elastic | CLEARDATA

SUCCESS STORY

ClearDATA boosts healthcare cloud security with Elastic

ClearDATA deploys Elastic Security to help healthcare customers migrate to the cloud, protect patient data, and comply with regulatory standards.

Region
United States

Industry
Software & Technology

Solution
Elastic Security

Reduces investigation times by more than 50%

- With the deployment of Elastic Security, ClearDATA reduced average incident investigation times from up to eight hours to as little as two hours.

Reduces the storage hardware costs

- Searchable snapshots in Elastic help ClearDATA comply with data archiving standards while reducing dependency on costly hot storage.

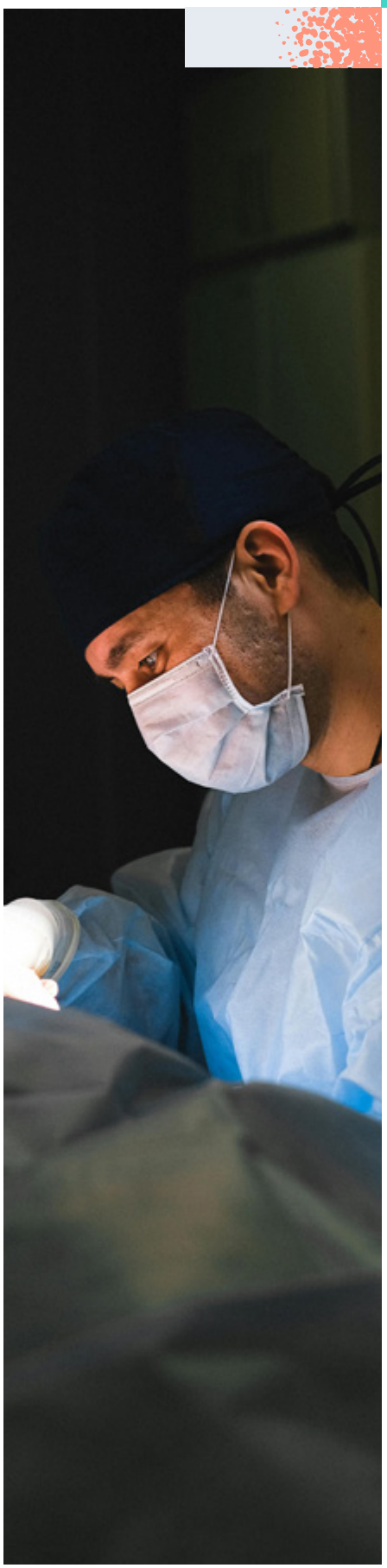
Increases capacity of security team

- ClearDATA's security team is better prepared to protect a fast-growing customer base thanks to simplified and streamlined processes in Elastic.

Cloud computing offers many advantages for healthcare organizations, such as more scalable and flexible infrastructure to support innovation and lower costs by shifting toward OpEx models. Given the stringent regulatory standards for healthcare, including HIPAA and GDPR, as well as the general need to protect patients from cyber threats, the move to the Cloud can be daunting to say the least.

Many healthcare organizations partner with security and compliance specialists to manage their cloud migration and mitigate risk. ClearDATA is one of the leading providers in this space. Its HIPAA- and HITRUST-compliant cloud computing platform is explicitly designed for healthcare organizations who want to migrate their IT infrastructure.

John Whetstone, Vice President of Managed Cybersecurity Services, ClearDATA, says, “We know the healthcare industry inside out and how best to provide security, compliance, and protection all in one place.” This includes four key services for customers moving to a cloud environment: managed detection and response (MDR), a specialized cyber threat intelligence program for healthcare, vulnerability management, and a team that manages backend infrastructure.



Moving to a unified cloud security solution

Previously, ClearDATA used a mix of disparate solutions to deliver a secure cloud environment including endpoint security, cloud workload protection, vulnerability detection, and a managed SIEM. The sprawling inventory of varied security tools hindered efficiency, drove up costs, and could even be viewed as a security risk given the lack of consistency.

“It took a lot of effort to pull these elements together,” says Whetstone. “We were definitely in the market for a unified solution to integrate or replace our incumbent security tools.”

When he researched the latest version of Elastic Security, Whetstone realized that he could achieve this goal and provide ClearDATA customers with a future-proofed cloud SIEM environment. “We made the strategic decision to go with Elastic for extended detection and response (XDR). It meant that

we could move away from multiple vendors while gaining full visibility of our cloud environments and the endpoints that we needed to cover."

