Securing the future of healthcare

kaspersky bring on the future

go.kaspersky.com/healthcare

2023

Vaccinating healthcare's post-COVID digital transformation

Given the scale and severity of the COVID-19 pandemic, it's no surprise that the impact on healthcare providers globally has been immense.

Workforce burnout, supply chain disruptions, staff shortages and strikes. Record waiting lists for routine surgery, and record wait times for cases requiring an ambulance. Patients whose chronic illnesses worsened due to lack of treatment as the pandemic raged, resulting in even greater pressure on resources that had already been stretched to the limit.

All these issues made headlines around the world — symptoms of a healthcare sector which itself seems in desperate need of treatment.

But there's another side to the post-COVID coin, with analysts such as **Forrester** suggesting 'The COVID-19 pandemic accelerated healthcare transformation by a decade...' and 'To thrive in this dynamic market, healthcare organizations must invest in transformation and workforce talent or risk their market foothold.' Or **Deloitte**, who noted that 'The COVID-19 pandemic permanently changed global health care — from accelerating the adoption of new technology and care delivery models to increasing the focus on sustainability and resiliency.'

Against this background, another pandemic shows no signs of abating. **HIPPA Journal** reported that in the US alone in 2022, 290 hospitals were potentially affected by **ransomware attacks**, and there were 707 healthcare industry **data breaches** of 500 or more records — with almost 52 million records being stolen as a result of cybercrime.

According to the non-profit **Center for Internet Security**, 'The healthcare industry is plagued by a myriad of cybersecurity-related issues. These issues range from malware that compromises the integrity of systems and privacy of patients to distributed denial of service (DDoS) attacks that disrupt facilities' ability to provide patient care.'

In this whitepaper we'll therefore examine both the impact of cybercrime on the global healthcare sector, and, more importantly, how providers can embrace and fully exploit the opportunities presented by digital transformation — by understanding and minimizing the risks, and implementing the latest technologies securely.

For the **12th year in a row,** healthcare had the highest average data breach cost of any industry

$ 10.1 million

Average cost of a healthcare sector data breach

42%

Increase of a breach cost in the healthcare industry since 2020

IBM Cost of a data breach report 2022

Rethinking risk: resetting strategies and raising the bar

Healthcare is a major target for cybercrime, according to **PwC analysis**. With healthcare's shift toward digitization and customer centricity, business and operations risks are also evolving, requiring rethinking of risk management and controls. The past year was struck by cyber breaches, and all indications point to 2023 keeping pace, if not being even more challenging in the face of global events.

Cyberattacks may bring delayed patient care, loss of privacy or even more severe brand and economic consequences. As organizations look to transform their operations to evolve the customer experience, reduce costs and improve efficiency, they need to be vigilant in anticipating, understanding and controlling their risks in compliance, operations, finance and technology.

Key healthcare trends and how to manage them securely

Leading commentators such as Forrester, Deloitte and PwC have highlighted what they see as the key trends affecting healthcare providers in 2023 and beyond.

In their 2023 Global Health Care Outlook, for example, Deloitte looked at five key areas that are critical to the transformation of healthcare over the next decade, including virtual health delivery, digital transformation, increased focus on health equity and sustainability, and building a more sustainable workforce.

Similarly, in the report Next in health services 2023, PwC highlighted six pivotal issues for the industry, including confronting affordability and disrupting costs, digitizing healthcare, attracting and retaining customers, rethinking risk, solving clinical workforce shortages and delivering deals value.

Philips, meanwhile, outlined 10 healthcare technology trends for 2023. These include addressing workforce shortages with workflow automation and AI, digital upskilling through continuous training and education, enabling remote operations through virtual collaboration, vendor-neutral and interoperable informatics solutions, healthcare's continuing move to the cloud, seamless patient monitoring within and beyond hospital walls, and initiatives related to equitable and inclusive healthcare delivery, climate action, decarbonization, and understanding how environmental health impacts human health.

Based on a combination of these analyses and our own experiences in working with healthcare providers around the world, there are five interrelated trends we believe organizations need to deal with securely if they are to avoid the kinds of cyberattacks mentioned above, and benefit from the many improvements in health outcomes enabled by digital transformation.

These include:

- Virtual care and remote / telemedicine
- Data security and cloud adoption
- AI and the Internet of Things (IoT)
- The relentless challenge of ransomware
- The role of human actors

We'll now look at each of these trends in detail — including the potential security risks and how these can be managed more effectively.

