sysdig | IMMUTA

CUSTOMER STORY

Immuta Engineers Cutting-Edge Security with Sysdig

As the market leader in cloud data governance, Immuta provides a universal platform through which data engineering and operations teams can control access to cloud-based analytical data sets. Through its unique approach to data security, Immuta helps clients not only simplify policies but also improve data utilization. The company works with businesses across multiple high-security industries, including financial services, healthcare, and the public sector.

Some of Immuta's customers include Sony, Swedbank, Thomson Reuters, the Mercedes-Benz Group, and the United States Air Force.

IMMUTA®

INDUSTRY

Software Technology

CHALLENGES

- Inability to detect and respond to risks and threats across cloud environments
- Must meet governance and compliance standards required by customers in high-security industries
- Difficulty prioritizing risks due to excessive noise and false positives
- Insufficient visibility into the Kubernetes environment

OUTCOMES

- Refined vulnerability management policy to improve both efficiency and security
- Achieved SOC2 and ISO270001 certifications; currently working toward PCI-DSS compliance
- Enabled seamless migration to AWS Bottlerocket, eliminating the need for Immuta to maintain its own 'gold' image, saving 8-12 hours per month
- Implemented a continuous feedback loop to ensure 100% policy compliance of containers prior to deployment

CHALLENGES

Engineering a Better Approach to Security

Immuta's software as a service (SaaS) platform secures credentials used to access highly sensitive data, a product that caters to clients in regulated industries. Since its inception, Immuta has prioritized security, beginning with its engineering team. The Site Reliability Engineering (SRE) team at Immuta forms the cornerstone of its security strategy, driving infrastructure and tooling decisions.

"As a CISO, it's rare to have a team that proactively drives initiatives as much as our SREs do," explained Mike Scott, CISO at Immuta. "They do a lot of heavy lifting for us. Our focus is on making their management and consumption tasks easier, which ultimately benefits our entire operation."

Early on, Immuta used a legacy security provider with network roots that initially worked well enough, but its weaknesses became increasingly clear as the company grew. The platform was not only expensive and lacking in support, but also left gaps in prioritization, vulnerability exposure, runtime threat detection, and forensics.

"Vulnerability management and runtime protection data was very hard for us to consume," Scott said. "The tool was difficult to configure and tune, customization was limited and often required bouncing between tabs and interfaces, resulting in thousands of false positives. We couldn't prioritize remediations effectively without significant manual effort, nor did we have a good way to demonstrate compliance; pulling data out of the tool was incredibly difficult."

These challenges were compounded by Immuta's highly ephemeral Kubernetes environment. The legacy tool attempted to address this by bolting an acquired solution onto an existing toolset, but the process was far from seamless. This highlighted the need for a partner with deep Kubernetes and cloud-native roots.

> "Few providers excel in detection and response for AWS Kubernetes, and many don't even offer preventative features. Sysdig stands out by understanding crucial aspects that their competitors miss."
>
> **Mike Scott**
> CISO, Immuta

CHALLENGES

"Kubernetes wasn't inherently designed for security, and legacy toolsets support for it was limited," Scott said. "This wasn't a concern when our software was customer self-managed and hosted on-premises. Our customers could deploy our containers behind a DMZ and leverage their existing security infrastructure to monitor and secure them. We knew this would change with our transition to SaaS."

"Our previous vendor struggled with several critical aspects of Kubernetes," he continued. "Our SRE team faced significant challenges in tuning and managing the environment due to limitations in the toolset not tailored for a Kubernetes environment. This resulted in gaps in reporting and visibility."

In order to detect, prioritize, and respond to risks and threats across its ecosystem, Immuta needed to find a new security platform. Its existing vendor simply could not provide the necessary visibility, response, and reporting capabilities. With this in mind, Immuta began its search. It quickly ran into legacy tools selling their spin on cloud detection and response.

