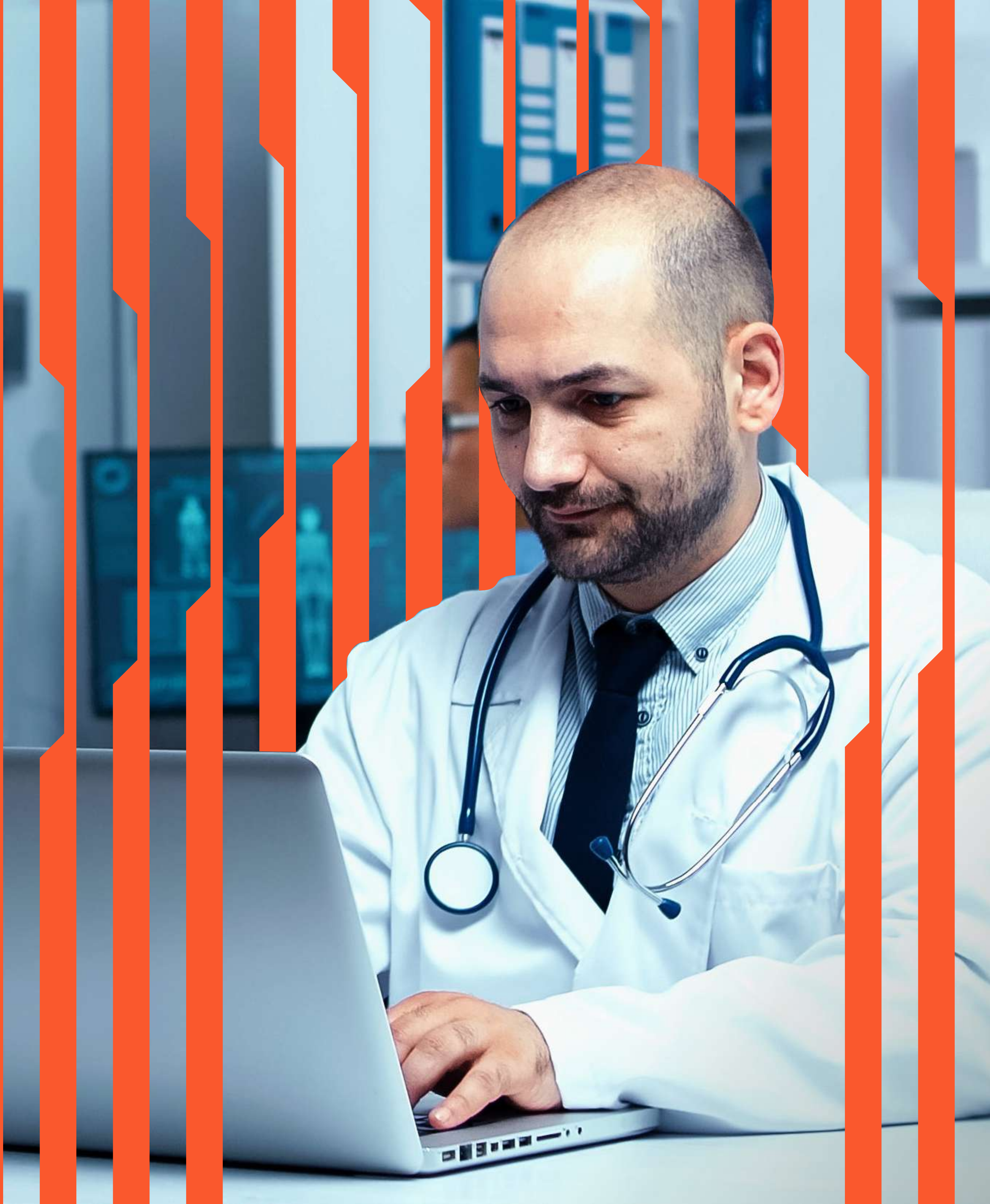
paloalto® NETWORKS | HEALTHCARE

The Healthcare CISO's Guide to Cybersecurity Transformation

Key strategies for the secure modernization of patient care



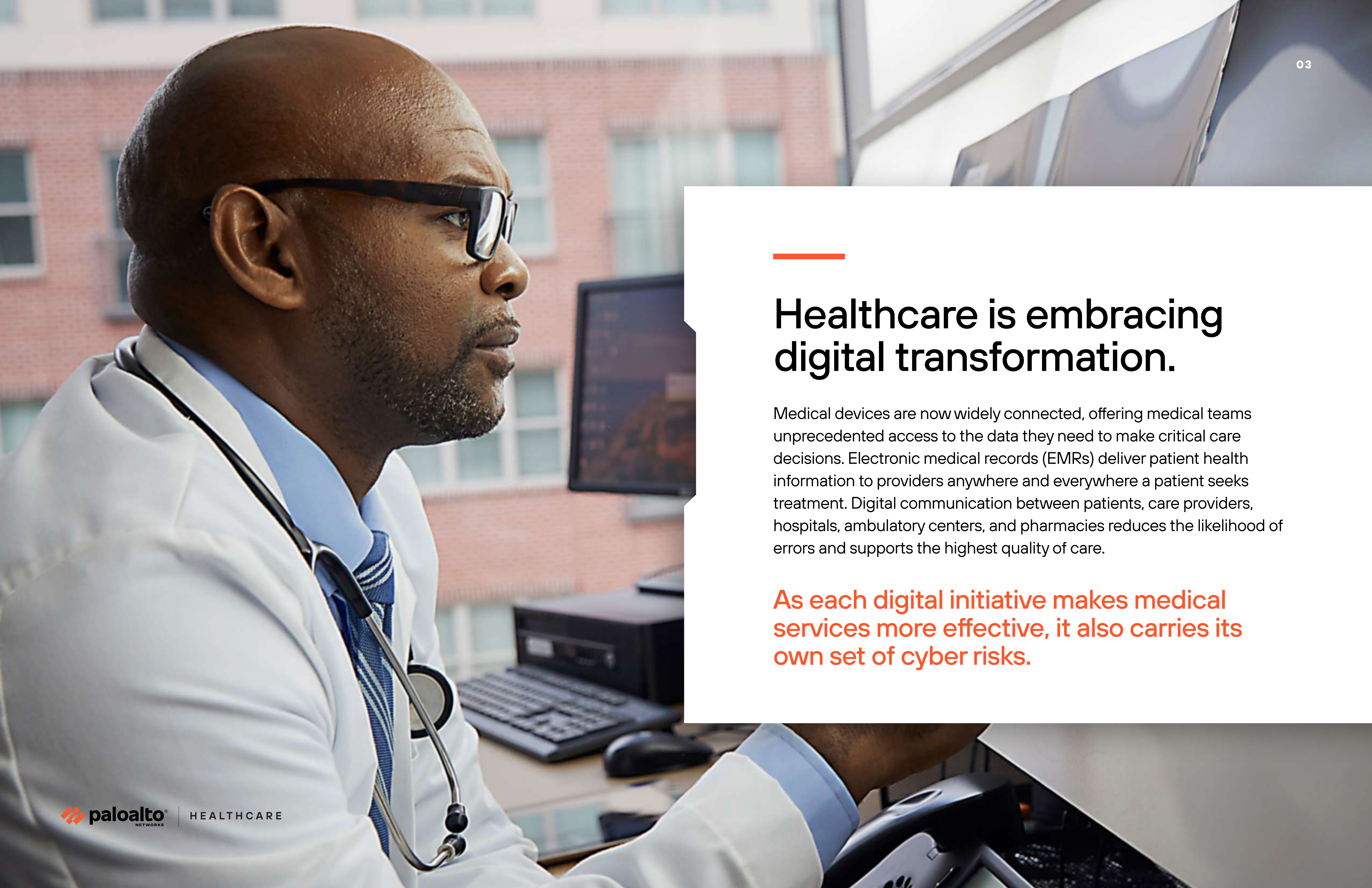
The Healthcare industry is in the midst of rapid technological change. As new devices and cloud applications allow providers to make care more flexible, personalized, and data-driven, healthcare organizations are accelerating modernization to improve the quality of care they provide and achieve better patient outcomes. As a result, IT plays an ever-increasing role in the relationship between doctors and their patients.

As the rate of modernization increases, healthcare organizations' digital environments are becoming vastly more dynamic and complex, potentially opening the door to cybercrime. In the first nine months of 2023, the medical data of more than 61 million people was exposed across more than 400 attacks, demonstrating the urgency of concerns around patient data privacy and integrity.[1] With threat actors using increasingly sophisticated tools and techniques to exploit any vulnerability, security must be an essential part of every digital initiative.