60% of executives

PWC PULSE SURVEY, JANUARY 2022

say digital transformation is their most critical growth driver

In the US alone, there were 11 reported healthcare data breaches of more than 1 million records in 2022 and a further 14 data breaches of over 500,000 records.

The majority of those breaches were hacking incidents, many of which involved ransomware or attempted extortion.

Trend #1: Virtual care and remote / telemedicine

$ 175.2 billion

↗26.7% CAGR

projected global Remote Patient Monitoring (RPM) market size **by 2027**

Devices like weight scales, pulse oximeters, blood glucose meters, blood pressure monitors, heart monitors and wearables will improve clinical prognosis and remove socioeconomic hurdles due to social determinants of health.

In many advanced economies, the shift from face-to-face appointments to consultations by phone or video resulting from COVID-19 has been dramatic. When the pandemic struck, the last thing overworked doctors and nurses wanted was direct contact with patients potentially infected with the virus, while the last thing those patients wanted was to spend time in busy waiting rooms for exactly the same reason.

As a result of the pandemic, telehealth has gone from an underused resource to the preferred way for many patients to receive care almost overnight. The convenience and comfort delivered by telehealth for the management of nonurgent routine care for mental health, chronic disease or pain, for example, has made it a far better option than reverting to appointments that are always face-to-face.

As **Deloitte** has noted, 'While COVID-19 demonstrated new ways that remote interactions can improve patient care and lower costs for providers, it has also raised new concerns about sustainability of current health care models. Virtual health delivery is not a substitute for traditional care, instead it offers new ways of care delivery that were not possible in the past. It has the potential to inform, personalize, accelerate, and augment people's ability to care for one another. The time has come to embrace emerging technologies and design health care delivery for the future. With over one billion people worldwide without any form of medical care and almost a billion people who have no access to modern medicines, virtual health will present an opportunity to change lives and make a difference.'

How to manage virtual care and remote / telemedicine securely

In certain respects, the challenges involved in securing virtual care and remote medicine are similar to those resulting from the explosion in remote working.

For patients of doctor's surgeries, for example, clogged phone lines and the difficulty of speaking to overworked receptionists mean it can be easier to arrange appointments or order repeat prescriptions via text, email or the surgery's web portal — all of which need to be effectively protected.

Also, following a remote consultation, patients may be required to upload photos, videos or other information directly to their medical records — necessitating a level of cybersecurity very similar to that of remote workers being granted endpoint access to corporate systems.

Unfortunately, threats targeting endpoints are becoming increasingly 'evasive'. Specifically designed to bypass existing endpoint protection, these threats are hard to detect thanks to the range of evasion techniques being adopted — particularly the use of legitimate and system-native tools.

By staying undetected for longer, evasive threats also have the time to explore and entrench themselves into an organization's infrastructure and cause the greatest amount of damage — be it a data breach, ransomware attack, directly overriding operations etc.

As a result, effective protection that enables patients to interact with their care providers securely via their preferred devices, how and when they need to, is an absolute priority for virtual care and telemedicine. And that's in addition to the diverse challenges involved in securing all the different kinds of devices used in remote patient monitoring (RPM) — as discussed in Trend #3.

In the absence of centralized quality control of telehealth at the application level, their security can significantly vary from product to product. Another unfortunate fact is that smaller companies, like start-ups, simply do not have enough hands and resources to control the quality and safety of their applications. Accordingly, such applications may contain many vulnerabilities currently unknown to the public that cybercriminals can find and use.

Trend #2: Data security and cloud adoption

Like many aspects of digital transformation, unrelenting increases in both the quality and quantity of patient data held by healthcare providers has both upsides and downsides.

On the plus side, every piece of data collected about citizens' health — from their discussions with local health professionals to the data recorded by their online searches, mobile phones, fitness trackers and other wearables — helps give healthcare providers a clearer understanding of how and where treatments and interventions may be needed.

On the minus side, citizens can be extremely sensitive about the privacy of their personal data — especially electronic health records (EHRs). In the UK, for example, a plan to make general practitioners' health data for everyone in England available to researchers and companies for healthcare research and planning had to be abandoned following a **huge public outcry**, during which more than a million people opted out of National Health Service (NHS) data-sharing in just one month.

