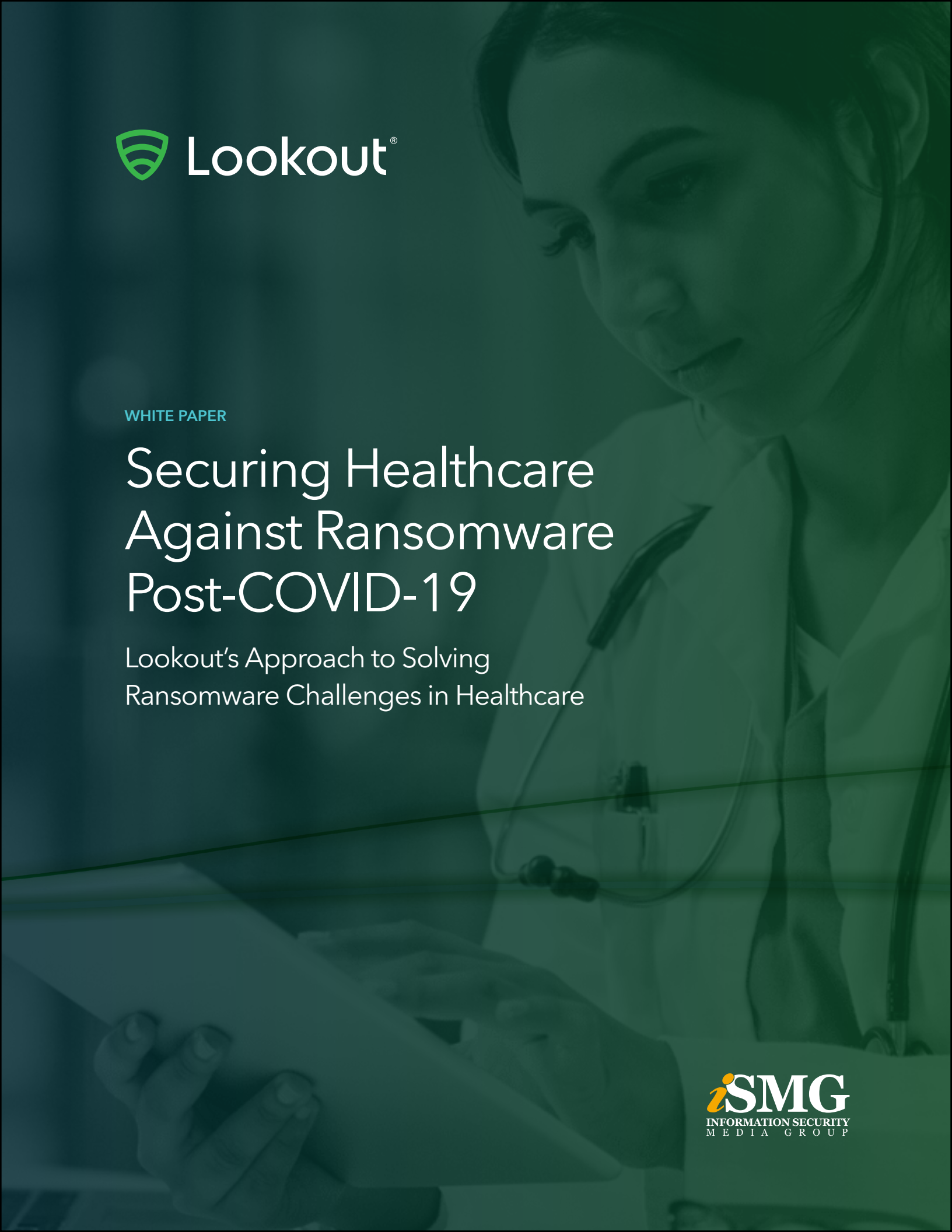

Lookout®

WHITE PAPER

Securing Healthcare Against Ransomware Post-COVID-19

Lookout's Approach to Solving Ransomware Challenges in Healthcare

iSMG
INFORMATION SECURITY
MEDIA GROUP

Introduction

The COVID-19 pandemic arguably compressed years of digital transformation for the entire healthcare industry. Rapid deployment of new and existing technologies, including telemedicine, has enabled practices and hospitals alike to stay productive - but not without an increase in cyberattacks on the industry.

