sysdig | BIGCOMMERCE

CUSTOMER STORY

BigCommerce Achieves Real-Time Cloud Security

BigCommerce is a cloud-based e-commerce platform that makes it easy for businesses of all sizes to create, launch, and grow their online stores. It is known for its ease of use, flexibility, scalability, and robust partner ecosystem. But that alone isn't what makes it exceptional – it's the fact that the company maintains security updates, patches, and compliance regulations for customers.

This unique approach has enabled the company to undergo exponential growth. Established in 2009, BigCommerce works with tens of thousands of merchants all over the world. At the same time, the company has managed to keep its IT, security, and engineering teams both lean and efficient.

BIGCOMMERCE

INDUSTRY

Software Technology

CHALLENGES

- Address visibility gaps with comprehensive end-to-end platform support
- Identify and prioritize misconfigurations and vulnerabilities
- Unify compliance requirements and security controls
- Quickly generate granular, actionable insights with as few clicks as possible

OUTCOMES

- Respond to threats in 2 seconds
- 80% reduction in vulnerability noise
- 20% increase identifying and prioritizing misconfigurations and vulnerabilities

CHALLENGES

Not All CNAPP Vendors Are the Same

For BigCommerce, security and compliance are nonnegotiable. Its retailers make billions of dollars in sales each year, and there's no shortage of threat actors looking for a payout. To ensure that BigCommerce's customers did not have to worry a single second about security, the company maintained a robust security stack, including a cloud-native application protection platform (CNAPP) from a well-known cybersecurity vendor.

Unfortunately, they found the tool operationally challenging. Alert noises required more resources than what was feasible, and their support left them feeling alone.

"The vendor's approach to upgrades caused us some significant problems in production," said Jordan Bodily, Senior Infrastructure Security Engineer at BigCommerce. "Between updates, the vendor would randomly push out policies that would reset and retrigger all of our policies. We also couldn't deploy to a specific number of agents – we had to either update individually or do everything at once."

The relationship came to a breaking point. Bodily and his team began the search for an alternative by defining what they needed.

"Threat detection was probably most important to us, particularly the ability to capture command-line inputs in real time," Bodily said. "We also required a solution with a strong cloud security posture management (CSPM) component and runtime protection so that we could identify what was overpermissive in our environment; for instance, if a bucket had cross-account relationships or if we had open posts that should be closed."

The capacity to run ongoing benchmarks against frameworks such as NIST, PCI, ISO, and CIS was also a must. This would allow BigCommerce to conduct regular assessments of its risk and threat management efforts. Finally, the company required full integration support for TerraForm, along with the ability to transmit logs to a security and event management (SIEM) tool.

> "We like that Sysdig uses knowledge of what is in use during production to help us make better-informed posture decisions. It can help filter out 80% or more of the noise. The bottom line is that CSPM is Sysdig's bread and butter, and that inspires confidence."
>
> **Jordan Bodily**
> Senior Infrastructure Security Engineer
> at BigCommerce

SOLUTIONS

Only Two CNAPPs Were Worth Considering

BigCommerce started its search with a long list of vendors that they quickly began to whittle down.

“We eliminated most of the vendors because they aggregate events, giving us access at various increments. Most took anywhere from 30 minutes to several hours to provide scan results,” Bodily said. “This simply didn’t work for us.” As a result, BigCommerce narrowed it down to Sysdig and one other vendor.

“We then looked deeper into both solutions to see what they could do,” Bodily said. “A few weeks later, we deployed Sysdig.”

Sysdig enables security and engineering teams to identify and eliminate vulnerabilities, threats, and misconfigurations in real time. Leveraging runtime insights gives organizations an intuitive way to both visualize and analyze threat data. For BigCommerce, it also met their compliance requirements.