This puts healthcare providers in a difficult position. Delivering a seamless healthcare experience often requires collaboration between different providers, who therefore need to share sensitive patient data while working within the boundaries of government regulation. But to continue to drive healthcare innovation such as that envisaged by the NHS data-sharing initiative, they need to be able to reassure citizens that their data is safe and secure, and that the information they're being asked to provide is justified by the quality, capabilities and personalization of the healthcare services being offered to them.

One way that providers are looking to achieve this is through increased cloud adoption. As **PwC** has noted, 'Technology and cloud infrastructure allow stakeholders to exchange, store and integrate data and enable interoperability. It's also the foundation of a vastly improved and more seamless experience for every stakeholder in healthcare — consumer, member, clinician, employer and even regulator. The largest health plans are setting the stage with technology-enabled budgets of $1 billion or more, and leading health systems are embracing the cloud.'

Why is medical data so attractive to cybercriminals?

- Its richness and sensitivity make it extremely valuable.
- It needs to be open and shareable — including being accessed remotely, opening new doors to attack.
- Due to budget restrictions, many healthcare providers operate outdated technology which they lack the specialist IT resources to properly defend.
- The limited security of medical devices makes them relatively easy entry points for cybercriminals.
- Many healthcare staff aren't educated in how to recognize and deal with the most basic cyberthreats.

The cloud is a critical technological enabler for creating truly connected and integrated IT infrastructures in healthcare. Such infrastructures need to be highly secure and highly scalable, allowing healthcare providers to rapidly adapt to fluctuating demand without having to worry about data security.

Cloud adoption in healthcare has traditionally lagged behind.

However, in recent years we have seen fast-growing acceptance and adoption in many parts of the world — a trend we expect to continue in 2023. In tandem, we will see a further proliferation of software-as-a-service (SaaS) solutions delivered through the cloud.

Philips: 10 healthcare technology trends for 2023

How to manage data and cloud adoption securely

Unfortunately for healthcare providers, the financial value of patient records has turned many hospitals and clinics into the equivalent of a poorly protected bank in a Wild West movie. But whereas in the movies, outlaws ran the risk of losing their lives to an unexpectedly well-armed sheriff, now all cybercriminals have to do is buy a cheap ransomware kit on the dark web, or, for a more sophisticated attack, purchase ransomware-as-a-service including a technical support hotline, advice on which organizations and/or individuals to target and how, and specialist expertise to help negotiate, secure and launder the ransom.

Breaches can also result from everything from unpatched legacy systems to human error or deliberate fraud. But whatever the cause, breaches threaten patient confidentiality and can damage an organization's reputation.

Endpoints — including servers, workstations and mobile devices — are the source of the majority of cybersecurity problems encountered by organizations. As a result, high quality endpoint protection has to be the first line of defense against attempted security breaches. And those planning to or already moving medical data to public, private or hybrid cloud environments need to invest in specialist cybersecurity specifically designed to secure these workloads.

45% of breaches
occur in the cloud

Recommended means of preventing healthcare data breaches also include

- Strong email security to prevent phishing and business email compromise (BEC) attacks.
- Strong web security to prevent issues related to phishing and malicious websites.
- Security awareness training to help staff become a healthcare provider's first line of defense.
- Implementing a zero-trust network architecture to help reduce risks related to supply chain attacks.

Average data breach costs comparison

$ 5.02 million	$ 4.24 million	$ 3.80 million
Private cloud model organizations	Public cloud model organizations	Hybrid cloud model organizations

IBM Cost of a data breach report 2022

Trend #3: AI and the Internet of Things (IoT)

Citizens and patients may not necessarily be aware of it, but artificial intelligence (AI) and the Internet of Things (IoT) are transforming healthcare by performing the same tasks humans do, but more efficiently, more quickly and at a lower cost.

As noted by **Deloitte**, 'As more digital health technology is incorporated into clinical processes through cloud computing, machine learning, and internet-connected devices, it can significantly reduce care costs. In addition, technology offers a solution to the shortage of critical care physicians.' And, 'Emerging technologies such as AI, telehealth, blockchain, and monitoring devices, such as sensors, wearables and ingestibles, are providing real-time and continuous data about our health and our environment. This is redefining the future of health care and health delivery.'

PwC echoes these thoughts, suggesting that 'The industry will find value in data-sharing partnerships that take advantage of a surge of medical information from wearable sensors and other health-monitoring devices. Many will boost investments in digital tools to be more effective and nimble'. And, 'AI will be transformational. Tech-led partnerships will serve as sources of innovation and collaboration, enabling better clinician staffing as well as diagnosing and treating patients using at-home blood tests, telepathology, medical imaging, data repositories and more.'

