Lookout®

SOLUTION BRIEF

Securing Healthcare's Digital Transformation to the Cloud

Key Facts

1. The rapid adoption of telehealth has accelerated digital transformation; resulting in an increased use of cloud services and both managed and unmanaged devices by healthcare providers and patients.
2. Healthcare organizations experienced a 194% increase in mobile phishing exposures between Q4 of 2020 to Q1 of 2021. Cyberattackers use mobile phishing to steal login credentials in order to gain access to apps and data across the infrastructure.
3. Ransomware is the unrelenting enemy of the healthcare industry. In today's complex ecosystem of devices, networks, apps, users, and data, ransomware is often the primary challenge facing healthcare organizations.

Industry-wide digital transformation took place overnight

The pandemic of 2020 drove broad telehealth adoption by patients and healthcare providers alike. It was a catalyst for years worth of digital transformation across the entire industry in a matter of months.

Many organizations that previously relied on having employees on site had to enable those workers to deliver the same high-quality care from remote locations without compromising security or patient privacy.

While both patients and providers were unsure of telehealth efficacy at first, it has grown in popularity and appears to be here to stay. As a result, hybrid work will remain and there are fundamental changes to security and privacy that must be considered for the future.

Telehealth has become the most viable way for care providers of all types to remotely meet, diagnose and follow up with patients. Whether a primary care physician is diagnosing a child at home or a psychiatrist is checking in on patients, many practices have recognized the value of telehealth.

Telehealth has also increased accessibility for patients who may not have had easy access to quality care due to distance, available transportation or physical disability. Much like mobile shopping or banking, telehealth brings an undeniable element of convenience to the patient and can be performed from any device.

For healthcare providers to keep up, they need to embrace telehealth and create a secure, private experience for both themselves and their patients.

In addition, the platforms upon which healthcare providers rely experienced changes that create new security and privacy risks. As healthcare providers connected to platforms like Epic, Cerner, Allscripts, and Athenahealth from home, they inevitably used unmanaged devices out of necessity. In their clinic or hospital, providers use managed devices provided for them. At home, they used the tablet or smartphone that was available.

Using unmanaged devices eliminated the visibility and security controls created to secure access and protected privacy. This created the risk of malware and advanced persistent attacks going undetected.

If attackers compromise an unmanaged device or steal login credentials, they have a very high chance of quietly infiltrating the infrastructure and stealing data.

Attackers target healthcare organizations because they possess personally identifiable information (PII) in addition to private health data. This includes payment card data, social security number, address, phone, and emergency contact information. As a result, they make for ripe targets.

Finally, the biggest issue for healthcare is ransomware. In 2020, there was a 123% increase in ransomware attempts against the healthcare industry. The pandemic put immense pressure on every resource in the healthcare industry, including IT and Security teams.

Ransomware groups exploited the pandemic and bombarded the industry with highly targeted and customized ransomware campaigns that crippled some medical institutions. Similar to other industry-wide shifts, this problem is not likely to subside quickly or soon.

You need to regain control of data and users

Your healthcare practice shares a common goal with every other practice in the industry – provide the best care to patients while safeguarding their sensitive data and personal privacy. You also share a common challenge in that you no longer have the same visibility and control as more is happening outside your four walls and on devices and networks you don't manage. This presents new challenges for security, privacy and compliance.

In addition to industry-specific standards like HIPAA and HITRUST, you also need to comply with regional and international data protection laws like GDPR and CCPA. With data traveling wherever it's needed, it can be incredibly difficult to ensure compliance with these standards and laws.

Electronic medical records (EMRs), diagnoses, prescriptions, and more are being stored and shared through cloud services that are accessible from any device or location. Without the right set of capabilities to prevent data loss, protect privacy and detect insider threats, you can't control what a user does with data once it leaves the perimeter.

Ransomware – an insidious enemy that isn't going away

Ransomware groups are getting smarter and operating like businesses to increase their profit through increased success rates. They target healthcare systems because they know the provider can't afford to be shut down. As a result, they believe that healthcare targets are more willing to pay the ransom in order to get their data back.

In 2020, over 600 clinics, hospitals, and healthcare organizations reported that they suffered from a ransomware attack. These attacks almost always start with compromised employee credentials.

Attackers target employees with phishing attacks, increasingly through mobile channels, and use the credentials to enter the infrastructure unnoticed. Once they are in, they move laterally through the infrastructure, exfiltrate significant amounts of sensitive data, lock the administrators out and encrypt the data for ransom.

Even when you pay the ransom, there is no guarantee that all of the data is returned or that the group won't leak the data to destroy your reputation.

Traditional security solutions can't keep up

Every industry has shifted to be more reliant on cloud and mobile services and, as a result, faces more security challenges. Healthcare is not immune to this, as the threat landscape of tactics, techniques and procedures (TTPs) that attackers use to target the industry favor advanced phishing and ransomware attacks rooted in access to cloud infrastructure. Traditional security solutions can't keep up as the healthcare industry stabilizes after a disruptive year that brought about so many new technologies and practices.

Adoption of the cloud has enabled healthcare organizations to leverage SaaS apps that increase productivity and cloud-based infrastructure that can dynamically scale as needed. It has also introduced new risks. With legitimate credentials, anyone can access these resources from anywhere outside the traditional perimeter. Without visibility into the context of who or what is connecting to cloud-based resources, security teams could be missing telltale signs of a threat actor entering the infrastructure.

In addition, there is also the challenge of ensuring that on-premises infrastructure is secured in the same way as cloud-based infrastructure. As both work and infrastructure remain hybrid, ensuring secure access to the entire infrastructure equally can be problematic and leave gaps that attackers exploit as a backstage pass to your highly valuable assets.