How do you increase operational resilience and ensure that the data, devices, and applications your medical teams rely on to care for patients remain secure and available?

At Palo Alto Networks, we have deep, industry-wide insight into the biggest risks you face—and where to focus for the greatest impact on your organization's cybersecurity posture.

[1] U.S. Department of Health and Human Services, 2023.



Healthcare is embracing digital transformation.

Medical devices are now widely connected, offering medical teams unprecedented access to the data they need to make critical care decisions. Electronic medical records (EMRs) deliver patient health information to providers anywhere and everywhere a patient seeks treatment. Digital communication between patients, care providers, hospitals, ambulatory centers, and pharmacies reduces the likelihood of errors and supports the highest quality of care.

As each digital initiative makes medical services more effective, it also carries its own set of cyber risks.

Healthcare organizations are prime targets

Because healthcare organizations possess sensitive data, such as protected patient health information (PHI), which carries a high monetary value for cybercriminals, they're uniquely attractive to threat actors. They also can't afford downtime since IT plays a critical role in care delivery and patient safety. When a healthcare organization experiences a cyberattack, it has no choice but to protect its data and keep its systems available, regardless of the cost.

Today, cyber criminals are using AI and ML to increase the speed and efficiency of their attacks. Across the industry, the number of ransomware attacks more than doubled between 2016 and 2021.[2] In one year, between 2021 and 2022, the industry experienced 525 incidents, with confirmed data disclosure in 436 of the incidents.[3]

$2.2M

Average ransomware demand[7]

78%

Increase in ransom payments[4]

144%

Increase in ransom demands[4]

$10.1M

Average cost of a data breach in healthcare[5]

Key conditions driving risk

Legacy systems

Many healthcare organizations still run critical care operations on legacy systems, and 83 percent use outdated software, which is more vulnerable to attack.

Providing access to sensitive health data housed on aging systems over unsecured personal networks exposes the systems to threat actors.

Expanding threat surface

From connected MRI scanners to patients accessing their care portal from a smartphone, the volume of endpoints connecting to the IT infrastructure is skyrocketing.

Many of these endpoints are highly vulnerable, running outdated operating systems and interacting with other legacy systems.

Limited resources

With budgets tightening and cybersecurity talent hard to recruit and retain, it's becoming increasingly difficult to protect the organization.