Each of these advances, however, brings further concerns around data security. The sheer number of connected devices already creates huge administrative headaches for healthcare providers. It's been estimated, for example, that a large hospital can have around **85,000 medical devices** connected to its network, including MRIs, computed tomography, ultrasound, nuclear medicine and endoscopy systems, as well as systems communicating with clinical laboratory analyzers such as laboratory information systems.

But if the volume of data currently produced by medical devices has felt like a flood, the IoT is destined to unleash a tsunami of new big data — opening up previously unthought-of applications for AI, but also a new level of complexity in processing, managing and securing this ever-more sensitive data.

Lack of oversight of cybersecurity of networked medical devices in hospitals

Cybersecurity controls are required to protect medical devices that are connected to the internet, other medical devices, or internal hospital networks. Without those controls, the devices could be accessed by unauthorized individuals and patients could be at risk of harm.

If cybersecurity controls are lacking, devices could be vulnerable to an attack that could potentially impact critical healthcare systems. While there have not been any known cases of cyberattacks being conducted specifically to cause patients harm, patients may inadvertently be harmed as a result of an attack conducted for other reasons.

In tandem with this, the poor security of the majority of IoT devices creates its own threats. Who, for example, would want to use an automated insulin delivery system if there was even the remotest possibility it could be hacked?

How to manage medical devices and IoT securely

Connected medical devices are an integral part of modern healthcare and patient care, but the security risks associated with them can be difficult to understand and mitigate. Clinics providing staff with mobile devices to facilitate their work can also face serious issues due to lack of centralized security management.

Medical devices face the risks of being a part of the corporate network, as well as those unique to the embedded systems on which they're based. Traditional antivirus solutions, however, cannot fully defend against the latest advanced, targeted and malware threats to embedded systems, including medical equipment. Embedded systems in medical devices therefore need more than antivirus — requiring cybersecurity based on a combination of Default Deny with Device Control.

IoT devices, meanwhile, require the implementation of specialist security across the IoT ecosystem — minimizing risk and addressing cybersecurity threats to IoT systems and embedded devices through tools securing every software and hardware component of these interconnected systems — without overloading individual systems or devices or limiting overall flexibility.

Trend #4: The relentless challenge of ransomware

Cyberattacks on healthcare providers often cause IT system outages, which in many cases have lasted several weeks causing considerable disruption to patient care. While there have not been any known cases of cyberattacks directly causing fatalities, the lack of access to patient data causes diagnosis and treatment delays that affect patient outcomes. Multiple studies have identified an increase in mortality rates at hospitals following ransomware attacks and other major cyber incidents.

It's impossible to overstate the scale of the disruption and other unique challenges posed to healthcare providers by ransomware.

As reported by **HIPAA Journal**, healthcare ransomware attacks can cripple IT systems, prevent patient medical records from being accessed, cause disruption to patient care, and put patient safety at risk. Recovering data and restoring systems can take weeks or months, and mitigating the attacks is expensive, with considerable loss of revenue due to downtime.

One of the most notorious cybercriminal gangs in recent years targeting healthcare and public health providers in particular has been the Hive ransomware-as-a-service (RaaS) group — in relation to which the US Cybersecurity and Infrastructure Security Agency (CISA) released **an advisory alert** in November 2022. According to FBI information, Hive ransomware actors had victimized over 1,300 companies worldwide, receiving approximately $100 million in ransom payments.

As an example, in September 2021, Hive was responsible for attacks on four US healthcare facilities. One of these, a medical center in Missouri, had patient information stolen from its servers, which was subsequently posted online including names, medical information and Social Security numbers. Hive was also responsible for a ransomware attack against Memorial Health, forcing staff to work from paper charts, and resulting in emergency room diversions and appointment cancellations.

In January 2023, the **FBI** announced that it had disrupted Hive's activities, shielded more than 300 victims and prevented attacks valued at $130 million. But given the value of healthcare data, and that any information stolen is highly sensitive and confidential, making healthcare providers more likely to pay a ransom, there are plenty more threat actors waiting to take their place.

