrative staff to C-level executives, as anyone could click the wrong link at the right time. Because an effective awareness program requires a professional approach with an expert, healthcare facilities may benefit from outsourced training through a security awareness company.

### Data Backup

It seems obvious, but there's a reason companies are paying hackers ransom demands: they aren't backing up their data. Managed service providers that specialize in the process of backing up and safeguarding data can help, and are well-versed with helping an organization protect itself from cyber attacks like ransomware.

– WatchGuard

[2] *2. WatchGuard Technologies, "Q1 2017 Internet Security Report"*

# CHALLENGE

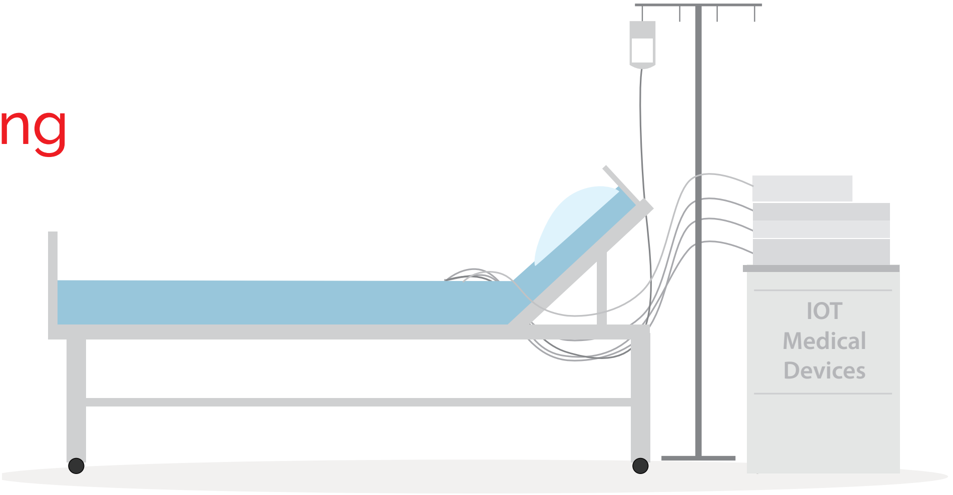
## Securing the Internet of Medical Things (IoMT)

Redefining how we interact, heal, live, and thrive, the Internet of Medical Things is transforming the healthcare sector. Embedded devices – including defibrillators, infusion pumps, pacemakers, and much, much more – now incorporate Wi-Fi, remote monitoring, and near-field communication technologies, and enable health professionals to modify and fine tune implanted devices without intrusive procedures. Another subset of medical IoT – "talking" medical devices – offers audio cues with medication reminders, information about procedures, and more. These types of devices are not only used by patients but also widely employed by hospital staff. There are talking thermometers that read current temperatures with just the click of a button, and even plans for "smart bandages," capable of indicating whether a wound has healed and sending a progress report to the physician.

With patient experience enhanced, healthcare costs reduced significantly, and treatment outcomes improved – the benefits of medical IoT are undeniably exciting. But as hackers take advantage of the typically weak security on embedded devices, defending them – and the people they're connected to – has taken on new urgency, with the innately personal nature of these devices inviting serious consequences.

First and foremost, there's a critical need to protect connected patients, as attackers could potentially hack an ill-secured infusion pump to administer a fatal dose. Vulnerable medical devices also connect to a huge range of sensors and monitors, making them entry points to larger hospital networks and the theft of sensitive electronic medical records, or a devastating ransomware attack that holds critical systems hostage. With most hospitals currently averaging 10-15 connected devices per bed, the exposure to these risks is huge, and only growing.

With most hospitals currently averaging **10-15 connected devices per bed**, the exposure to these risks is huge, and only **growing**.



# SOLUTION

## For: Securing the Internet of Medical Things

### IoT Segmentation

Firewalls do protect IoT devices, preventing hackers, viruses, and worms from reaching your connected devices over the Internet by denying unauthorized traffic. Segment your IoT network for best UTM (Unified Threat Management) service protection – the more you segment your networks, the harder it is for hackers to access all of your devices and information.