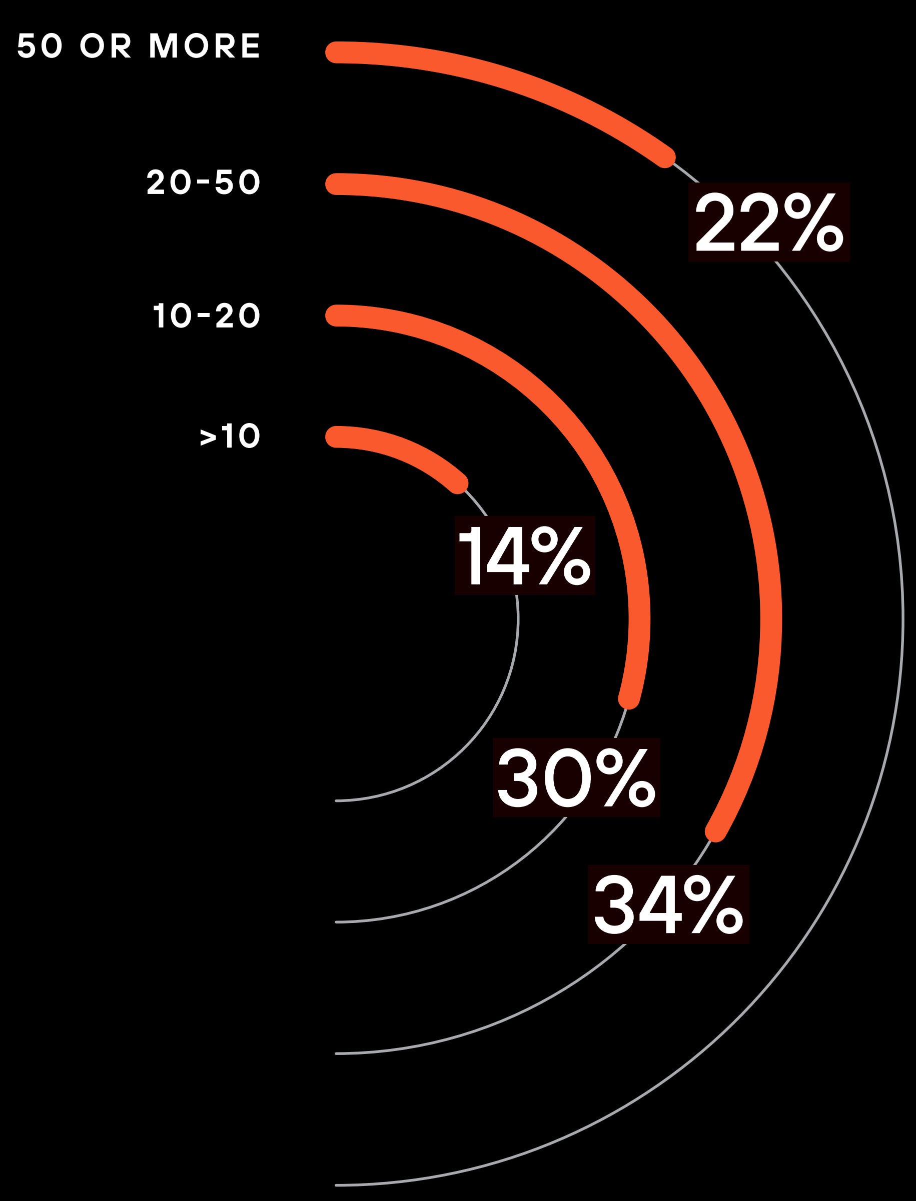
This can cause a slow reaction to fast-moving threats or delayed discovery of a threat that's already nested in the network. Today, the mean dwell time before detection is 28 days.

[2] JAMA Health Forum, 2023.
[3] Verizon 2023 Data Breach Investigations Report.
[4] Palo Alto Networks 2022 Unit 42 Ransomware Threat Report.
[5] 2022 IBM Breach Report.

Complexity challenges your ability to respond

Across the Healthcare industry, security leaders are working to modernize legacy systems, minimize vulnerabilities, and protect the entire organization. In many cases, that means relying on use case-specific security solutions and best-of-breed point solutions to address each new area of risk. As a result, the number of point solutions employed by healthcare security teams is rising.

Usage of point products in healthcare organizations[6]



[6] "What's Next in Cyber" survey of 1,300 organizations worldwide.

Three trends dominating modernization in healthcare

1 Rise of remote care

Opportunity

Telehealth allows healthcare organizations to deliver care where and when patients need it, including in rural and under-served communities. Patients appreciate the access, convenience, and reduced stress telehealth provides. In 2021, 37 percent of Americans used telemedicine for at least some services.[7]

Challenge

Providers who deliver telehealth services often work remotely, requiring secure access to EMRs and other PHI. Patients and care providers connect to telehealth services on a vast array of devices, significantly expanding the threat surface healthcare organizations need to secure.

2 Proliferation of connected devices

Opportunity

Connected devices are proliferating across healthcare environments, from HVAC systems, cameras, and access sensors that ensure a safe care environment to Internet of Medical Things (IoMT) devices that increase operational efficiency and improve patient outcomes. By 2030, providers in the United States are expected to employ 1.3 billion devices that can connect to the Internet, data center, and cloud.[8]

Challenge

Using connected devices dramatically increases the number of endpoints connected to IT infrastructure. Because IoMT devices play a critical role in patient care and safety, it's essential to keep these devices available and secure at all times. However, many of these devices are inherently vulnerable, making them an attractive target for cybercriminals. In 2021, 83 percent of IoMT devices were targeted in a cyberattack.[9]

3 Increasing complexity in medical IT environments

Opportunity

New tools, applications, and services are constantly improving healthcare organizations' ability to deliver quality care. With data and applications hosted in data centers and the cloud or delivered by SaaS providers, medical IT environments are becoming more dynamic and versatile than ever before.