41%

Growth of the share of breaches caused by ransomware in the last year

49 days

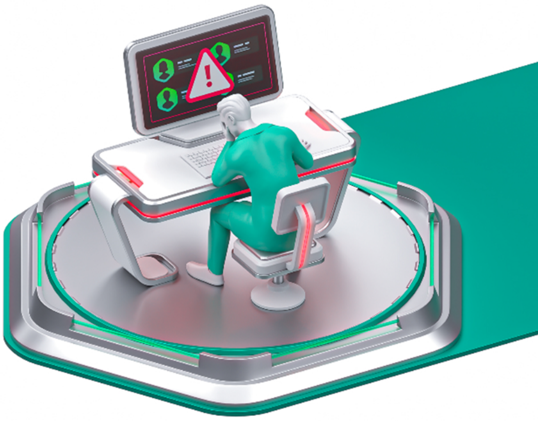
longer than average to identify and contain

$ 4.54 million

Average cost of a ransomware attack

IBM Cost of a data breach report 2022

How to defend against ransomware securely



Ransomware has no place in society, let alone healthcare, which is why initiatives such as No More Ransom have been established with the aim of eradicating it.

Ideally, organizations should implement endpoint security with the proven ability to detect and prevent a high proportion of ransomware — or even 100%. Advice from No More Ransom on how to avoid becoming a victim of ransomware also includes:

- Keeping corporate devices' operating systems and applications updated
- Reducing the likelihood of malicious content reaching your networks
- Using enhanced passwords and changing them on a regular basis
- Being wary of accessing company data through public Wi-Fi networks
- Providing your staff with cybersecurity education and awareness training
- Turning on local firewalls and disabling Windows PowerShell
- Knowing your assets and compartmentalizing them
- Securing access to Remote Desktop Protocols (RDPs)
- Regularly testing your systems
- Managing the use of privileged accounts
- Securing your teleworking equipment
- Installing apps from trusted sources only
- Monitoring data exfiltration
- Using strong authentication

Trend #5: The role of human actors

As if the external threats to healthcare providers weren't challenging enough, the sector also struggles with insider threats.

The HHS Health Sector Cybersecurity Coordination Center (HC3) characterizes an **insider threat** as 'potentially a person within a healthcare organization, or a contractor, who has access to assets or inside information concerning the organization's security practices, data, and computer systems, [who] could use this information in a way that negatively impacts the organization.'

This could include careless or negligent workers, malicious insiders, inside agents, disgruntled employees or third parties.

In its 2018 Data Breach Investigations Report, Verizon found that healthcare was the only industry to have more internal actors behind breaches (56%) than external. And even though its **2022 report** (which analyzed 23,896 security incidents, 849 of which occurred in the healthcare sector, compared to 655 in the previous year) found that external threats accounted for 61% of observed threat actors in healthcare, Verizon said this did not mean insider threats were no longer prominent in the sector.

'While the make-up of the insider breach has moved from being largely malicious misuse incidents to the more benign (but no less reportable) Miscellaneous Errors, we have always been able to rely on this industry to tell the insider threat story,' the report noted.

In healthcare, security efforts often focus on the network perimeter and implementing measures to block external threats, but insider threats can be just as damaging if not more so. Insiders can steal sensitive information for financial gain, take information to provide to their next employer, or abuse their privileged access to cause significant harm.

And, whether they're malicious or accidental, insider breaches can have major consequences for organizations, including reputational damage, loss of revenue, the theft of intellectual property, reduced market share and even physical harm.

Following a four-year decline, insider data breaches in healthcare **surged in 2020**.

> 8.5 million records

were exposed or compromised in those incidents — more than double the number of breached records by insiders as 2019.

In fact, more records were breached by insiders in 2020 than in 2017, 2018 and 2019 combined. In 2020, 1 in 5 data breaches was an insider incident.

The Ponemon Institute's 2020 Cost of Insider Threats Report found that while malicious insiders accounted for 23% of insider threat incidents, negligent insiders were the root cause of 63%.

How to manage insider threats securely

The US Cybersecurity and Infrastructure Security Agency suggests organizations build a comprehensive **insider threat mitigation program** to tackle insider risks.

As it notes, 'Successful insider threat mitigation programs employ practices and systems that limit or monitor access across organizational functions. Insider threat mitigation programs need to be able to detect and identify improper or illegal actions, assess threats to determine levels of risk, and implement solutions to manage and mitigate the potential consequences of an insider incident. Organizations should form a multi-disciplinary Threat Management Team to create an Incident Response Plan, ensuring their response to an insider incident or potential threat is standardized, repeatable, and consistently applied.'