Most of the technology adopted during this period of rapid evolution focused on solving the challenge of keeping employees and patients connected regardless of their location. Telemedicine, for example, enabled existing patients and doctors to connect. It also expanded healthcare accessibility to those who may have a disability that prohibited them from getting to the doctor. This has made telehealth the norm for both patients and doctors – so much that 37% of patients in one survey said they intend to continue using telemedicine services after normalcy returns.[1]

In addition to connecting patients and providers, healthcare organizations also had to keep their staff productive from anywhere. This meant expanding access to sensitive compliance-related data that's stored in collaborative cloud or private apps from any personal, managed, or unmanaged device. Platforms such as Google Workspace became widely used, which helped enable productivity but also increased risk.

37%

of patients in one survey said they intend to continue using telemedicine services.

Over the course of 2020, nearly 1 in 10 healthcare workers encountered a malicious mobile app on their device. Taking it a step further, 1 in 4 workers with Google Workspace on their device encountered a mobile phishing link.

Due to the rapid digital transformation it has undergone, the healthcare industry is facing a fundamentally new threat landscape. Providers need to understand the challenges ahead, the problems they will face and most importantly how to solve these issues. Modernizing traditional models of user, device, network, and data control with the right security platform is necessary if a provider wants to keep ahead of the next ransomware or advanced persistent threat campaign.

Healthcare's ransomware problems and challenges

> Healthcare entities are clearly the main target of these attacks because their data is not only critical, and therefore valuable, but healthcare facilities deal with life-and-death matters every day.
>
> Jason G. Weiss, retired FBI adviser

Healthcare organizations are seen as captivating targets, specifically targeted by ransomware gangs.

Warnings and Advisories

In April, the FBI issued a warning that, "Cyber actors will likely increase cyber intrusions against healthcare systems – to include medical devices – due to mandatory transition from paper to electronic health records, lax cybersecurity standards, and a higher financial payout for medical records in the black market."[2]

The FBI warning adds, "The healthcare industry is not technically prepared to combat cybercriminals' basic cyber intrusion tactics, techniques and procedures, much less against more advanced persistent threats. The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

Another report[3] notes that cybercriminals are targeting the healthcare sector because they believe hospitals are more likely to meet their ransom demands as they seek to keep functioning during the pandemic. It notes that ransomware and other cyberattacks on healthcare entities globally increased 45% in the last two months of 2020, double the increase in cyberattacks across all industry sectors worldwide.

Furthermore, in the United States, the Department of Health and Human Services' HIPAA Breach Reporting Tool website, which lists health data breaches affecting 500 or more individuals, showed a surge of ransomware and other hacking incidents reported in 2020.[4] The count exceeded 600 breaches, compared to an average of 368 annually, or some 3,685 major health data breaches reported since recording started in September 2009.

As the pandemic began surging, so did reports of phishing messages using COVID-19 as the social engineering hook.[5] The World Health Organization even issued an advisory on ongoing cyber scams such as fake URLs for virus tracking maps.

As a result of the social engineering opportunities presented by the pandemic, Lookout reports that in the first quarter of 2021 alone, nearly 20% of healthcare workers were exposed to a mobile phishing threat.[6] Since most other attack types start by a threat actor phishing for credentials, this trend is particularly concerning.

20% **In the first quarter of 2021 alone, nearly 20% of healthcare workers were exposed to a mobile phishing threat.**

Using PII as a Threat

Attackers have also broadened their tactics for carrying out ransomware.[7] In addition to encrypting data, attackers are now downloading privileged data and threatening to release or sell personally identifiable information (PII) if the ransom isn't paid.

This affects compliance with HIPAA in the U.S., and data privacy regulations such as GDPR in Europe and CCPA in California. Violation of these laws can result in heavy fines. Organizations may have to pay up to 4% of global turnover in the case of violating GDPR – or legal action on an individual or class action basis. For example, at least four lawsuits seeking class action status were filed against Scripps Health by patients whose information was stolen in a ransomware attack.[8]

Another supplier of healthcare technology, San Antonio-based CaptureRx, had to notify its healthcare providers' clients that patient details such as medical records, name, date of birth and prescription information could have been exposed following a ransomware attack. CaptureRx serves more than 500 hospitals and health centers in 45 U.S. states via a pharmacy network of more than 3,500 pharmacies. HIPAA Journal reported that more than 24,000 patients' personal information has been exposed so far.[9]

22.8M

patients affected by a healthcare data breach between January and June 2021.

Nightmare Scenarios

In another occurrence, on May 14, 2021, Ireland's state health services provider, the Health Service Executive (HSE), shut down all its IT systems following a ransomware attack that had an impact on all national and local systems involved in all core

health services.[10] Being unable to deliver health services was the nightmare scenario that health organizations dread.

HSE says it has not and will not pay a ransom – which is the advised action both legally and from the security community, as paying ransoms is no guarantee of data being returned. Even if the attacker provides a decryptor after the ransom is paid, it doesn't always work. Plus, those who pay are more likely to be attacked again.