### Cloud-Managed Secure Wi-Fi

Both patient and staff IoT devices require access to consistent, reliable Wi-Fi, but it's paramount that access be safe as well. WatchGuard cloud-managed access points have built-in Wireless Intrusion Prevention System (WIPS) to ensure protection, extending and enhancing our security to wireless IoT devices. Leveraging patented Marker Packet technology, WatchGuard provides the most reliable WIPS in the industry, and with the lowest rate of false positives. This solution can run as wireless security only alongside an existing Wi-Fi infrastructure – it doesn't have to be a rip-and-replace.

– WatchGuard

*2. WatchGuard Technologies, "Q1 2017 Internet Security Report"*

# CHALLENGE

## Maintaining Compliance and Accreditation

Mandated by a universal need for safe and quality care, healthcare organizations in every region around the world must adhere to national or local privacy regulations and hospital accreditation programs. Introduced in 1996, HIPAA – the Health Insurance Portability and Accountability Act – set the standard for protecting patient data in the U.S. As part of this legislation, privacy and security rules were established, specifying safeguards that must be implemented to protect the confidentiality and integrity of Protected Health Information (PHI.) Initially, only doctors, hospitals, and insurance companies were required to comply with HIPAA specifications, however a 2013 update increased the scope of HIPAA to address the increased use of outsourcing and cloud providers in healthcare. Any service that transmits, stores, or receives PHI data is now categorized as a "Business Associate" and has to comply with HIPAA – failure to do so ranges in fines from hundreds to upwards of millions of dollars, to say nothing of the costly loss of credibility and potential revocation of medical licenses.

Internationally, JCI (Joint Commission International) is also focused on improving patient safety – through education, advisory services, and accreditation – in more than 100 countries. The accreditation program involves an on-site survey conducted by a commission team at least once every three years, and focuses on the overall quality and safety of a facility's healthcare delivery, including its IT program. Though the organization has no concrete power to enforce its standards, many regions within the U.S., for example, require hospitals to achieve Joint Commission accreditation in order to even be eligible for licensing and Medicare reimbursement.

A 2013 update i**ncreased the scope of HIPAA** to address the i**ncreased use of outsourcing** and **cloud providers** in healthcare.

# SOLUTION

## For: Maintaining Compliance and Accreditation

Rx

### Multi-Factor Authentication (MFA)

Many regulatory bodies are mandating the adoption of stronger authentication measures in healthcare environments. One of HIPAA's technical safeguards, standard 164.312(d), requires organizations to implement procedures to verify that a person or entity seeking access to electronic protected health information is, in fact, a legitimate user. WatchGuard's MFA solution, AuthPoint, can help you to comply with strong multi-factor authentication on an easy-to-manage Cloud platform with a user-friendly mobile app - bringing effective security together with low total cost of ownership.

### Access Controls

Limit access to sensitive network data to only those roles within the organization that require it. WatchGuard Firebox appliances enable you to easily control and audit which personnel can access sensitive network resources.

### Visibility

A granular monitoring and reporting option for your network is key to achieving – and maintaining – compliance. Dimension, a cloud-ready network visibility solution that comes standard with WatchGuard's UTM firewall platform, includes HIPAA report templates that make it easy to prove your compliance status.

– WatchGuard

The potential of emerging technology within the healthcare sector is boundless, transforming care delivery, patient satisfaction, and the very industry itself.  With intuitive solutions from WatchGuard, healthcare quality and equipment can continue to evolve – securely.

**Global Headquarters**
**United States**
Tel: +1.800.734.9905
Email: sales@watchguard.com

**European Headquarters**
**The Netherlands**
Tel: +31(0)70.711.20.85
Email: sales-benelux@watchguard.com

**APAC & SEA Headquarters**
**Singapore**
Tel: +65.6536.7717
Email: inquiry.sea@watchguard.com