Challenge

Ensuring that data, applications, and services are always available across the organization, including in distributed care networks and by remote users, is driving unprecedented complexity in medical IT environments. Managing this expanding landscape requires resources many organizations simply don't have. Point solutions that address each security challenge individually are no longer a viable approach.

[7] Centers for Disease Control and Prevention, 2022, [8] Gartner, 2021., [9] HIPPA Journal, 2021.

Modernizing security to enable digital transformation

You need a holistic, unified approach to cybersecurity to leverage technology, effectively deliver distributed care, and improve patient outcomes without increasing cyber risk.

Rather than relying on multiple tools that require complex, manual integrations, security operations should seamlessly protect your entire IT infrastructure and deliver the tools to manage and control security efficiently.

How do you simplify comprehensive visibility and streamline natively integrated security context? How can you enable a prevention-first approach to protecting and controlling your environment in a dynamic threat landscape?

Let's look at some of the most pressing challenges healthcare organizations have today—and how overcoming them can help you build a security approach that supports your organization's future.

FOCUS ONE

Securely deliver care from anywhere

The goal

A distributed care model allows you to create a more patient-centric experience in every location, whether care is delivered in person or via telemedicine. Ideally, you want to provide seamless, reliable access—ensuring necessary system uptime, performance, capacity, and security—so medical staff are always prepared to deliver quality patient care.

The challenge

Securing the IT infrastructure necessary to achieve a distributed care model with siloed security solutions is costly, drives complexity, and results in inconsistent security across care channels. Without seamlessly integrated solutions, it's more difficult to enforce least-privileged access or ensure consistent outcomes and controls.

Where to focus

▼

A modern SASE approach to security provides the flexibility and scalability needed to deliver distributed patient care securely.

▼

The solution should ensure continuous trust validation and security inspection of all traffic—and enable a consistent least-privileged access policy across all applications, devices, users, and data.

▼

The solution should simplify onboarding new users and deliver secure and controlled interconnectivity between providers, medical centers, and remote clinics.

FOCUS TWO

Secure connected devices

The goal

The connected devices you're employing today improve operational efficiency and bring the benefits of your technology investments closer to patients. Meanwhile, innovation in IoMT is constantly offering new opportunities to make care more responsive and improve patient outcomes. Ideally, you want full visibility into your entire landscape of connected devices and the confidence to deploy new devices—empowering providers, protecting patient and institutional data, and maximizing device utilization and ROI.

The challenge

Connected devices are inherently difficult to secure. Some are managed by IT, but others are managed by third parties, or not managed at all. Today, the proliferation of IoMT and other connected devices is occurring too quickly for security teams to identify them manually, let alone manage and protect them all. A complex security stack limits visibility and increases the difficulty of automating threat detection and response, putting at risk the data your IoMT devices process and the vital functions they perform.

Where to focus

- A unified platform approach to connected device and endpoint security reduces deployment and management overhead.
- Automating device discovery, visibility, security policy enforcement, and threat monitoring simplifies operations.
- Breaking down product silos and leveraging a trusted security provider's threat intelligence helps you rapidly hunt and investigate suspicious behaviors and protect against zero-day threats.

FOCUS THREE

Simplify security through consolidation

The goal

A consolidated approach to security simplifies management, reduces stress on your security team, and enables better enforcement of Zero Trust policies. Ideally, you want security planning to be an integral part of each new technology initiative, ensuring that your organization can deploy the technologies that improve patient care without introducing high levels of cybersecurity risk.

The challenge

Up to this point, most healthcare organizations have employed a best-of-breed point solution approach, creating a security stack that's not fully integrated and requires a significant investment of security team resources to manage. As your IT infrastructure expands and becomes more dynamic, this creates massive security sprawl, driving up costs while jeopardizing your ability to maintain data availability and compliance.

Where to focus

- A platform-based approach begins with an integrated solution, making it possible to reduce the number of security tools in use and simplify security operations.
- The platform should maximize security automation, decreasing the burden on the security team and reducing detection and response times.
- Over time, a platform that meets your short- and long-term needs simplifies procurement.

Additional focus areas

Enabling work from anywhere

Goal

Support a mobile, hybrid workforce to maximize productivity.

Challenge

Legacy VPN solutions are difficult to manage and lack visibility.

Safeguarding patient data

Goal

Protect sensitive data, including EMRs and other PHI, and maintain compliance.