> "When I log into Sysdig, it just makes sense. It's improved my understanding as a CISO and helped bridge the gap in language between the security and SRE teams."
>
> **Mike Scott**
> CISO, Immuta

EDR ≠ CDR

"We didn't want to buy an endpoint tool and a posture tool," recalled Scott. "We wanted to buy something more comprehensive. We needed high-speed transactions, security, and compliance that didn't impede anyone's workflows. In addition, we also aimed to find a tool that would allow us to control ongoing costs without compromising our security posture by reducing the number of vendors and interfaces the team needs to use and manage."

According to Scott, this was not something Immuta could find with on-premises native solutions, such as endpoint detection and response (EDR).

CHALLENGES

Visibility into cloud-native services was necessary for full context. On-prem tools typically struggled with machine identity, resulting in numerous orphaned findings. These tools also didn't always keep pace with the rapid evolution of the cloud and the security offerings provided by cloud solution providers.

Eventually, Immuta's SRE team landed on **Sysdig**.

"We saw the capabilities and were immediately confident that this was what we were looking for," said Matt Williams, Engineering Manager, SRE at Immuta. "Two features that got us really excited were in-use vulnerability detection and configurable runtime detection. The 'in-use' vulnerability detection has been a huge win for the SRE and Security teams at Immuta. It has allowed the teams to focus on exploitable vulnerabilities and not code snippets that cannot be executed or modified within the containers themselves. The feature has saved hours of triage and manual analysis and led to a significant improvement in our remediation efforts."

The decision to adopt Sysdig was not simply about replacing Immuta's existing tooling, but about making the new solution easier to adopt for its engineering team.

Within one month, Immuta had Sysdig fully implemented across all hosts.

By focusing on enabling a cloud-engineer centric toolset, Immuta saw a quicker time to value. "Sysdig's usability and support has allowed us to exceed our needs and move on to creating real value for the team at Immuta, and for our customers," said Scott.

> "With our previous tool, extracting data to demonstrate policy compliance was nearly impossible due to its complexity. Sysdig, however, enables us to generate reports with just a few clicks."
>
> **Matt Williams**
> Engineering Manager, SRE, Immuta

SOLUTIONS

No More Noise

Over the first six months of its deployment, Immuta's SRE and security teams worked together to reduce the number of security findings in their environment from 20,000 to 3,000 — the latter being a normal state of affairs. They have also eliminated thousands of irrelevant security notifications and false positives.

"From an analyst perspective, Sysdig has been instrumental in proactively managing vulnerabilities and alerts," Scott said. "Our SRE team can tune rules in a meaningful way that engages my team effectively. When we pull up Sysdig, we typically have fewer than 200 alerts."

Prior to deployment, multiple teams would have had to review these findings to make them actionable. With Sysdig, this is no longer the case.

Slack integration has also been a big positive for Immuta, as it makes triaging much simpler. Sysdig's prioritization and features, such as risk ranking, also give the security team a better view of issues, allowing them to manage high- and critical-level risks while also reducing administrative overhead.

> "SREs and security professionals often speak different languages. Sysdig has empowered us to be proactive and bridge the gap in the language we speak. We're now having more productive discussions, allowing us to focus on driving innovation."
>
> **Mike Scott**
> CISO, Immuta

"Sysdig Secure goes beyond mere vulnerability detection and actionable insights," Scott elaborated. "It significantly enhances my ability to comprehend Kubernetes workload dynamics. Unlike our previous tool, which seemed geared towards those familiar with coding, Sysdig's interface is more intuitive and accessible, which is crucial for me as a CISO."

"Sysdig also performs significantly better in Kubernetes compared to our previous solution," Scott noted. "It allows us to concentrate on issues like failed logins and environment changes, filtering out routine Kubernetes activities."

SOLUTIONS

A New Approach to Vulnerability Management and Compliance

“Sysdig has streamlined our vulnerability management, freeing us to concentrate on more critical initiatives and achieve greater results,” Scott said “We’re currently updating our policies based on the insights we’ve gained from Sysdig.”

