Lookout®

Protecting Critical Data During Healthcare's Transformation

SECURITY CHALLENGES AND SOLUTIONS FROM ENDPOINT TO CLOUD

HEALTHCARE E-BOOK

The consequential transformation of healthcare

Virtual visits transformed the healthcare industry, making preventive care accessible to remote patients online. This change, while beneficial, also meant that millions of healthcare workers and patients who were new to telehealth had to learn how to operate in unfamiliar territory.

Medical practitioners and patients began to meet virtually, using their own smartphones, tablets, laptops and other personal mobile devices while exchanging messages related to sensitive healthcare issues through unfamiliar platforms.

This led to an unprecedented number of personal mobile devices accessing healthcare data in the cloud. There, providers could manage data at scale, adapt faster to change, improve the patient experience, coordinate diagnostic care and treatment and drive operational efficiencies.

It's no longer business as usual. Although some data and apps still remain in on-premises data centers, others – such as electronic personal health information (ePHI), electronic health records (EHRs) and electronic medical records (EMRs) – are moving into the cloud.

But in the cloud, data and apps can be accessed from anywhere using any device, which renders traditional perimeter security ineffective. Now, remote healthcare workers and patients with personal mobile devices and apps converge in the cloud to access data from wherever they want.

But the lofty expectation of instant access to any app or service in the cloud from any device – no matter where you are – is antithetical to security, healthcare data protection and personal privacy.

Healthcare's current transformation agenda

Apps are in the cloud, telehealth visits are common and personal devices are used for remote work. Learn more about the impact on data security.

WATCH THIS ISMG VIDEOCAST →

Table of contents

Healthcare security challenges

Although the cloud offers tremendous benefits, it also has its share of security challenges.

During healthcare's on-premises-to-cloud transformation, IT and security teams remain accountable for protecting confidential data regardless of where it travels, whether it's on an endpoint or in the cloud. This means making sure that personal mobile devices are secure before and while they're connected to your cloud apps and infrastructure.

Why is endpoint security critical to healthcare? Because healthcare professionals are using personal or unmanaged mobile devices to access sensitive data while working outside the organization's perimeter.

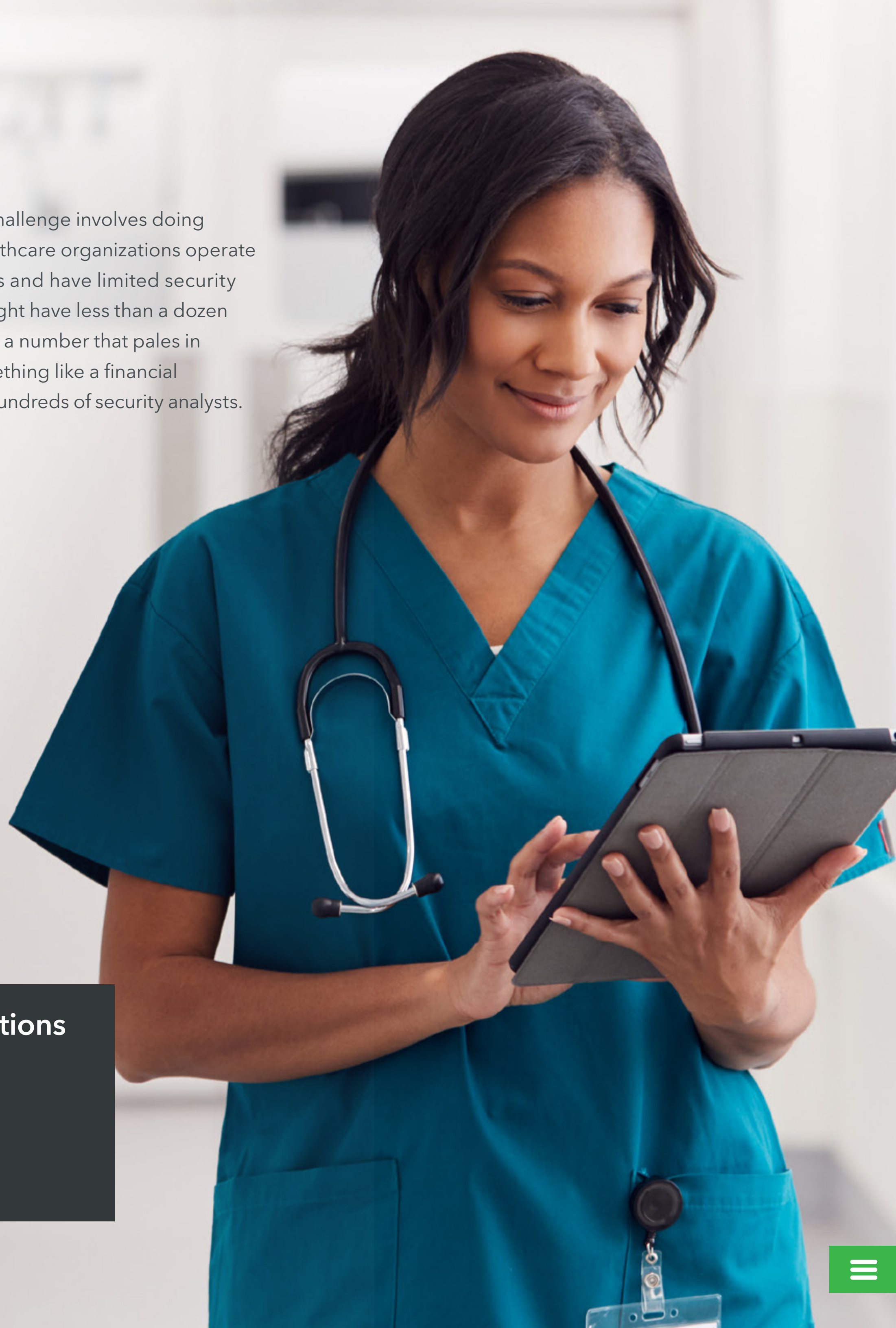
As a result, security teams no longer have visibility into the devices connected to their infrastructure, leaving the organization vulnerable to catastrophic data breaches and ransomware attacks