Challenge

Vulnerable devices, risks of SaaS and cloud provider-hosted applications, and an expanded attack surface put data in jeopardy.

Zero Trust

Goal

Eliminate implicit trust with continuous validation in every digital interaction.

Challenge

Implementing Zero Trust in a highly interconnected healthcare environment is inherently difficult, and complex security and data silos exacerbate the challenge by creating inconsistent protection.

Where to focus

Enabling work from anywhere: Ensure remote access that includes continuous trust validation, security inspection, and comprehensive visibility.

Safeguarding patient data: Control access to applications and data, both at rest and in motion, across all networks, SaaS applications, devices, clouds, and users.

Zero Trust: Deploy consistent Zero Trust controls across the organization with a platform-based approach, including device-specific access and data controls.

Additional focus areas

Autonomous security operations

Goal

Leverage centralized intelligence, analytics, and AI to automate security operations.

Challenge

Human-first security operations are siloed and overwhelmed by too many alerts without enough context or insight. As a result, they can't respond to threats quickly enough.

Acquisition-ready architecture

Goal

Accelerate the integration of newly acquired organizations to support continuity of care.

Challenge

Newly acquired organizations can have unknown risks, leading to undefined exposures that can slow integration and increase time to value.

Secure cloud transformation

Goal

Reinvent the patient-provider digital experience to improve both healthcare outcomes and operational efficiency.

Challenge

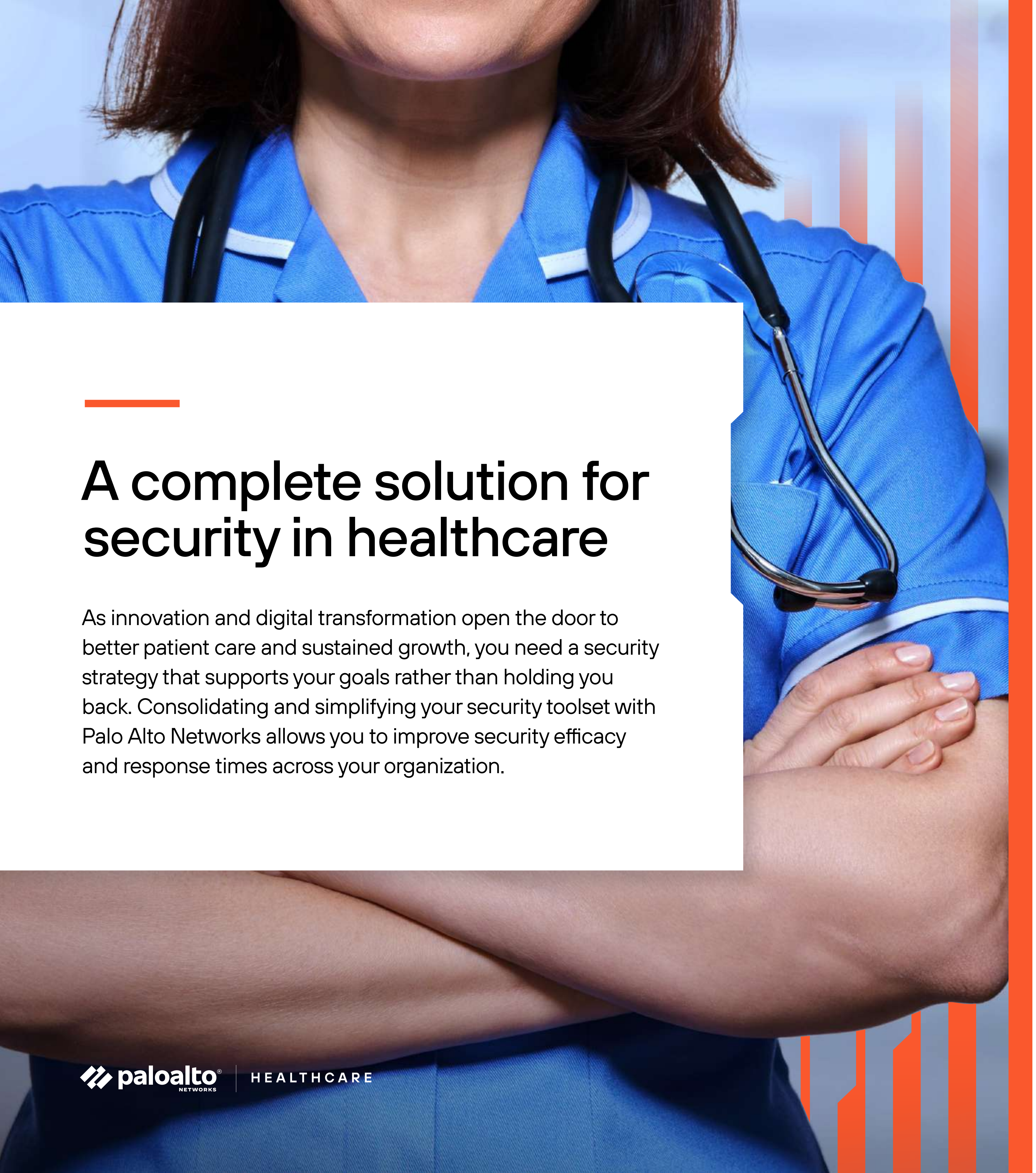
Transformation without a security-first mindset increases the attack surface while exacerbating the challenge of fragmented and bolted-on security.