When it comes to the scale of data losses, by July 2021, more than 22.8 million patients had been affected by a healthcare data breach during the year. This represented a 185% increase from the same time period last year when just 7.9 million individuals were affected, according to a report from Fortified Health Security.[11]

The problem for healthcare organizations is summed up well by retired supervisory FBI agent Jason G. Weiss, an attorney at law firm Faegre Drinker Biddle & Reath LLP. Weiss observes: "Healthcare entities are clearly the main target of these attacks because their data is not only critical, and therefore valuable, but healthcare facilities deal with life-and-death matters every day, and they have to do everything they can to get their systems back up or patients could literally die. Unless and until healthcare facilities can harden their networks, train their employees and prevent these attacks from starting, they are only going to continue to get worse."[12]

Why Target Healthcare Data?

All PII is valuable, but there are particular reasons why health PII is prized by criminals. Passwords or PINs can be changed and made worthless, whereas a user's health history can't be changed so it retains its value. As a result, patient PII is the most frequently compromised type of record in cyberattacks, according to Ponemon research.[13]

Ponemon also notes that healthcare data breaches are the costliest of any industry. One of the reasons why these breaches are more expensive than those in less-regulated industries such as hospitality, media and research is that regulators recognize its importance and impose higher fines. So it's unsurprising that for the eleventh year in a row, healthcare incurred the highest average breach costs, increasing from $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase.[14]

29.5%

average increase in breach costs, from $7.13 million in 2020 to $9.23 million in 2021.

As a result of increasing risk to the industry and high costs associated with data breaches, former healthcare CISO Sumit Sehgal notes that cyber insurers are now more closely scrutinizing potential clients to ensure that "as part of the information security risk management process, there is appropriate due diligence given to continuity of operations" in case of a ransomware attack.[15]

Preventing cyberattacks, reducing the impact when they occur and having a plan to respond and get back up and running in a timely manner all require specialist skills to implement and deploy. Unfortunately such cyber skills are in short supply in all sectors, including healthcare; in fact, (ISC)^2 identified a global workforce shortfall of 3 million cybersecurity professionals.[16] Therefore, healthcare organizations need to seek the help of security solutions providers that can enable them to secure employees, their devices, and the data they access. Providers should do so in a way that ensures alignment with compliance standards, respects privacy, and mitigates the risk of being the next data breach headline.

Potential remedies and their drawbacks

> Traditional security solutions are failing to keep up with the cyberthreat landscape as it rapidly evolves during this industry-wide digital transformation.

Cybersecurity for critical infrastructure has become an increasing concern for governments, especially in the wake of the May 2021 hack of the **Colonial Pipeline**,[17] which hit oil supplies on the United States East Coast. Healthcare too is identified by the government as a critical sector – and is now being prioritized. Information sharing, threat intelligence and expertise from government agencies and private sector organizations, particularly when helping with incident response, is clearly welcomed.

In addition to encouraging and facilitating best practice, governments and regulatory bodies are also setting minimum standards for cybersecurity, adding compliance to commercial interest as a driver of cybersecurity.

Another challenge for the health sector is that health workers will often use tablets to access Personal Electronic Medical Records (EMRs), or use personal devices to do so from home. These practices, while necessary, create security and compliance concerns.

Segmentation

Segmenting networks and avoiding giving too much access or privilege to any single user, logically leads to a Zero Trust approach which enforces minimum privilege. But when healthcare organizations are making a patient's records accessible to doctors and other clinicians who need them, the extent of segmentation possible may be less than what security professionals prefer. Sometimes administration and payments run on the same systems as treatment so that one can reference the other. This can make functionality and security a trade-off.

Patching

Maintaining up-to-date patching is a challenge for many organizations, given the frequency and volume of updates. With the plethora of devices and systems used in healthcare, it becomes a particularly onerous task. Automation of updates is a huge benefit, but automated downloads can also potentially cause problems, as was seen in the **SolarWinds incident**[18] where infected software updates from the company were being automatically downloaded. Since the update came from a trusted source, it bypassed the recipients' defenses, enabling the attackers to install a backdoor into the infected systems.

VPNs

In response to the switch to working from home, many organizations have increased the capacity of their corporate VPNs - in some cases, going from tens of VPN users to thousands. While VPN use improves security, such a sudden drastic expansion of use has presented a challenge to ensure secure connectivity across their infrastructure.

This approach can also mean that a single compromised device connecting to the infrastructure could put the entire organization at risk.