And then there is the cloud, where it's becoming very easy for any device and any user to connect. This makes it especially important to continuously evaluate the relationship between users, their devices and the data they access to distinguish between acceptable and malicious actions. It's only with an understanding of how your users behave, whether their device is compromised and how data is handled, that you can detect and stop cyber attacks. It's also important to detect unintentional misconfigurations and maintain security guardrails to prevent account compromise.

IT and security teams also assume a major role in identifying, preventing and remediating compliance violations in accordance with HIPAA, GDPR, HITECH, and other data privacy mandates.

Healthcare providers in every state, region and country will require different regulatory compliances, but regardless of location there are always stringent rules that require alignment. This becomes more difficult as data flows more freely between users, networks and devices every day.

Another daunting challenge involves doing more with less. Healthcare organizations operate with lean IT budgets and have limited security resources. Many might have less than a dozen IT security staffers – a number that pales in comparison to something like a financial institution that has hundreds of security analysts.



Protect healthcare data from endpoint to cloud

What's the best way to protect critical data in the aftermath of this healthcare transformation and where do you start? Overcoming security challenges can be daunting, but if you take the right approach it doesn't have to be.

In 2019, Gartner introduced an approach called the Secure Access Service Edge (SASE), a Zero Trust security architecture that addresses healthcare's transformation challenges. A cornerstone of SASE is the integration of multiple security solutions into a single endpoint-to-cloud architecture.

PDF

Visibility into data and threats

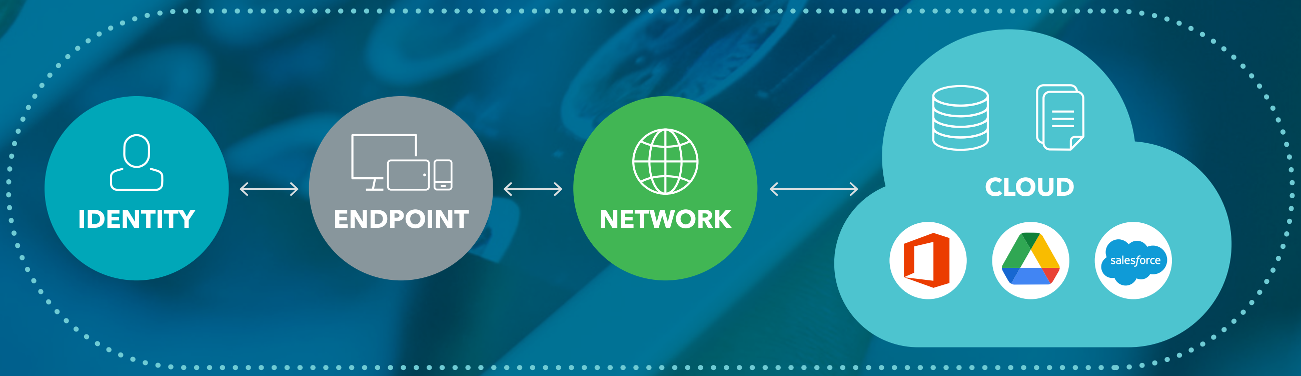
Learn how this healthcare provider secures ePHI and stops malware threats on 8,000 iPads used by its mobile medical team.

