CLEARDATA™

CSPM: The Solution to Healthcare's Biggest Cloud Threats

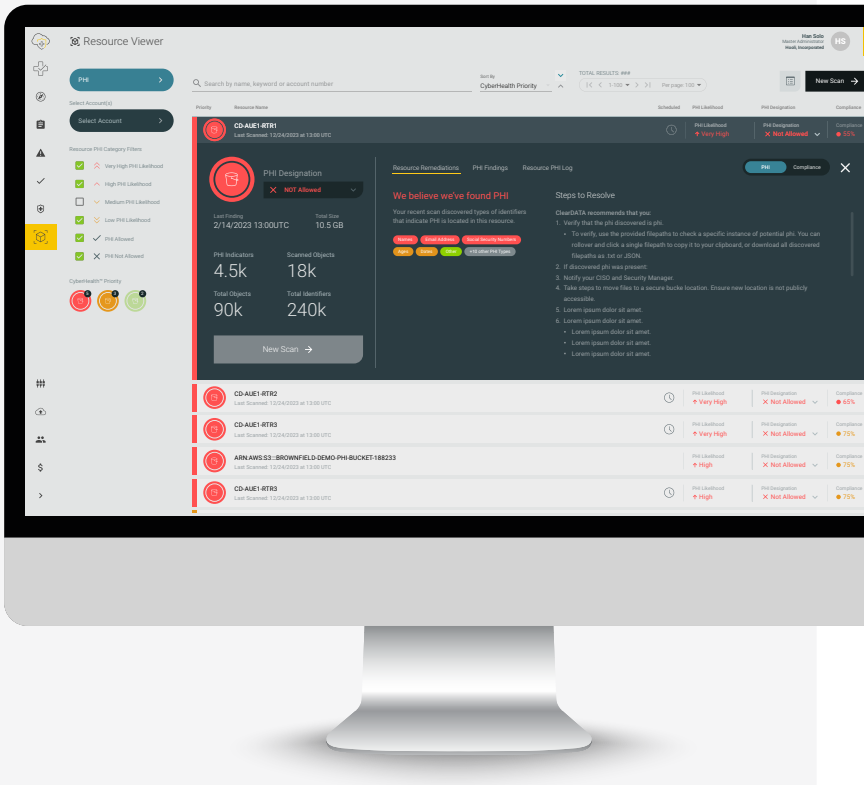
Chances are you're among the 73% of healthcare organizations that have embraced the cloud in recent years. And while you've gained many advantages by doing so, moving to the cloud has exposed you to the biggest threat in cloud security: cloud misconfigurations.

Errors in cloud security configuration expose you to the risk of a breach, which costs healthcare organizations an average of $11 million and can result in significant reputational harm.

To avoid this risk, you need the right **cloud security posture management (CSPM)** solution—a set of tools, practices and processes designed to help organizations ensure the security and compliance of their cloud environments. CSPM solutions continually monitor cloud configurations to detect vulnerabilities and other security risks and protect you by eliminating these vulnerabilities. However, not all CSPM solutions have the right capabilities for healthcare organizations.

So, what CSPM solution should you choose? And what CSPM features are critical for the healthcare sector?

In this guide, we share key attributes you should prioritize in a solution.



▶ YOU NEED
A healthcare expert

Any old CSPM solution won't do. Healthcare has its own unique challenges and regulatory requirements—which is why you need a CSPM built by healthcare experts. A CSPM provider experienced in healthcare understands the nuances of healthcare laws and regulations—especially those related to protected health information (PHI)—and can tailor their solutions to address industry-specific compliance and security needs.

You also need a partner who is certified by the Health Information Trust Alliance (HITRUST) and can help you implement HITRUST's common security framework (CSF). As the gold standard for healthcare cloud security, the CSF incorporates all the healthcare laws and regulations governing healthcare information security as well as other information security best practices.

If your partner is not HITRUST certified or an expert in the healthcare sector's cloud security needs, they might leave open access points that expose your organization to hackers.

HITRUST CSF Certified · HIPAA COMPLIANT · GDPR COMPLIANT · GxP Pharma Solutions · ITIL · AICPA SOC · NIST · CIS SecureSuite Membership

YOU NEED

A CSPM solution powered by a policy-as-code engine

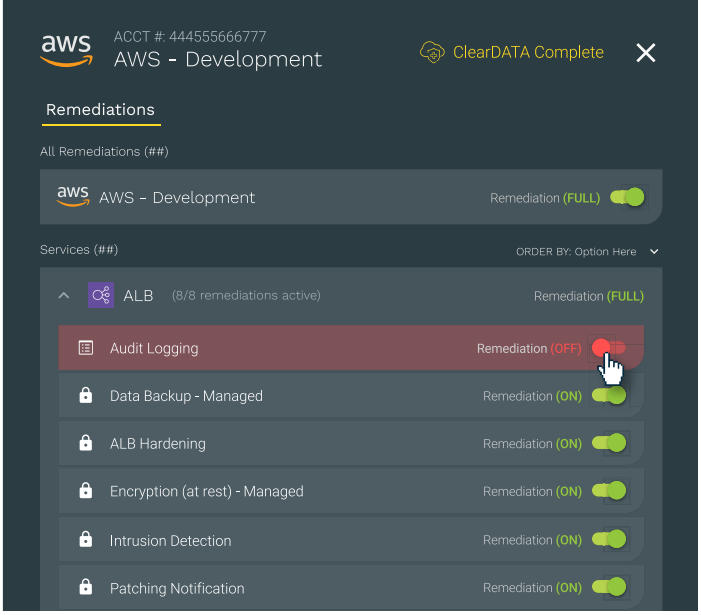
Because a CSPM purpose built for the healthcare industry must comply with many laws and should meet the HITRUST CSF, you want to choose a CSPM with a policy-as-code engine. This kind of engine translates the many rules, policies, and best practices around healthcare cloud security into specific code. That code then operates to first configure your cloud settings correctly and then to monitor and update the settings as needed.