As part of this initiative, Immuta has achieved both SOC2 and ISO270001 certifications, and plans to pursue PCI-DSS in the near future. Scott and his team have also been collaborating with the SRE team to align their vulnerability management policy with cloud practices, enhancing Immuta’s overall defensibility. Sysdig’s vulnerability reporting functionality has significantly supported these efforts.

“With our old tool, it often felt like our vulnerability reports were merely security theater. We were forced to depend on spreadsheets and manual analysis to do the real work,” Williams said. “We just checked a box for runtime protection without being able to configure it effectively for vulnerability management. With Sysdig, we’ve refined our vulnerability management policy, making us more secure and efficient.”

“When I log into Sysdig, everything is intuitive,” Scott said. “It’s improved my effectiveness as a CISO and enables even junior members of the SRE team to manage vulnerabilities independently.”

> “In the past, the security and product teams had to manage vulnerabilities because the SRE team lacked effective prioritization tools. Sysdig changed that — reducing notifications from thousands to hundreds and providing valuable, actionable data in our vulnerability reports.”
>
> **Mike Scott**
> CISO, Immuta

Shifting Security Left

Immuta's long-term goal is to establish a continuous feedback loop between security, SRE, and product engineering. To support this strategy, the company integrated Snyk and Sysdig. This integration allows security feedback to be provided directly to product engineers, shifting security left to harden containers prior to deployment.

With Sysdig's runtime detection, Immuta can immediately identify any runtime vulnerabilities upon deployment, providing greater assurance to their customers.

"One of our drivers for adopting posture management and vulnerability scanning from day one was that our customers were already doing it," Scott said. "Being able to assure customers that things were locked down out of the gate has been incredibly valuable, as has to notify them of potential issues in production environments without bothering the SRE team."

> "Sysdig is not only cost-effective, but highly scalable and frictionless. Our partnership has significantly improved outcomes for both our team and customers. We trust that Sysdig will continue delivering substantial value moving forward."
>
> **Mike Scott**
> CISO, Immuta

Capturing Third-Party Problems

As Williams' colleagues on the SRE team respond to alerts, one particularly valuable feature is Sysdig's capture capability.

"We've used Sysdig to debug problems in infrastructure," Williams explained. "If third-party software misbehaves during deployment, we often don't know exactly what it's doing since we don't own the code. Sysdig gives us the visibility needed to figure out what's going on."

Sysdig has also proven invaluable in keeping up with Immuta's evolving cloud ecosystem. For instance, the company recently transitioned from CentOS to Amazon's Bottlerocket OS, a move that previous tools would not have supported.

"The migration to Bottlerocket was seamless," Scott noted. "While we might have cobbled together a similar solution with cloud security posture management tools, it would have been a nightmare. Sysdig enables us to adopt new technologies and achieve our goals without tool sprawl."

Ongoing Value Through Collaboration

When evaluating security vendors, multiple contenders actively courted Immuta alongside Sysdig. Ultimately, the company selected Sysdig for three key reasons.

The first was Sysdig's engineering-driven approach to cybersecurity. The second was that Sysdig demonstrated a deep understanding of Kubernetes in a way that other vendors do not. Finally, there was Sysdig's customer-centric partnership approach.

"It's been a great partnership since day one," said Scott.

Immuta's shift from on-premises to cloud necessitated a fundamental rethinking of its approach to security. It was this transformation that led it to adopt an engineering-focused tooling strategy and entrust vulnerability management to its SRE team — a strategy poised to benefit Immuta well into the future.

To learn more about Immuta, visit **immuta.com**

IMMUTA®

INDUSTRY

Software Technology

INFRASTRUCTURE

Amazon Web Services (AWS)

ORCHESTRATION

Amazon EKS

SOLUTION

Sysdig Secure

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

To learn more about Sysdig, visit **sysdig.com.**

REQUEST DEMO →