READ THE CASE STUDY →

From a healthcare perspective, SASE calls for security delivered in the cloud. Achieving this requires:

1. **Complete visibility.** From unmanaged devices up to the cloud and everything in between. This includes visibility into the unique risk levels of users, devices, apps and data. Visibility also plays a key role in ensuring compliance with data privacy regulations.
2. **Unified insights.** Your security infrastructure should be integrated and delivered by one provider to manage policies, detect cyberthreats and perform conclusive incident investigations. This will give you actionable insights from endpoints to the cloud.
3. **Precise access controls**. To protect data without impeding productivity, it's critical to enforce Zero Trust access that has the intelligence to continuously adapt to changes in user, device, location, and cloud app status and context.

INTEGRATED ENDPOINT-TO-CLOUD SECURITY



Continuously assess mobile device risk

Tablets, smartphones, Chromebooks and other mobile devices are essential to how healthcare professionals and patients manage their work and personal lives. And despite the risk these devices present, they can still connect to and access critical healthcare apps and data just as much as a traditional endpoint.

Mobile users are particularly susceptible to phishing attacks mounted by cybercriminals because of how many ways attacks can be delivered. SMS, email, messaging apps, social media platforms, games, and even dating apps offer attackers the opportunity to socially engineer individuals.

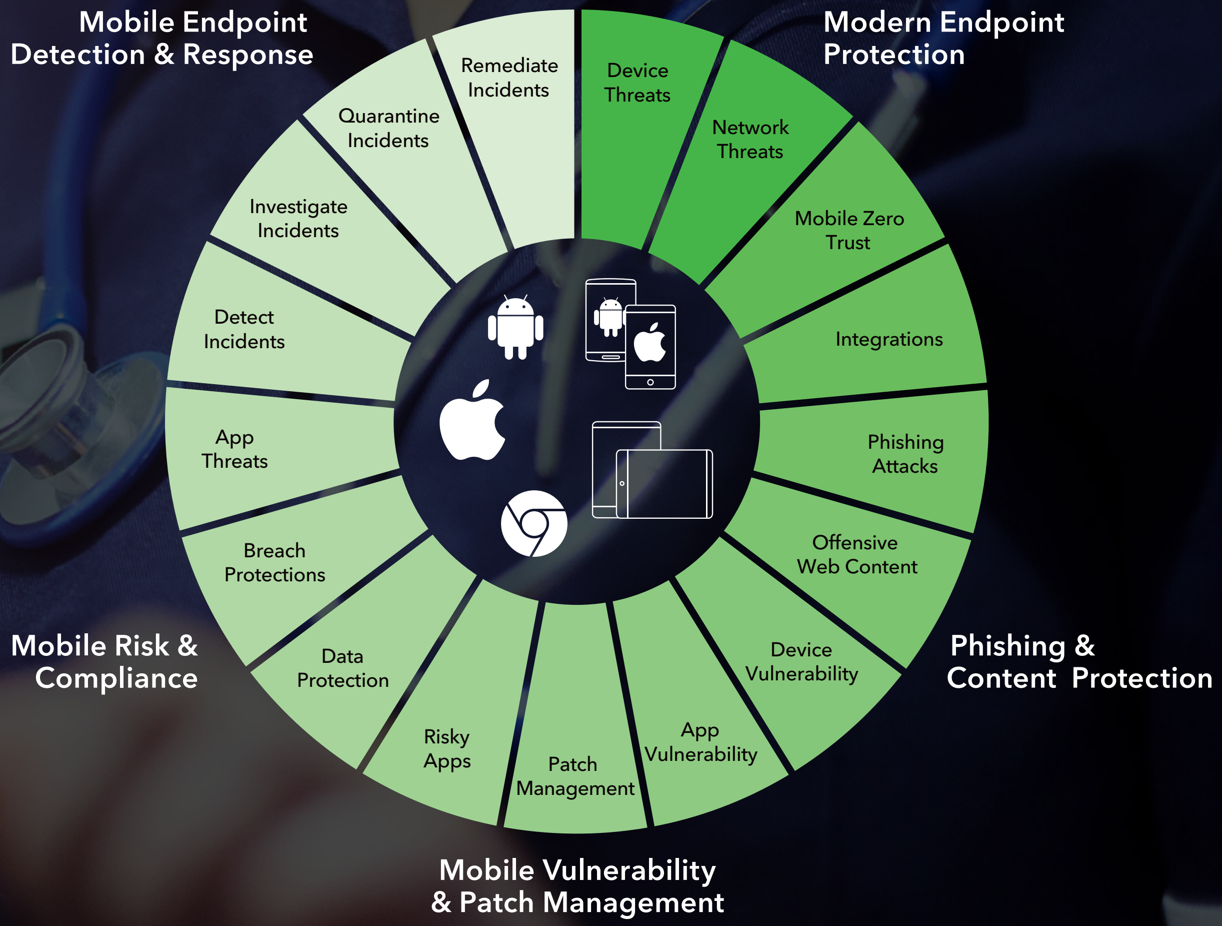
This may lead to stolen credentials that the attacker uses to compromise the organization or launch a ransomware attack. Consequently, mobile devices can represent a vulnerability to your infrastructure if they're not properly secured.