That is, getting your cloud configurations right isn't a once-and-done process. There are continually new developments, whether in the regulations or your cloud services, that require updates to your configurations. Moreover, any time you add new elements to your cloud infrastructure, your CSPM has to set and monitor new security configurations.

Moreover, the CSF and the various healthcare laws around PHI are not the only policies that must be captured by the policy-as-code engine of your CSPM. You want an engine that is also continuously updated with additional information, including:

- New privacy regulations
- Regulatory enforcement actions
- Insurance settlements relating to data security events
- New standards from the National Institute of Standards and Technology (NIST)
- Changes in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud
- Real threat data experienced by the healthcare industry

Any of these changes may require new code to update your cloud configurations to preserve their security.



YOU NEED

A solution with guided and automated remediation

Just as important as the completeness of your policy-as-code engine is, your CSPM should also correct any problems or incorrect settings it encounters. For example, when your cloud service makes updates, you don't want a solution that merely identifies an issue, leaving your team to fix it.

You instead want the solution to move rapidly to make any needed changes so that there isn't a gap in security for hours or even days while you wait for your team to make updates. Large enterprises take an average of 88 days to fix misconfigurations after discovery. In healthcare cloud security, where every second counts, automated remediation can be the difference between a breach and a protected environment.

In fact, an experiment by researchers found that a fake cloud database was attacked within minutes of being indexed by search engines used by attackers. Over the course of the 12-day experiment, the database was attacked 175 times. Results like these show that bad actors are continually probing for vulnerabilities. They use automations that scan the entire internet for cloud misconfigurations. If your remediation process takes hours or even a week, as it did for this company, chances are your data will be compromised.

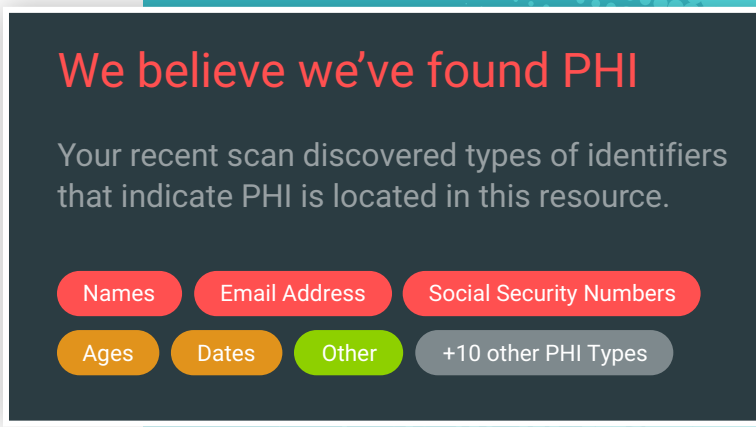
You're protecting patient data, so you need to move extremely fast. That means you need CSPM software that will give your team compliance assessment results within 24 hours, and the ability to choose how you want and need to remediate — with either guided or automated remediation — to speed up the process of fixing misconfigurations and vastly improving your compliance posture.

▶ YOU NEED

The ability to locate PHI with clear guidance

Most CSPM solutions stop at monitoring and protecting your cloud configurations—in effect, securing your perimeter. And while having a secure perimeter is critical, of course, you likely care about more than just that. You likely also want to know where exactly your PHI is and where it's going.

For that reason, you want a CSPM solution that can locate PHI. A CSPM solution with sensitive data governance can help healthcare organizations identify potential security threats and take immediate action to remediate them, thereby reducing the risk of data breaches. If a breach does occur, having a record of how PHI was accessed and handled can help expedite the response process. Identifying and tracking PHI will also help during any necessary data audits. By having a record of where PHI is stored, who has access to it, and how it is managed, organizations can provide concrete evidence of their compliance efforts.



This capability also ensures that you can visualize where PHI resides and provides clear governance you can act on quickly. With sensitive data governance, you can remediate potential risks that can lead to PHI leaks. For example, without the ability to locate PHI, a healthcare organization might not realize that it's storing PHI in a particular container and fail to set the right security configurations for that container. Without the right security settings, your organization is at risk of a breach.

There's only **ONE** solution with these capabilities for healthcare

Only one solution on the market has all the above attributes. ClearDATA's CyberHealth™ Platform is a proven, HITRUST-certified, healthcare-specific CSPM solution that automates continuous cloud security while also enabling your organization to locate and track its PHI. Moreover, it is the only security and compliance cloud solution purpose-built for healthcare.

CLEARDATA™

ClearDATA.com | (833) 99-CLEAR

How can ClearDATA help protect your PHI in the cloud?

With our CyberHealth Platform, now available as software-only or with ClearDATA managed services, the best-fit choice for security and compliance protection in the public cloud is all yours.

Request a Consultation

©2023 ClearDATA
MKT-0116 Rev. A, October 2023