Where to focus

Consolidate security operations with a single, automation-first platform for integrated and holistic threat hunting, prevention, detection and response, and incident investigation.

Establish a process for profiling and reducing risk in acquisition targets in collaboration with M&A teams, and accelerate integration of systems and resources to accelerate time to value.

Implement a cloud-native security approach with the flexibility to secure each new digital initiative, from application source to cloud infrastructure to cloud runtime environments.



A complete solution for security in healthcare

As innovation and digital transformation open the door to better patient care and sustained growth, you need a security strategy that supports your goals rather than holding you back. Consolidating and simplifying your security toolset with Palo Alto Networks allows you to improve security efficacy and response times across your organization.

With Palo Alto Networks, you can:

Securely deliver care from anywhere

Our flexible and scalable cloud-delivered platform provides secure access and an enhanced experience to deliver care in any location, in person or online.

You'll provide your medical teams with a robust, consistent, efficient, and secure experience and ensure patients' protected access to telehealth, data, and medical resources.

Secure connected devices

Our unified platform delivers comprehensive visibility, complete endpoint protection, threat detection, and rapid investigation and response for managed devices.

You'll enable healthcare IT and biomedical teams to discover, track, secure, investigate, and respond to all IoMT and other connected devices, supporting innovation and continuous care delivery.

Simplify security through consolidation

Our products all combine to deliver a comprehensive platform spanning network, cloud, identity, and device security.

You'll gain the ability to provide care to your patients in person and virtually, remain compliant, and control costs while increasing the efficiency and effectiveness of your security operations.

Achieve improved security and operational outcomes

With the simplified management and holistic security approach from Palo Alto Networks, your next digital initiative won't need to wait while you test and procure another security solution. You'll have all you need to accelerate critical projects for your organization to innovate, grow, and deliver the highest quality of care.

Enabling work from anywhere

Ensure a consistent, secure, and efficient experience for your entire workforce so they can access data, applications, and services from anywhere.

Autonomous security operations

Provide centralized, automated intelligence and analysis across your environment, improving security outcomes while reducing SOC resources.

Safeguarding data

Protect all patient data from any source, at rest and in motion, across your entire digital landscape.