Understanding the risk posture of each mobile device is essential – especially if a personal device can be used to access patient data.

Identifying risky data access and transfer permissions, malware and other mobile threats is critical to HIPAA compliance. To align, organizations must have steps in place to prevent these threats, report data compromise and breach incidents.

You can maintain a strong security posture by continuously assessing the risk levels of all mobile devices and apps. It is ideal to do this before they access any part of the infrastructure and continue to do so for the duration of the connection.

If done right, mobile devices and apps can also be incredibly helpful by providing rich telemetry data that can be analyzed using machine intelligence. The results enable teams to quickly detect and investigate potential threat behaviors and understand if an active attack involves mobile devices, where the attacker is and what they are doing. Organizations that can integrate mobile data with their other security insights are able to bring light to a massive blind spot in their incident investigation and threat hunting efforts.



The critical role of mobile device and app risk assessment in endpoint-to-cloud security

Preventing data compromise on mobile devices

How did one of the largest U.S. healthcare systems reduce the risk of malware and data leakage from non-compliant mobile device apps?

READ THE CASE STUDY →

Understand behaviors and mitigate exposure

Some of the most critical threats you will encounter won't start with malware deployment. Instead, cyber attackers look to compromise accounts and behave like users to remain undetected.

So, whether you are defending against ransomware or insider threats, you need awareness of what's going on with your users and their accounts. That's why it's essential to have a baseline of how your healthcare employees typically behave when they access apps and data.

A cloud access security broker (CASB) provides user and entity behavior analytics (UEBA) that make it easier to understand behavioral disparities and determine if they're indicative of a cyberattack, a malicious insider or an unintentional action.