Along with a thorough risk mitigation program, detection analysis and post-breach forensics, **HC3** has also suggested ways in which healthcare organizations can prevent insider threats, including:

- Revising and updating cybersecurity policies and guidelines
- Limiting privileged access and establishing role-based access control
- Implementing zero-trust and multi-factor authentication (MFA) models
- Backing up data and deploying data loss prevention tools
- Managing USB devices across the corporate network

To reduce the risks posed by insider threats, putting policies in place to immediately prevent access to corporate systems by former employees should unquestionably be added to this list. And, given that in any environment — including the most highly regulated — people can make honest mistakes, so should effective cybersecurity awareness training to help reduce these errors.

Summary

An often-quoted sentiment in healthcare goes along the lines that 'If we need prioritize spending on patient care or cybersecurity, the safety of our patients will always come first.'

Laudable though this is, the broad and continually expanding nature of the healthcare threat landscape means effective cybersecurity needs to be seen as an investment in patient care, not a drain on resources that could be better used elsewhere.

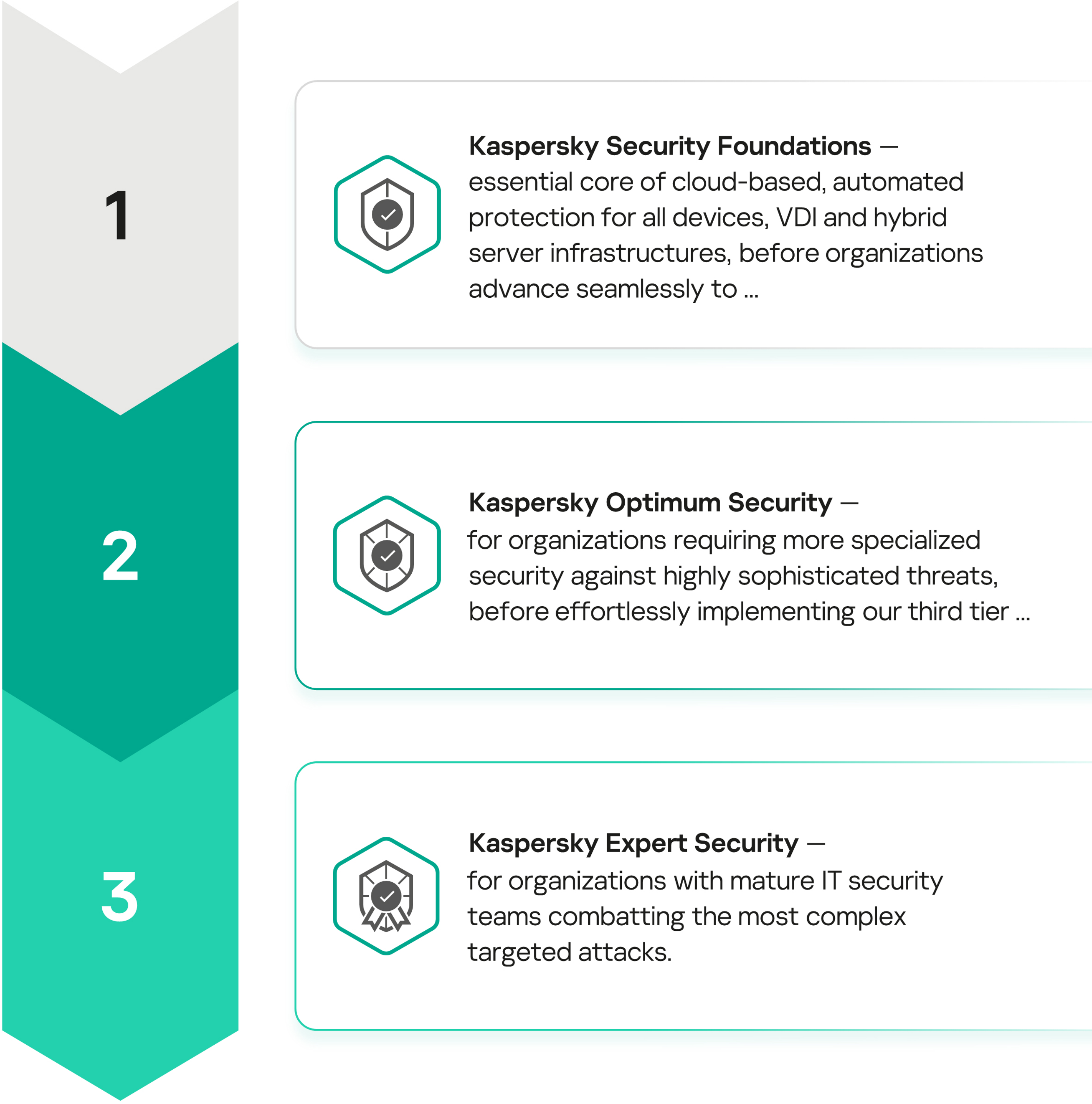
63% of health sector leaders say they're very concerned about cyberattacks