Cloud Adoption

It is true that cloud adoption has sped up among those that were lagging, whether from lingering security concerns or financial constraints. Higher rates of cloud adoption have enabled healthcare organizations to leverage SaaS apps that increase productivity. In addition, cloud-based infrastructures are enabling organizations to dynamically scale as required.

But while cloud services today have more modern security measures built in than those on-premises, true endpoint-to-cloud security is very difficult to achieve. Cloud brings its own set of risks that need to be understood and mitigated. Not least are the supply chain issues, with suppliers also under attack.

"Cloud vendors are seen as holding high volumes of data – in particular, personal health data when the vendor serves the healthcare sector," reports Kate Borten,[19] president of privacy and security at the consulting firm The Marblehead Group.

There's also the challenge of ensuring that on-premises infrastructure is secured in the same way as cloud-based services.

Securing identity, access, and privilege escalation have always been important in preventing ransomware, but they have become even more key components of security posture. In addition, organizations need visibility into who is accessing what resource, for what purpose.

Security teams that don't have visibility of the context of who or what is connecting to cloud resources could be missing telltale signs of a threat actor entering the infrastructure. That's because anyone with legitimate credentials can access cloud-based resources from anywhere outside the traditional perimeter. The hurdle of gaining access to a specific secure location or device no longer applies.

> Lookout's SASE approach integrates mobile endpoint security with cloud access security broker and zero trust network access.

The Lookout Approach

Lookout's approach is to enable organizations to implement a full endpoint-to-cloud security strategy, ensuring data can securely go wherever it's needed.

The variety of endpoint devices that now have access to corporate infrastructure make it a priority to ensure that security teams have visibility into activities associated with data, users, apps and services. They need to regain the visibility

they had when almost every user and device was inside the perimeter. Otherwise, it becomes nearly impossible to know what risks they face.

Secure Access Service Edge

The way to regain this visibility and protect employees, data and devices is to implement secure access service edge, or SASE,[20] 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.

While U.S. President Biden's May 2021 executive order on cybersecurity[21] targeted the federal government, the measures apply equally to the private sector. The order says organizations must adopt security best practices and advance toward Zero Trust architecture. They must also accelerate movement to secure cloud services, including software as a service, or SaaS; infrastructure as a service, or IaaS; and platform as a service, or PaaS.

Lookout's SASE approach integrates mobile endpoint security with cloud access security broker and zero trust network access.

Cloud Access Security Broker

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.

With continuous monitoring of user and entity behavior analytics, or UEBA, security teams can detect and respond to insider threats and advanced cyberattacks. Lookout provides advanced data loss prevention that can classify, encrypt and restrict sharing of users' data on the fly so that only authorized users have access. Lookout also performs automated assessment of all of an organization's cloud apps and infrastructure to ensure they are properly configured.

Healthcare workers and organizations rely on cloud-based SaaS platforms and infrastructure to access sensitive patient data. They need to ensure secure access and handling of that data, proper security configuration of cloud resources, and continuous monitoring of user and entity behaviors in order to align with HIPAA and other compliance standards.

Zero Trust Network Access

> ZTNA enables teams to create dynamic resource access policies that only grant users access to the resources they need to get their work done.

Lookout ZTNA provides seamless access to any on-premises apps or infrastructure. It also extends the security benefits of cloud infrastructure to legacy and private apps.

ZTNA enables teams to create dynamic resource access policies that only grant users access to the resources they need to get their work done. This approach helps modernize the access process by reducing reliance on VPN. This helps solve VPN challenges such as giving unrestricted access to their infrastructure without any context, not understanding whether the device connecting is free of malware or if the user is who they say they are. VPN can also give other devices on the user's network access to an organization's infrastructure. Each of these issues can be a massive security risk.

Ransomware attacks most frequently start with a threat actor compromising an employee's credentials, which they will then use to log in to the infrastructure, move laterally until they find valuable resources, and then exfiltrate large amounts of data before locking up parts of the infrastructure and demanding the ransom. ZTNA and CASB help mitigate the risk of this happening by enabling security and IT teams to implement granular access policies that take into account contextual signals about the user, device, location, and more that could indicate a compromised account.

> Cyberattackers are increasingly targeting mobile devices because they are at the intersection of our personal and professional lives.

Mobile Endpoint Security

When it comes to MES, Lookout notes that the problem of security on mobile devices is often overlooked, creating a gap in organizations' security architecture. While mobile operating systems are considered to be more resilient, cyberattackers are increasingly targeting them[22] because mobile devices are at the intersection of our personal and professional lives. These devices contain a treasure trove of data, and attackers use them as the initial point of intrusion into your organization.