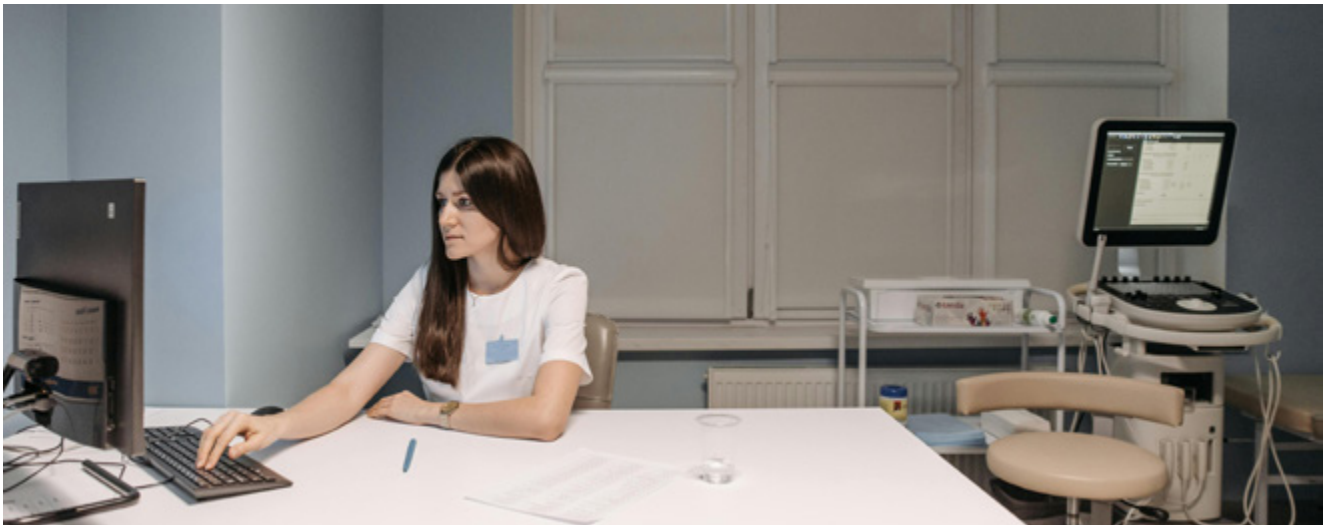
Elastic Agent plays a central role in ClearDATA's deployment, offering a single, consistent method for connecting multiple data sources to the Elastic Stack. "It is now a lot easier to add monitoring to our infrastructure, including endpoint data from Elastic Defend, cloud-native telemetry data, and data from other cybersecurity solutions such as our own external attack surface monitoring tool. All of this connects back to our ClearDATA CyberHealth PlatformTM," says Whetstone.

A clear view of security through a single pane of glass

With a unified monitoring system in place, the ClearDATA team can now visualize and track events from a 'single pane of glass'. "The team can switch between browser tabs to understand what has happened on a given machine, the attack surface, and all the potential outcomes. Putting this information in one place boosts confidence and accelerates our incident response times," says Whetstone.

> There's no comparison between Elastic and our previous security vendors. In the past it used to take an average of six to eight hours to conduct a proper investigation. We cut that down to two to three hours within the first two weeks of bringing Elastic online.

John Whetstone
Vice President of Managed Cybersecurity Services
ClearDATA



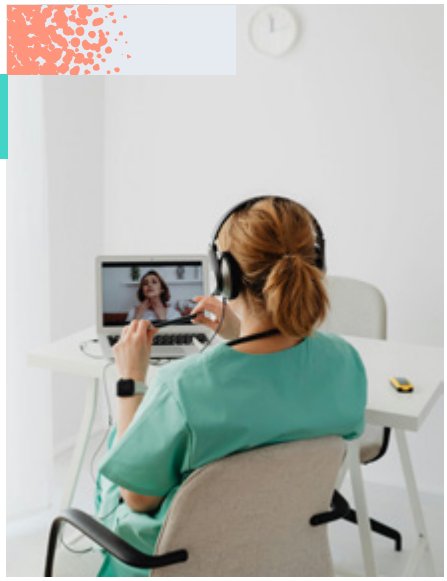
Reducing threats, boosting confidence

Elastic Security, thanks to its searchable snapshots feature, enables ClearDATA to comply with data retention standards while reducing the cost of storage. “In the past, we kept our data on expensive hot cloud storage. With Elastic, the snapshots are essentially our archive function. That’s a major benefit in terms of being able to maintain compliance on behalf of our customers while reducing our reliance on costly long-term storage,” says Whetstone.

Whetstone also sees an opportunity to grow ClearDATA’s business model by charging for services as well as licenses. “We are now in a position where we can look at chargeback mechanisms for customers related to data ingestion. That means our security team went from being a cost center to a profit center, which is a great place to be,” he says.

Simplifying and streamlining processes also increases the capacity of the security team. “There are just 11 of us servicing more than 200 customers. One of the biggest wins is that Elastic enables us to ramp up our activities at scale,” says Whetstone.

Looking to the future, Whetstone wants to integrate additional data sources using Elastic Agent. He also sees the potential of Elastic machine learning to analyze data and generate models for threatening patterns of behavior. “Even today we’re still discovering new features in Elastic Security such as Data Exfiltration Detection, which alerts us to abnormal volumes of data transfer,” says Whetstone.



> This isn’t just a security play. In the long term, Elastic Security becomes a business accelerant, enabling us to expand our business with existing customers and reach new markets. It’s been huge for us.

John Whetstone
Vice President of Managed Cybersecurity Services, ClearDATA

Address complex threats with Elastic Security, built on the Elastic Search AI Platform, to streamline SecOps.

Learn more

elastic