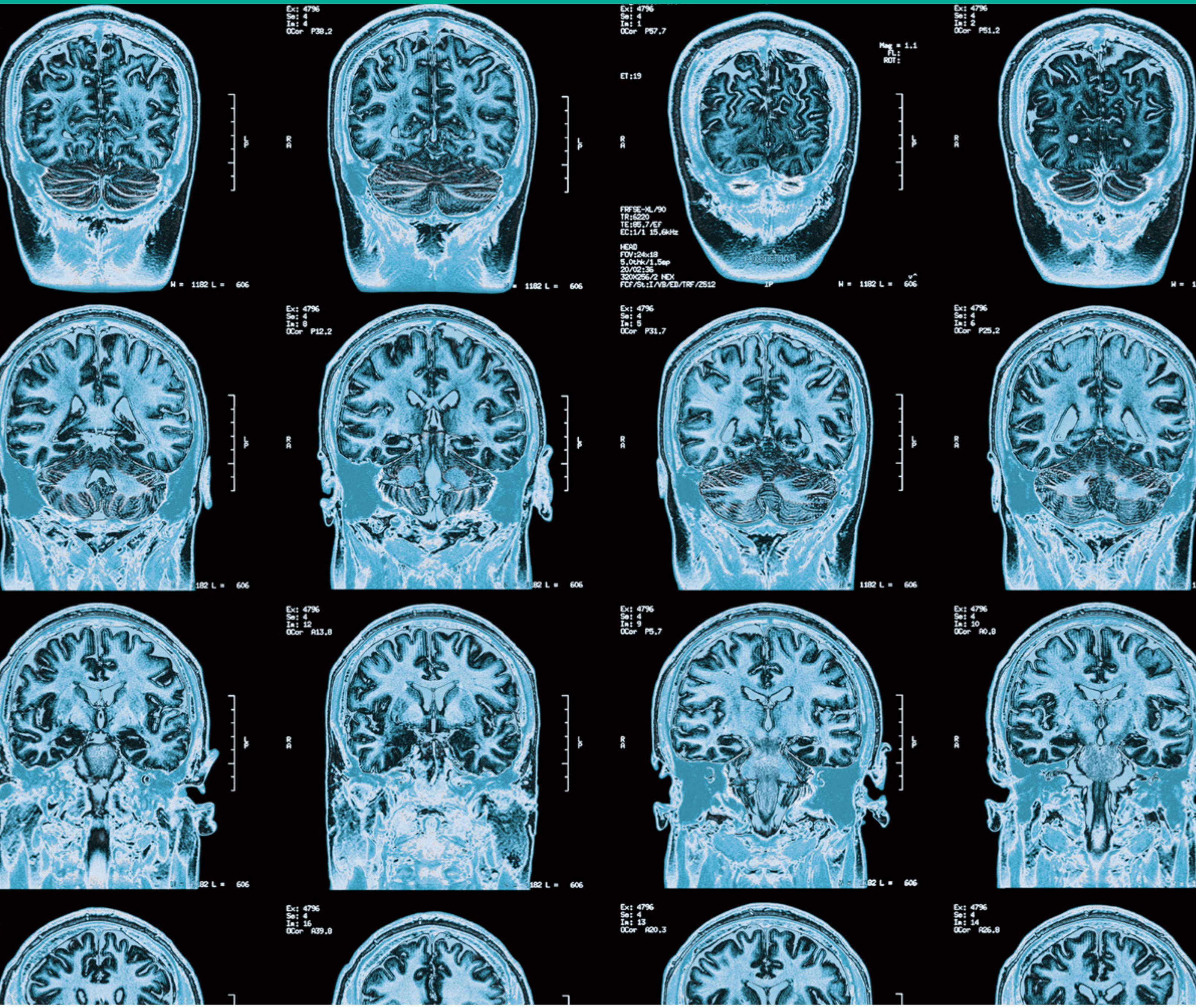
Kaspersky for Business

KASPERSKY lab



HEALTHCARE: IS YOUR MISSION IMMUNE?

True Cybersecurity for first responders

#TRUECYBERSECURITY

HEALTHCARE: MISSION UNBREACHABLE

Almost 90% of healthcare organizations experienced a breach in the past two years. And almost half of those had suffered more than five breaches[1]. Protect sensitive data and systems from accidents and emergencies with Kaspersky Lab's True CyberSecurity. It combines ease of use with Humachine™ intelligence to protect healthcare organizations from the threats they face.

COMPROMISED IMMUNITY

Ransomware attacks on multiple hospitals blocking staff access to vital systems and taking weeks to clear up[2], a cyber attack that wreaked havoc on meal delivery and pathology results[3], an unencrypted drive with almost 30,000 patient records on it goes missing...[4] All in the first three months of 2016.