You need to regain the visibility you used to have inside your perimeter

Healthcare organizations, regardless of their size of specialty, need to regain the visibility and control they once had when most every user and device was inside the perimeter. Without them, it's nearly impossible to know the full breadth of risk that you are up against.

The first step is implementing secure access service edge (SASE), which will put your IT and security teams back in control. SASE is grounded in the philosophy of Zero Trust, which assumes every device or user is compromised until proven otherwise. Applying this mindset to your broader security strategy will help you provide the right security posture to back up all the fundamental changes that have taken place across the industry.

Lookout SASE integrates mobile endpoint security (MES) with cloud access security broker (CASB) and zero trust network access (ZTNA). CASB provides full visibility into the interactions between users, endpoints, cloud apps and your data. It also enables you to dynamically dial in Zero Trust access controls.

ZTNA provides seamless access to any apps or infrastructure regardless of whether they reside in traditional data centers, public clouds, or hybrid environments. It also extends the security benefits of cloud infrastructure to legacy apps.

MES secures mobile devices, which are often overlooked and can create a gap in your security architecture. Cyber attackers increasingly target them because mobile devices are at the intersection of our personal and professional life.

For more resources to help understand how to secure your healthcare organization, visit the Lookout Healthcare Solution Page.

Industry-wide digital transformation took place overnight

Healthcare organizations underwent many years' worth of digital transformation in 2020.

- Suddenly, organizations that could rely on having employees on site every day had to enable them to be just as productive from home without sacrificing security.
  - Looking forward, an element of hybrid work will remain for the foreseeable future.
- Telehealth became the most viable way for care providers to connect with patients during the pandemic.
  - Much like with mobile shopping or banking, mobile healthcare is far more convenient to the customer.
  - This change will remain as healthcare access remains important on a national level.
- A mix of managed and unmanaged devices are being used to access highly sensitive compliance-related data.
  - Healthcare organizations don't just possess data related to patient health. They also store payment data, social security numbers, and other highly sensitive and personally identifiable information.
- Ransomware groups are going after healthcare organizations
  - Attackers are leveraging the fact that healthcare organizations are under immense pressure as a result of the pandemic and targeting them with customized ransomware campaigns

Data and users are constantly moving in and out of secured infrastructure

Your mission is to safeguard sensitive data while providing seamless care to your patients. But you no longer have the visibility and control you used to have as activities are happening outside your hospital walls and on devices and networks you don't manage.

With data traveling wherever it's needed and teams no longer having the visibility they once did when everything stayed inside the traditional perimeter, it can be difficult to ensure compliance.

- EMRs, diagnoses, prescriptions, and more are being stored and shared through cloud services that are accessible from any device and location.
  - Without the right tools, you can't control what a user does with data once it leaves the perimeter.
- In addition to industry-specific compliance standards like HIPAA, other data privacy regulations such as GDPR and CCPA also need to be respected.

Ransomware is your worst enemy and it isn't going away

Ransomware groups know that healthcare systems can't afford to be offline, so they may have greater success in getting a ransom.

- Ransomware attacks almost always start by phishing employee login credentials that give the attackers better odds of entering the infrastructure unnoticed.
- Once they compromise the credentials, the attackers will move laterally through the infrastructure, exfiltrate massive amounts of data, and lock the administrators out as they demand their ransom.
- In 2020, over 600 clinics, hospitals, and healthcare organizations reported that they suffered from a ransomware attack

Traditional security solutions can't keep up

Traditional security solutions cannot keep up with the needs of healthcare organizations that are going through rapid digital transformation in the age of a rapidly evolving cyber threat landscape.

- Adoption of the cloud has enabled healthcare organizations to leverage SaaS apps that increase productivity and cloud-based infrastructure that can dynamically scale as needed. It has also introduced new risks.
- With legitimate credentials, anyone can access these resources from anywhere outside the traditional perimeter.
- Without visibility into the context of who or what is connecting to cloud-based resources, security teams could be missing telltale signs of a threat actor entering the infrastructure.
- There's also the challenge of ensuring that on-premises infrastructure is secured in the same way as cloud-based services.

You need to regain the visibility you used to have inside your perimeter

Organizations need to regain the visibility they had when most every user and device was inside the perimeter. Without that visibility, it's nearly impossible to know what risks you're up against.

- In order to regain visibility and protect employees, data, and devices like you still have a perimeter, organizations need to implement secure access service edge (SASE) to put IT and Security teams back in control.
- SASE is grounded in the philosophy of Zero Trust, which assumes that every device or user is risky until proven otherwise.

Lookout SASE integrates mobile endpoint security (MES) with cloud access security broker (CASB) and zero trust network access (ZTNA).

- CASB provides full visibility into the interactions between users, endpoints, cloud apps and your data. It also enables you to dynamically dial in Zero Trust access controls.
- ZTNA Provides seamless access to any apps or infrastructure regardless of whether they reside in traditional data centers, public clouds, or hybrid environments. It also extends the security benefits of cloud infrastructure to legacy apps.
- MES secures mobile devices, which are often overlooked and can create a gap in your security architecture. While mobile operating systems are considered to be more resilient, cyberattackers increasingly target them because mobile devices are at the intersection of our personal and professional life. These devices have a treasure trove of data and attackers use them as the initial intrusion into your organization.

Lookout®

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit **www.lookout.com** and follow Lookout on its **blog**, **LinkedIn**, and **Twitter.**

For more information visit
lookout.com

To learn more about Lookout Healthcare soluion, visit
lookout.com/solutions/healthcare