Acquisition-ready architecture

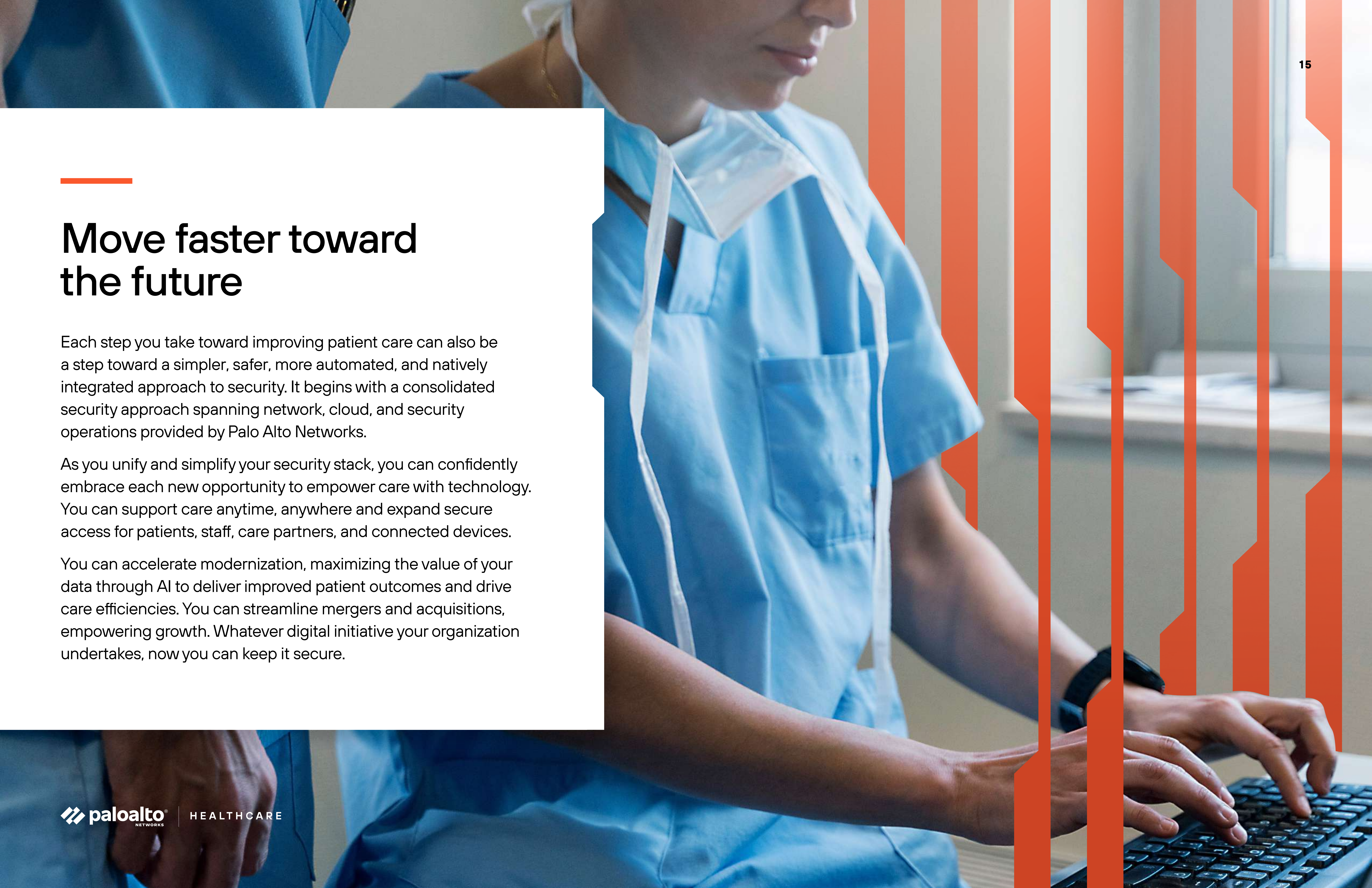
Leverage our SASE architecture and Cortex® platform to eliminate hidden security risks and build secure interconnectivity that enables an accelerated time to value for any acquisition.

Zero Trust

Accelerate your Zero Trust journey by deploying consistent policies and controls across the environment with a platform approach.

Secure cloud transformation

Continuously discover, evaluate, and mitigate risk with streamlined management and native integration.



Move faster toward the future

Each step you take toward improving patient care can also be a step toward a simpler, safer, more automated, and natively integrated approach to security. It begins with a consolidated security approach spanning network, cloud, and security operations provided by Palo Alto Networks.

As you unify and simplify your security stack, you can confidently embrace each new opportunity to empower care with technology. You can support care anytime, anywhere and expand secure access for patients, staff, care partners, and connected devices.

You can accelerate modernization, maximizing the value of your data through AI to deliver improved patient outcomes and drive care efficiencies. You can streamline mergers and acquisitions, empowering growth. Whatever digital initiative your organization undertakes, now you can keep it secure.

paloalto NETWORKS | HEALTHCARE

Take the next step.

Simplify and strengthen your healthcare organization’s security and make the future possible with Palo Alto Networks.

WWW.PALOALTONETWORKS.COM/HEALTHCARE