It's a tough diagnosis to accept, but the FBI's finding that the healthcare industry "Is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures, much less against more advanced persistent threats"[5] is borne out by the evidence, with barely a week in 2016 passing without news of a data breach or cyber attack on a healthcare organization somewhere around the world.

90%

of healthcare organizations experienced a breach in the past two years

30,000

patient records went missing on an unencrypted drive as a result of Ransomware attacks

[1] Ponemon Institute, 6th Annual Benchmark Study on Privacy and Security of Healthcare Data 2016

[2] https://www.scmagazine.com/ransomware-holds-data-hostage-in-two-german-hospitals/article/528823/

[3] http://www.psnews.com.au/qld/490/tech/hack-attack-on-a-hospital-it-system-highlights-the-risk-of-still-running-windows-xp

[4] https://www.scmagazine.com/indiana-university-health-arnett-hospital-loses-usb-drive-with-29k-records/article/529666/

[5] FBI Cyber Division, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain."

MULTIPLE VULNERABILITIES

To be fair, healthcare organizations make very attractive targets for cybercriminals: they gather, share and store large amounts of highly sensitive personal data – from medical information to banking, insurance and other details. They also operate large numbers of internet-connected devices, including highly specialized medical equipment, alongside staff computers and increasing numbers of mobile devices. And that's before we even begin to consider vulnerabilities in medical devices such as heart pacemakers or insulin pumps.

There's a lot of high-tech, smart thinking going on. The problem is that most of the people working in healthcare are – rightly – focused on the patient. They're not cybersecurity experts. And, like most end users, they're vulnerable to the same kinds of attacks cybercriminals use to steal information and inflict operational damage in other industry sectors.

The key difference seems to be one of vulnerability, which is partly self-inflicted: The Healthcare Information and Management Systems Society's (HIMSS) finding that too many healthcare organizations are failing to deploy even the most basic security solutions –such as anti-malware, firewalls or basic encryption tools[6] – is worrying. On a more positive note, it means solutions are readily available for organizations that come to understand that over-reliance on the same limited set of cybersecurity tools yields similar results to over-use of antibiotics: efficacy declines and, ultimately, immunity is compromised.

When patient safety depends on data security, it's vital that healthcare organizations adopt a more agile approach to cybersecurity – one that enables them to use the latest threat intelligence as a security weapon rather than relying on traditional, over-used techniques that cybercriminals have long developed ways to defeat or work around.

Kaspersky Lab's True Cybersecurity approach helps build resistance to the threats every healthcare organization faces. By combining multi-layered security with cloud-assisted threat intelligence and machine learning, it's possible to adopt a more agile, easy-to-manage approach to cybersecurity – without compromising on protection.

PLUGGING THE CYBERSECURITY GAPS

When it comes to cybersecurity, many healthcare organizations aren't managing to plug the gaps in their systems:

86%

have installed anti-malware tools

81%

use firewalls

64%

encrypt data in transit; 59% data at rest

57%

use patching and vulnerability management

52%

have mobile device management in place.

41%

use a web security gateway; 37% messaging security gateway

The Healthcare Information and Management Systems Society[7]

[6, 7] HIMSS cybersecurity Survey 2016

EVERYONE IS WATCHING – BUT ARE YOU LOOKING?

No one is more aware of the healthcare industry's IT vulnerabilities than cybercriminals. In a black market over-running with stolen credit card details and log-ins, medical records – which typically deliver a near-complete picture of the individual they belong to – represent a lucrative payday.
And even if market values drop, there's always ransomware – malware designed to encrypt vital data and hold it 'hostage' until the organization pays up; no buyer more willing than the organization that owns and needs the data.
It's not just the cybercriminals who are watching; wherever they operate in the world, healthcare organizations are subject to regulations governing data protection. From the EU's over-arching General Data Privacy Regulation (GDPR) to America's healthcare-specific Health Insurance Portability and Accountability Act (HIPAA), the goals are pretty much the same: ensuring the protection of sensitive, personally identifiable information.

KEEPING IT REAL

Medical records are lucrative for a key reason: they typically contain data that remains valid for many years. Whether it's date of birth and social security number or insurance and banking data, medical records are something of a one-stop-shop for criminals who want to launch personalised phishing attacks, commit fraud and ID theft or simply sell the data. To get to this information they'll use malware, phishing, malicious web sites and exploit vulnerabilities in hardware and software at healthcare organizations.