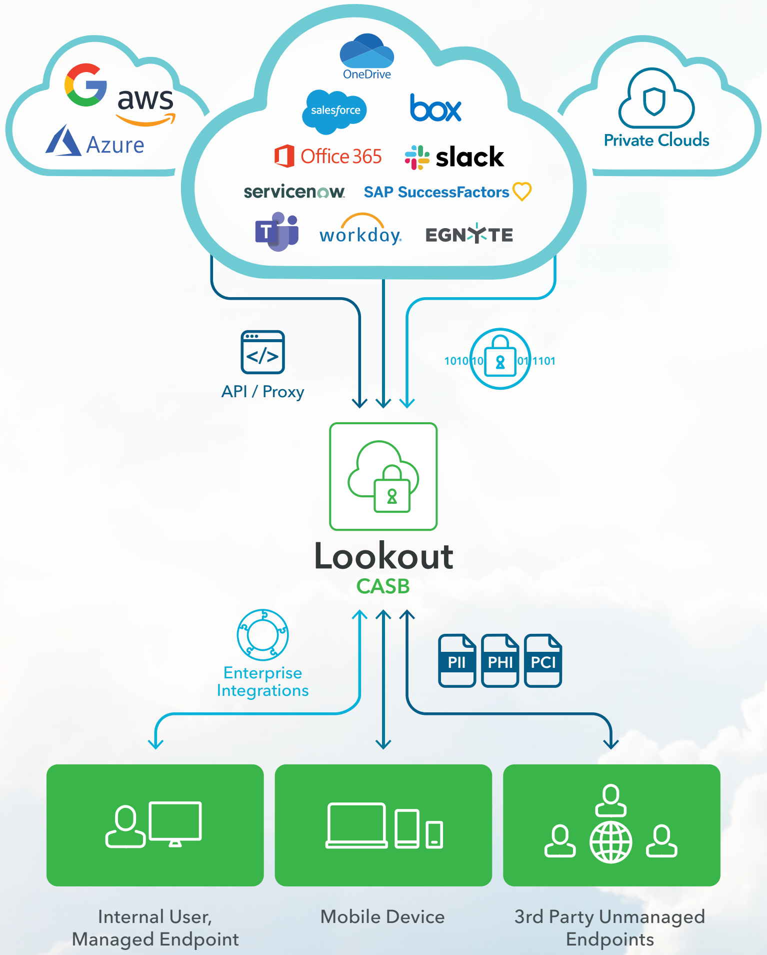
Threat indicators may include excessive file downloads, multiple unsuccessful login attempts, and logins from new or restricted locations. These behaviors often indicate a compromised account that adversaries are using to move laterally, locate valuable data and steal ePHI, EHR and EMR.

Just like any other technology that processes and stores your data, you need to understand the risks involved.

Threat actors are always looking for new ways to infiltrate your infrastructure, including ways to exploit SaaS apps.

CASB can give you visibility into the security posture of the cloud infrastructure and apps that your healthcare system relies on. Cloud security posture management (CSPM) and software-as-a-service security posture management (SSPM) capabilities call out SaaS and IaaS misconfigurations that could be the vulnerable point in your infrastructure that threat actors take advantage of.

It's also important to identify and mitigate healthcare data exposure in the cloud, unwittingly caused by shadow IT. With everyone working away from the office, it's easy for employees to onboard software that isn't approved by IT. Again, CASB provides you with the visibility to expose unauthorized shadow IT apps and services that may cause unintentional exposure. It integrates with wired and mobile devices, firewalls and proxy services to monitor healthcare cloud services to assess usage and vulnerabilities.



The importance of understanding user behaviors and mitigating exposure to ensure endpoint-to-cloud security

Major hospital group protects data in the cloud

Learn how one of the world's largest private operators of healthcare facilities secures SaaS apps and services in the cloud.

READ THE CASE STUDY →

Manage and enforce precise access controls

CASB is critical in securing your entire cloud environment, but that's only one part of your healthcare organization's attack surface.

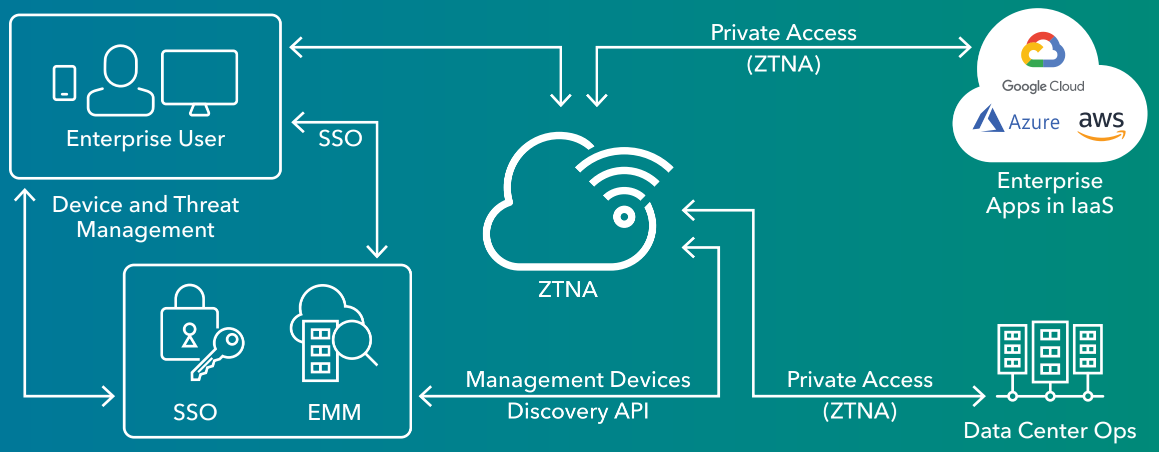
Many healthcare providers require some apps to run in a data center or private cloud infrastructure. In fact, IDG says that most IT decision-makers believe apps that come in contact with critical data must be on-premises.