> “We want to know when things are making inbound or outbound connections to risky IPs or if there are any anomalous processes going on. Being an e-commerce platform, we support a checkout flow as well. We want to understand what traffic we’re getting into the platform as well as traffic that’s happening outbound, and we can achieve that with Sysdig.”
>
> **Jordan Bodily**
> Senior Infrastructure Security Engineer
> at BigCommerce

SOLUTIONS

Identifying and Prioritizing Real Risk in Real Time

“Whenever we get an event or log, we want it to tell as much of a story as possible without having to click multiple times through the user interface. Correlation and context is everything,” Bodily said. “Being able to look at the Sysdig UI and immediately know what’s happening is invaluable.”

“We also want to know when things are making inbound or outbound connections to risky IPs or if there are any anomalous processes going on,” Bodily said. “Being an e-commerce platform, we support a checkout flow as well. We want to understand what traffic we’re getting into the platform as well as traffic that’s happening outbound, and we can achieve that with Sysdig.”

BigCommerce also appreciates the speed at which Sysdig operates. Bodily and his colleagues could not imagine relying on any solution that gives attackers as much as an hour’s head start. “I do not want to know when someone’s in my environment 15 minutes or several hours later,” Bodily said. “With Sysdig, we can identify and address potential threats in real time.”

Every Second Counts

According to the **2023 Global Cloud Threat Report**, cloud attackers are quick and opportunistic, spending only 10 minutes staging an attack. This is down from 16 days in on-premises environments.

Another major benefit is the fact that Sysdig automatically produces differentials between its scans.

“A lot of companies don’t provide differentials,” Bodily said. “It’s extremely time-consuming to handle them manually. As someone who has to do vulnerability management every couple of weeks, I greatly appreciate the amount of time Sysdig saves.”

“We also like that Sysdig uses knowledge of what is in use during production to help us make better-informed posture decisions. It can help filter out 80% or more of the noise,” Bodily said. “The bottom line is, CSPM is Sysdig’s bread and butter, and that inspires confidence.”

SOLUTIONS

Vulnerability Management Doesn't Have to Take Half a Day

"Something kind of cool that we've been able to do with Sysdig is feeding events into our SIEM and building queries based on those events," Bodily said. "So for example, say someone installs a packet or a RubyGems outside of Puppet, our configuration management tool. We actually receive an alert and can immediately reach out to that person."

Believe it or not, this is only scratching the surface of how BigCommerce eventually plans to use Sysdig. The company is also planning to explore leveraging Sysdig for PCI 4.0, intrusion detection systems, and automation.

"We want to automate as much as we can around manual processes like vulnerability management," Bodily said. "Right now, we can easily kill half a day or more on vulnerability management. We think Sysdig can help us get 95% of that time back by reducing it to 10 or 15 minutes."

"Our end goal is to have Sysdig handle most of the manual work and have one person review the results, then we're off on the rest of our duties," he said.

> Right now, we can easily kill half a day or more on vulnerability management. We think Sysdig can help us get 95% of that time back by reducing it to 10 or 15 minutes."
>
> **Jordan Bodily**
> Senior Infrastructure Security Engineer
> at BigCommerce

From Vendor to Partner

Perhaps the most significant draw of Sysdig for BigCommerce was the company behind it. Bodily and his colleagues were delighted to see product, engineering, support, and security engineering all involved in the sales and deployment process. More importantly, they appreciated that when it came time to offer product feedback, Sysdig listened.

“This was ultimately the relationship and partnership that we were looking for,” said Dan Holden, Vice President of Cybersecurity at BigCommerce. “Each time we have a question, Sysdig is there in Slack to guide us with same-day support. That’s Sysdig’s great strength, and ultimately a major differentiator – they care.”

To learn more about BigCommerce, visit **bigcommerce.com**.

BIGCOMMERCE

INDUSTRY

Software Technology

INFRASTRUCTURE

Google Cloud Platform (GCP), Amazon Web Services (AWS)

ORCHESTRATION

Nomad

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 →

sysdig

CUSTOMER STORY

CS-BIGCOMMER REV. B 3/24