JupiterOne

CASE STUDY

How Codoxo Tackles Compliance on a Tight Budget

CODOXO

Codoxo is the premier provider of AI-driven applications that help healthcare companies and agencies identify and act to reduce risks from fraud, waste, and abuse. Codoxo's Healthcare Integrity Suite helps clients reduce risks and costs across network management, clinical care, provider education, payment integrity, and special investigation units. The SaaS applications are built on their Forensic AI Platform, which identifies problems and suspicious behavior earlier than traditional techniques.

How Codoxo Tackles Compliance on a Tight Budget

Faced with compliance requirements and a brand new cybersecurity program, Codoxo Head of Security Witt Cunningham needed to become compliant at a price point suitable to their business size and available resources. Codoxo, formerly Fraudscope, recognized the breadth of JupiterOne and not only became healthcare compliant, but also built their future security program components using the JupiterOne platform.

Codoxo achieved improved security program maturity, cyber asset visibility, and security governance at a fraction of the cost of traditional security tooling.

Prior to using JupiterOne, Codoxo took six months to become SOC 2 compliant. By contrast, they achieved a rigorous healthcare certification in two months using JupiterOne.

Over half of the analysis and evidences required by the healthcare certification were gathered automatically and continuously with the JupiterOne platform.

Codoxo has since expanded their overall cyber security program by leveraging the JupiterOne platform. What started as primarily a compliance use case has now expanded into architecture, cloud management, and even developer-centric use cases.

Challenges

Needed a scalable compliance solution to achieve business critical SOC 2 compliance and health certification

Limited compliance budget and timeline to achieve results

Results

Achieved SOC 2 compliance in < 6 months

Became healthcare compliance in <2 months

Created a centralized view for the entire DevSecOps team to take action

Automated more than 50% of analysis and evidence gathering

Key Integrations

- AWS
- Qualys
- Knowbe4
- Jira
- Jamf
- Snyk

> “I couldn’t believe all of the integrations and data points that were incorporated into JupiterOne that I previously had to find in a makeshift way.”

Witt Cunningham, Head of Security at Codoxo

Stopping Healthcare Fraud Cold

Codoxo is an Atlanta, Georgia based insurance and healthcare startup launched from a PhD project at Georgia Tech. In 2017, founder and CEO Musheer Ahmed began building the AI-based SaaS platform to detect fraud, waste, and abuse within medical claims. Codoxo gives organizations the tools to quickly identify suspicious claims, collect actionable information, and collaborate across the organization to open, investigate, and resolve cases quickly. Since Codoxo sells to insurance and healthcare providers, the head of security, Witt Cunningham was tasked with ensuring compliance and privacy of their customers' data. As you might expect, this was not an easy task.

Compliance Isn't Cheap

Witt joined Codoxo in July 2018, just one year after the business was established. Like any freshly hired security leader, Witt needed to build out the Codoxo security program starting from a base of essentially zero. It took Witt and the Codoxo team approximately six months to tackle their first major project, a SOC 2 compliance audit. The project was expensive, resource intensive, and difficult to manage, delaying other security requirements due to the lack of resources.

Half of security is knowing what's in your environment and knowing what you have to secure. Witt determined that it's difficult and expensive to manually audit the security and technology infrastructure continuously for security governance needs. Not only is cyber asset visibility critical to the success of any security initiative, understanding the correlations between the cyber assets is what makes it possible to identify real risk. Witt and the Codoxo team were unable to cover the breadth of knowledge or dedicate the time required to achieve the goals of compliance, security visibility, and governance.

Traditional asset management tools and Governance, Risk and Compliance (GRC) solutions are expensive and unwieldy. A huge GRC platform would have been overwhelming to the Codoxo organization, both in price and operational overhead. And to top it all off, they needed to tackle an ever larger certification – healthcare compliance.

> **This is the best solution to meeting a DevSecOps requirement that I have seen to date.**

Enter JupiterOne

Facing another long and arduous certification process, Witt's luck turned when he met JupiterOne CEO Erkang Zheng at a conference. After a pitch and demo from the JupiterOne founder, Witt was impressed enough to give it a shot.

"I couldn't believe all of the integrations and data points that were incorporated into JupiterOne that I previously had to find in a makeshift way. There are tons of separate products to review to get just one healthcare compliance control locked in. Based on JupiterOne's technical capabilities I was able to formulate my results based on an easy to use query language. I was impressed with how

Key Results and Benefits with JupiterOne

6mos

Achieved SOC2 compliance in < 6 months

of evidence and analysis were automated and continuously gathered

of all controls assessments based on evidences pulled from JupiterOne

Became healthcare compliant in less than 2 months

it flowed, how it met our needs, and the fact that it was affordable."

Today, Witt uses JupiterOne as a modern GRC solution. JupiterOne met the Codoxo needs at a price that was acceptable to the leadership of the young startup. Specifically, Witt found significant value in the policies and procedures components of the JupiterOne solution.

"I've updated our policies and procedures multiple times over the last couple of years to help ensure compliance within complex industries like healthcare and government. As a born-in-the-cloud organization, it became challenging to comply with regulations written for a traditional, on-premise environment. J1 has created an impressive Policy and Procedure feature that is SaaS-oriented and easy to consume and use."

JupiterOne Grows for the Future

With JupiterOne in his corner, Witt was able to become healthcare compliant in two months. The key for speed was the fact that over 50% of all controls assessments were based on evidences pulled from JupiterOne. Codoxo had over 500 controls in their first pass. The ease of integration for just one infrastructure system (AWS) gave Witt insight into most of the controls he needed for the healthcare compliance.

Witt was able to quickly query cyber assets, pull graph views, and provide correlations that he could give to his auditing team. Within two months, largely based on the JupiterOne platform, Codoxo achieved healthcare certification. Without JupiterOne, this process would have taken at least 8-10 months using an enterprise-grade GRC and asset management system Codoxo could not afford, just to get something usable to submit for complete healthcare compliance.

Security is a never ending journey. Witt and Codoxo are continuing to walk that journey as they move forward the maturity of their cybersecurity program. "JupiterOne has quickly become a cornerstone product in our security arsenal." says Witt. Most recently, Witt added the ability to have every user in Codoxo log into JupiterOne. Developers, security engineers, and others now all have the ability to make queries against the JupiterOne cyber asset governance system. What started as primarily a compliance use case has now expanded into architecture, cloud management, and developer-centric use cases.

"This is the first product that I can actually show DevSecOps results. I can go through a DevSecOps launch, see all of the parts to the stack, are they encrypted, have they been vulnerability scanned, do they have patches, who has access to what...all from a centralized point of view. This is the best solution to meeting a DevSecOps requirement that I have seen to date."

JupiterOne is your security operations central command. Whether you're an established enterprise, or a budding startup, our cloud-native cyber asset management, visibility, and security platform empowers customers to centralize security operations, streamline processes, and drastically reduce enterprise risk.