Continuous monitoring of mobile endpoints with Lookout ensures that only devices that are free of threats can access your data and infrastructure. This mitigates the risk of threat actors exploiting OS vulnerabilities, delivering malware and using mobile phishing to quietly exfiltrate data from the user's device. Considering the amount of access mobile devices have to cloud-based apps and resources, they need to be included in an organization's overall security architecture strategy to prevent a massive blind spot on the devices employees use the most.

Lookout enables healthcare workers to securely use a mix of managed, unmanaged, personal and work-issued devices to stay productive at their workplace and away from it. In addition, it ensures compliance with data privacy standards that include mobile devices, which means healthcare organizations can show auditors that they have visibility into the risk profile and data handling that takes place from smartphones and tablets.

Conclusion

Healthcare organizations need complete visibility and dynamic controls over who accesses what information for what purpose. SASE can provide protection in the cloud as if there was still a perimeter. But without mobile context, dedicated SASE vendors have limited visibility into the security posture of the endpoint. To achieve security from endpoint to cloud, users should avoid stand-alone tools that increase complexity and instead seek an integrated platform offering. Lookout provides an integrated approach, delivering visibility into what's happening on managed and unmanaged endpoints, in the cloud and everywhere in between.

The Lookout approach ensures granular and dynamic access to match each user's risk posture, such as whether the device has malware installed or if the user is accessing sensitive data unrelated to their role. This enables comprehensive protection against even the most advanced insider threats and fileless cyberattacks.

By understanding what apps and data employees need for their work, and what information patients need and are entitled to access, Lookout enables users to securely and dynamically access what they are allowed and need – whether it's stored in enterprise applications within the perimeter, private cloud or cloud applications.

References

1 Piplsay, A global consumer research platform, https://piplsay.com/health-apps-and-telemedicine-how-popular-are-they/

2 https://www.healthcareinfosecurity.com/fbi-issues-healthcare-cyber-alerts-a-6779

3 https://www.healthcareinfosecurity.com/ransomware-attacks-in-healthcare-surging-a-15701

4 https://www.healthcareinfosecurity.com/ransomware-attacks-in-healthcare-surging-a-15701

5 https://securityboulevard.com/2021/07/hackers-exploit-the-covid-19-pandemic-for-cyber-scams/

6 Lookout

7 https://www.healthcareinfosecurity.com/blogs/business-ransomware-specialists-help-boost-profits-p-3066

8 https://www.healthcareinfosecurity.com/scripps-health-attackers-stole-phi-147000-patients-a-16797

9 https://www.hipaajournal.com/capturerx-ransomware-attack-affects-multiple-healthcare-provider-clients/

10 https://www.healthcareinfosecurity.com/irish-healthcare-sector-was-hit-by-2-ransomware-attacks-a-16661

11 https://go.fortifiedhealthsecurity.com/2021-Mid-Year-Horizon-Report-1.htm

12 https://www.healthcareinfosecurity.com/in-healthcare-ransomware-hitting-diverse-targets-a-16116

13 Cost of a Data Breach Report 2021, IBM/Ponemon, https://www.ponemon.org/

14 Cost of a Data Breach Report 2021, IBM/Ponemon, https://www.ponemon.org/

15 https://www.healthcareinfosecurity.com/interviews/how-cyber-insurance-for-healthcare-entities-evolving-i-4914

16 https://blog.isc2.org/isc2_blog/2020/11/2020-isc2-cybersecurity-workforce-study-skills-gap-narrows-in-an-unusual-year.html

17 https://www.lookout.com/blog/3-actions-to-take-based-on-the-colonial-pipeline-ransomware-attack?utm_source=3PW&utm_medium=OT&utm_campaign=WW-MU-EN-MU-RSW---ISMG-Healthcare-WP.ENT&utm_content=Colonial-Pipeline-Blog

18 https://resources.lookout.com/blog/what-solarwinds-teaches-us-about-zero-trust-for-mobile-endpoints?utm_source=3PW&utm_medium=OT&utm_campaign=WW-MU-EN-MU-RSW---ISMG-Healthcare-WP.ENT&utm_content=Solarwinds-Blog

19 https://www.healthcareinfosecurity.com/breach-victims-piling-up-in-wake-cloud-vendor-attack-a-16307

20 https://www.lookout.com/products/sase/what-is-sase-sase-meaning?utm_source=3PW&utm_medium=OT&utm_campaign=WW-MU-EN-MU-RSW---ISMG-Healthcare-WP.ENT&utm_content

21 Executive order: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

22 Executive order: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

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**.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io