PWC PULSE SURVEY, OCTOBER 2022

Kaspersky is a pioneer in helping healthcare providers protect data and business continuity 24/7 against cyberthreats ranging from commodity, advanced and evasive threats to targeted attacks — mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection.

Our **stage-by-stage cybersecurity approach** is designed to clarify which level of security as well as which specific solutions best suit your organization. The stages provide a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring a smooth transition from one IT security maturity level to another when the time comes.

Kaspersky’s step-by-step cybersecurity approach



1

Kaspersky Security Foundations – essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to …

2

Kaspersky Optimum Security – for organizations requiring more specialized security against highly sophisticated threats, before effortlessly implementing our third tier …

3

Kaspersky Expert Security – for organizations with mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** **Kaspersky Security Foundations** **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. → **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business and/or Kaspersky Embedded System Security → **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security → **Network:** Secure your perimeter with Kaspersky Security for Mail Server and Kaspersky Security for Internet Gateway → **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage → **Support:** Access expertise with Kaspersky Premium Support and Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** **Kaspersky Optimum Security** **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity → **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum → **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum → **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum and Kaspersky Managed Detection and Response Optimum → **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

→ **Equipped**: Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. Kaspersky Anti Targeted Attack Platform with Kaspersky EDR at its core empowers your team with XDR capabilities.

→ **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:

- Integrate immediate, actionable threat intelligence into your security program. Kaspersky Threat Intelligence gives you instant access to technical, tactical, operational and strategic threat Intelligence.
- Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with Kaspersky Cybersecurity Training.

→ **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:

- Take advantage of immediate support from the Kaspersky Incident Response team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
- Bring in a second opinion and managed threat hunting expertise from a trusted partner with Kaspersky Managed Detection and Response, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
- Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through Kaspersky Security Assessment.

Targeted Solutions

What	How
Kaspersky DDoS Protection	Covers a bandwidth of up to 2Gbps, with extensive service coverage, including attack analysis reports and anti-DDoS capability assessments. Optional automatic always-on DDoS mitigation, fortified by Kaspersky engineers running parallel checks to optimize defense according to the nature of each DDoS attack.
Kaspersky Embedded Systems Security	A multi-layered solution delivering unequalled protection to Windows* embedded devices — even those with limited system resources and running discontinued OSs. Offering a solid basis of system hardening technology stack, it adds multiple opt-in security layers such as exploit prevention or anti-malware, which means protection can be optimized for devices of different power levels — including vulnerable older PCs running unsupported OSs such as Windows XP.
Kaspersky Fraud Prevention	Advanced Authentication allows for frictionless and continuous authentication, cutting the costs of second factor processes for legitimate users, while keeping fraud detection rates high in real time. Automated Fraud Analytics thoroughly analyzes events that occur during the entire session, transforming them into valuable pieces of data. Protects the external perimeter of any business, ensuring safety and protection for clients.
Kaspersky Threat Attribution Engine	A malware analysis tool deployed on your network, “on premise”, or Amazon Web Services (AWS) that incorporates 27 years of Kaspersky’s database of APT malware samples. Delivers automated analysis of the “genetics” and “genotypes” of malware for code similarity with previously investigated APT samples to rapidly link new attacks to known APT malware, actors, campaigns and previous targeted attacks.
Kaspersky Research Sandbox	Emulates company-specific systems in an isolated environment, performing automated, behavioral malware analysis and enabling safe detonation, and detection of advanced and previously unseen threats.

* and Linux later in 2023

Cyberthreats News: www.securelist.com

IT Security News: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Technologies at a glance: www.kaspersky.com/TechnoWiki

Awards and recognitions: media.kaspersky.com/en/awards

Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky bring on the future