Compromised data carries risks that go far beyond financial fraud: it represents a direct threat to patient safety. Who are you treating? Is this the correct medication in the right dose? Whose MRI scans am I reading? Should this patient be given a diabetic meal? When I share this patient's data, is it secure? Who is accessing this data, copying it to external storage, taking it home on their latop? Is the person I'm prescribing this restricted medication to who they say they are? Is this person really a qualified medical practitioner or have they stolen someone's credentials?

In 2015, 112 million medical records were breached in the US alone[8]. There is no way of knowing when – or how – that data will be used. And those are just the attacks we know about; with more than 19,000 hospitals and healthcare facilities worldwide[9] - and the third-party support organizations, insurers, health boards that typically accompany them, there's a lot of ground to cover.

112,000,000

MEDICAL RECORDS BREACHED IN 2015

In this environment protecting the authenticity of data, transactions, access and presence on all systems – and the devices that connect to them – has never been more challenging.

And because these threats are constantly evolving, the cybersecurity approach you adopt needs to be just as agile. A solution built around access to the latest, cloud-assisted threat information can help keep pace with the changing cybercrime techniques. At the same time, machine learning combined with the best of human expertise helps ensure rapid threat prediction, prevention, detection and appropriate response.

[8] Ponemon Institute, *6th Annual Benchmark Study on Privacy and Security of Healthcare Data 2016*
[9] World Health Organization, *Clean Care is Safer Care* program lists 19,002 participating facilities in 177 countries.

INTRODUCING THE TRUE CYBERSECURITY APPROACH

Cyberattacks happen. In a world where you can't block everything, how healthcare organizations respond to attack is as important as prevention and detection.

By taking a proactive approach to cybersecurity, healthcare organizations can ensure that the onslaught of Trojans, ransomware, malware, web and mobile threats they face don't have to become massive data breaches or operational meltdowns.

Where uncontrolled web and device access and the use of unauthorized or insecure USB devices threaten security, it's possible to adopt a proactive, multi-layered approach to cybersecurity, mitigating the risk of error, down time or data loss that can jeopardize patient health, trust and your reputation. And to ensure that cybersecurity doesn't create additional IT management burdens, ease-of-use plays a central role in achieving both agility and effective cybersecurity.

This positive, agile approach is what Kaspersky Lab calls True Cybersecurity. It combines the very best of human expertise with big data threat intelligence and machine learning to provide HuMachine™ intelligence capable of defending against any type of threat your organization faces.

Let's take a look at the key threats to healthcare – and how True Cybersecurity helps treat them:

HACKING, MALWARE ATTACKS, PHISHING

Criminal attacks are the leading cause of data breaches in the healthcare industry, accounting for 50% of attacks.[10]

Throughout 2016, Kaspersky Lab analysts registered a huge amount of spam with malicious attachments and links. That's just one part of the more than 300,000 unique pieces of malware our technologies detected and blocked every day in 2016:

758,044,650

attacks launched from online resources located all over the world

261,774,932

unique malicious URLs detected

69,277,289

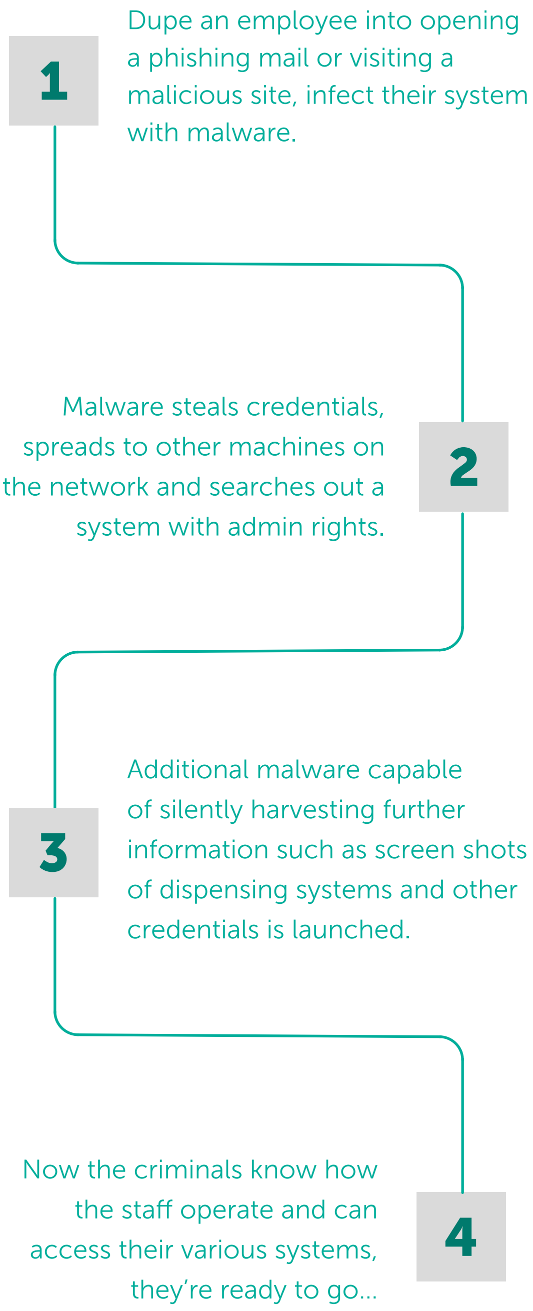
unique malicious objects detected.[11]