To ensure your Zero Trust architecture provides comprehensive protection, you need integrated controls from endpoint to cloud that mitigate and continuously monitor risk for your on-premises apps and endpoint devices. This should provide you with the same level of security and control over on-premises apps as it does in the cloud.

A cornerstone of endpoint-to-cloud security, Zero Trust Network Access (ZTNA) empowers you to enforce granular access controls across your entire security infrastructure with parity between cloud and on-premises services. This provides unified data control and mitigates the risk of an unauthorized data transfer outside your perimeter.

Unlike VPNs that allow unfettered access, ZTNA leverages identity- and context-aware access policies based on user and device risk levels. This helps stop malicious actors who continuously seek out weak points in the infrastructure to gain unauthorized access to vital compliance-related data such as ePHI and EHRs.

By understanding what your users need, ZTNA provides only the necessary access, preventing cyberattacks from spreading throughout your infrastructure. If bad actors control mobile devices or possess stolen account credentials, ZTNA can help prevent them from moving laterally to attack adjacent clouds that store healthcare data. It also works with multi-factor authentication and other identity solutions to strengthen access controls to on-premise legacy software.



The critical role of ZTNA in cloud-delivered security for healthcare

Healthcare security in the age of 5G and remote work

More unmanaged devices will use 5G networks for telehealth because it will likely be faster than a healthcare provider's Wi-Fi.

CHECK OUT THE BLOG AND PODCAST →

Advanced healthcare data protection

Although most cloud apps feature onboard security controls, healthcare organizations still require dedicated data loss prevention (DLP) capabilities that provide advanced, well-orchestrated protection to support complex use cases across multiple platforms and understand the types of healthcare data you have.

DLP policies enable you to consistently detect, classify and encrypt confidential healthcare data in emails, instant messages and other communication apps. It understands every type of data you have and classifies ePHI, EHR, EMR and other critical health information based on their importance and confidentiality. This includes data in motion, in use on a device and at rest in the cloud.

Integrated with CASB and requiring no software agents, DLP provides healthcare data matching, document fingerprinting, analysis of structured and unstructured data and protects against sharing offline information and files with unauthorized users.

To eliminate exposure, DLP scans historical data in cloud apps to discover unprotected information and open file shares.

You can also audit cloud data to identify sensitive information related to ePHI, EHR, EMR, HIPAA, GDPR, and PCI and enforce remediation to preserve data integrity and compliance.

The hidden risks of VPNs

Using VPNs to access cloud apps is like siphoning gasoline through a hose. It's all or nothing and consuming it has ill effects.

CHECK OUT THIS VPN INFOGRAPHIC →

CONCLUSION

Unified endpoint-to-cloud security for healthcare data

Without the perimeter you used to have, visibility and control over healthcare data across users, devices, networks and cloud services are lacking. You need a unified endpoint-to-cloud security platform that aligns with SASE to securely streamline healthcare operations and minimize business risk.

Integrated endpoint-to-cloud security continuously assesses mobile device risks, understands behaviors and mitigates exposure, provides dynamic access controls and offers advanced protection for healthcare data.

This modern Zero Trust approach to security protects your healthcare data from endpoint to the cloud.

It provides visibility into the risk levels of users, devices and apps; unified insights into malicious behaviors, threats and vulnerabilities; and precise access controls that adapt to ongoing changes in healthcare's transformation.

Four reasons to embed healthcare app security

Embedding security in healthcare apps protects against malware and cyberthreats while safeguarding the ePHI entrusted to you.

GET THIS IMPORTANT INFOGRAPHIC →

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.

Learn more

Protect your healthcare practice from endpoint to cloud with Lookout Solutions for Healthcare organizations

LOOKOUT.COM/SOLUTIONS/HEALTHCARE →