Spam and phishing are worthy of particular mention as they represent one of the most prevalent-yet-easy ways for cybercriminals to launch their attacks and gain wider access to systems, steal information or launch ransomware:

[10] *Ponemon Institute, 6th Annual Benchmark Study on Privacy and Security of Healthcare Data 2016*

[11] *Kaspersky Lab: Security Bulletin Statistics 2016*

OUTLINE OF A BREACH



1 Dupe an employee into opening a phishing mail or visiting a malicious site, infect their system with malware.

2 Malware steals credentials, spreads to other machines on the network and searches out a system with admin rights.

3 Additional malware capable of silently harvesting further information such as screen shots of dispensing systems and other credentials is launched.

4 Now the criminals know how the staff operate and can access their various systems, they're ready to go…

Kaspersky Endpoint Security for Business protects users from known, unknown and advanced threats using multi-layered technologies designed to block threats regardless of the route used. It combines the world's most tested, most awarded security with next-generation malware detection and mitigation technologies – all powered by our real-time, cloud-based global threat intelligence network, Kaspersky Security Network (KSN). The big data threat intelligence generated by KSN is further enhanced by machine learning algorithms and 20 years of human expertise – we call it HuMachine™ intelligence – for ultimate protection from any kind of threats.

RANSOMWARE & DISTRIBUTED DENIAL OF SERVICE (DDOS):

Ransomware and DDoS attacks were the top cyberthreat facing healthcare organizations in 2016.[12]

Indeed, ransomware was Kaspersky Lab's "Story of the Year" for 2016. With attacks on businesses of all sizes coming in at a rate of one every 40 seconds, it came as no surprise to Kaspersky Lab analysts that most malicious email attachments contained some kind of Trojan downloader for ransomware or cryptolockers.

Before 2016 was even a couple of months old, healthcare organizations across the world were under siege from crypto-locking malware – and paying a very heavy price, not just in Bitcoin ransom fees but in system failure, inability to access critical patient information and administrative shut-down as clerical staff were forced to return to paper-and-pen and fax machines to get the job done. At another hospital, a ransomware attack crippled the

[12] *Ponemon Institute, 6th Annual Benchmark Study on Privacy and Security of Healthcare Data 2016*
[13] *http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030*

X-ray facilities as the data needed for it to function properly was encrypted – as German media firm Deutsche Welle reported, a hospital spokesman said "We pulled the plug on everything...Computers, servers, even the email server, and we went offline."[13]

DISTRIBUTED DENIAL OF SERVICE (DDOS)

DDoS attacks have a similar operational effect to ransomware. They're designed to overload a network with so much junk packets that the systems crash, wreaking havoc on business continuity and vital service provision. As with ransomware, 2016 saw a marked increase in DDoS attacks – including multiple shatterings of the 'world's biggest DDoS' attack record. The really scary thing about DDoS attacks is that 'cheap and nasty' will do it – for mere dollars, pretty much anyone can 'borrow' time on an attack system, as the world discovered in October 2016 when a single individual ground some of the world's biggest web sites to a halt.

What does this mean for healthcare providers? Electronic healthcare records (EHRs) or any medical services you host in the cloud could be taken offline in seconds. And kept there for days while you either try to stop it or decide to pay the attacker to make it stop.

Kaspersky Lab technologies help mitigate these threats in several key ways:

Kaspersky DDoS Protection can monitor all online traffic and identify the early signs of an attack before diverting your traffic to our safe systems, cleaning it of malicious traffic, and returning it to you. In a True Cybersecurity sense, it's agile and easy to manage, while ensuring the authenticity of vital operational network traffic.

Kaspersky Lab's approach to anti-ransomware, meanwhile, is a multi-layered one that helps protect PCs, servers, mobile devices – and the files on them – from crypto-malware. In addition to our award-winning anti-malware, It includes Anti-phishing and anti-spam technologies to filter out the most popular vector for these attacks. For added security, our Automatic Exploit Prevention (AEP) technology can detect suspicious behaviours indicative of an attack – and stop them before they launch. Automatic rollback can also be triggered to ensure any damage is reversed. This real-time detection-and-response capability is automatic – delivering true agility in the face of some of the most challenging threats facing the healthcare sector.

MOBILE THREATS

Mobile technologies and devices are transforming healthcare. From workstations on wheels (WoWs) to tablets, smartphones and Bring Your Own Device (BYOD) policies, medical practitioners, administrators and even the patients themselves have access to sensitive data at their fingertips. Once data can be accessed from everywhere, security becomes a moving target.

Compromised mobile devices can be used by hackers to access any wider network to which the device connects. Meanwhile, sensitive data stored or accessed via mobile devices is vulnerable to something as low-tech as simple device theft.

Kaspersky Mobile Security and Mobile Device Management help mitigate mobile security and device management risks –even for employee-owned devices – by enforcing anti-malware installation, protecting sensitive data in a separate 'container' and applying anti-theft technologies. All managed from the same, easy-to-use platform as Kaspersky Lab's other security solutions, reducing complexity and driving IT management efficiency.

DATA THEFT OR LOSS

Ponemon research indicates that the average costs of a data breach for a healthcare organization is over $2.2m.[14] Because of their high value in the criminal underworld, medical records and their associated billing and insurance data are the most actively and successfully targeted. It's also the data most likely to be accessed without authorization, lost or stolen.

From stolen laptops to accidental email attachments and lost, unauthorized USB sticks, it seems there are as many ways to compromise healthcare data as there are genuine uses for it. The challenge for IT professionals is how to secure everything without compromising on the need for authorized sharing, storage and communication.

In addition to its leading anti-malware and detection capabilities, Kaspersky Lab's True CyberSecurity approach provides the most comprehensive protection to healthcare data through a combination of integrated technologies, including:

Data encryption prevents unauthorized data access caused by device loss, theft, data-stealing malware or unauthorized data access. Encrypt at file or full disk level and control data transfer to authorized removable media only. Encryption is a cornerstone of data protection best practice and is mandated as such by many state agencies globally.

Security for File Server provides centralized, real-time protection with advanced configuration settings while **Security for Collaboration** ensures that employees can share vital information and services – without sharing malware or other risks.

APPLICATION VULNERABILITIES

For many organizations, the weakest link in the security chain is already sitting on their systems – or sitting in front of them. Un-detected, unpatched application vulnerabilities are a leading threat to data security. From Adobe Flash to Microsoft Office and other widely used applications, vulnerabilities that can be exploited are highly prized by cybercriminals. And too often, we help them by not patching them or allowing end users to ignore update requests.

According to HIMSS[15], many healthcare organizations struggle with patch and

[14] *Ponemon Institute, 6th Annual Benchmark Study on Privacy and Security of Healthcare Data 2016*

vulnerability management – something it says can “lead to a large attack surface.” Known vulnerabilities that remain unpatched present an easy win for cybercriminals. But knowing where to begin, and where to find the vulnerabilities, never mind ensuring they’re patched quickly, is a challenge for many IT departments.

Kaspersky Lab’s powerful vulnerability scanning and patch management simplifies and automates the identification and elimination of application vulnerabilities. Easy inventory and image management combine with constantly updated whitelisting databases to reduce false positives and keep up to date with the latest threats. Because it’s centrally managed from the same integrated console as other Kaspersky Lab solutions, complexity is reduced, making it easier for organizations to integrate this vital process into day-to-day security tasks.

TRUE CYBERSECURITY CAN TRANSFORM HEALTHCARE SECURITY

Those tasked with securing IT in the healthcare industry are walking a difficult line – they have to enable communications and information flows while keeping barriers in place to protect the multiple devices, networks and data streams from data breaches and cyber threats.

The digital healthcare environment has the added risk that comes with non-security trained medical staff accessing and sharing confidential and highly sensitive data. New security vulnerabilities are opening up all over the place and, if left unprotected, will be seized on by cyberattackers.

Kaspersky Lab’s True CyberSecurity approach enables healthcare organizations to deliver on patient safety and privacy without compromising on IT security. By combining cloud-based big data threat information with machine learning and human expertise, it’s possible for us to deliver optimal detection and defence with minimal management challenges. Our multiple layers of security and easy-to-use centralized management mean you don’t have to choose between IT efficiency and effective protection.

DOWNLOAD FREE TRIAL

Kaspersky Lab global Website

Kaspersky Lab B2B Blog

[15] *HIMSS cybersecurity Survey 2016*