chronosphere

CASE STUDY

Abnormal Security: Cutting observability costs while boosting platform reliability

Abnormal

Executive summary

When Abnormal Security launched in 2018, it answered the call to protect companies against the attacks that were bypassing legacy email solutions. The company's AI-based threat detection engine for enterprise email security baselines known behavior to recognize abnormal behavior and autonomously prevent personalized, socially-engineered attacks. When it partnered with Chronosphere, Abnormal's homegrown Prometheus + Grafana monitoring solution had reached its limits and was unable to scale with the usage of its fast-growing cloud-native application.

The challenge

Two years into Abnormal's startup journey, the global pandemic hit, enterprises shifted to remote work, and socially-engineered email attacks like business email compromise accelerated at a blistering pace. Abnormal's self-configuring email security system integrates with Microsoft 365 and Google Workspace in one click—it was so easy to deploy, and blocked the most sophisticated email attacks so quickly, the cloud-native app saw a massive surge in customer demand.

As Abnormal's customer base scaled, so did its metrics. The company's 10-12 million active metrics were on pace to soar to 50 million. As much as 80%-95% of metrics came from real-time services deployed via Amazon Elastic Container Service (ECS). Also, the Prometheus instance itself ran on Amazon EC2 R5 (r5.24xlarge with 768 GiB of memory), one of the most expensive and memory-intensive instance types.

Abnormal's single-instance, homegrown Prometheus monitoring system – which was responsible for scraping all endpoints and consolidating all data – had met its match:

- Prometheus uses vertical vs. horizontal scaling, which meant Prometheus wasn't highly available. Any disruption with the EC2 instance caused multiple downstream issues.
- Experienced increased Mean Time to Detection (MTTD) of critical issues.
- Dashboards were slow to load – in fact, dashboards looking at time frames greater than 30 minutes wouldn't load at all.
- Prometheus had a limited retention period of two days due to both the administration and storage cost.
- Engineers accidentally caused Prometheus to crash by deploying new services ornadding new times series—meaning the team was flying blind and scrambling to troubleshoot the cause.

Looking for a solution

Abnormal required a solution that was:

- Reliability
- Control
- Flexibility
- Open-source compatibility

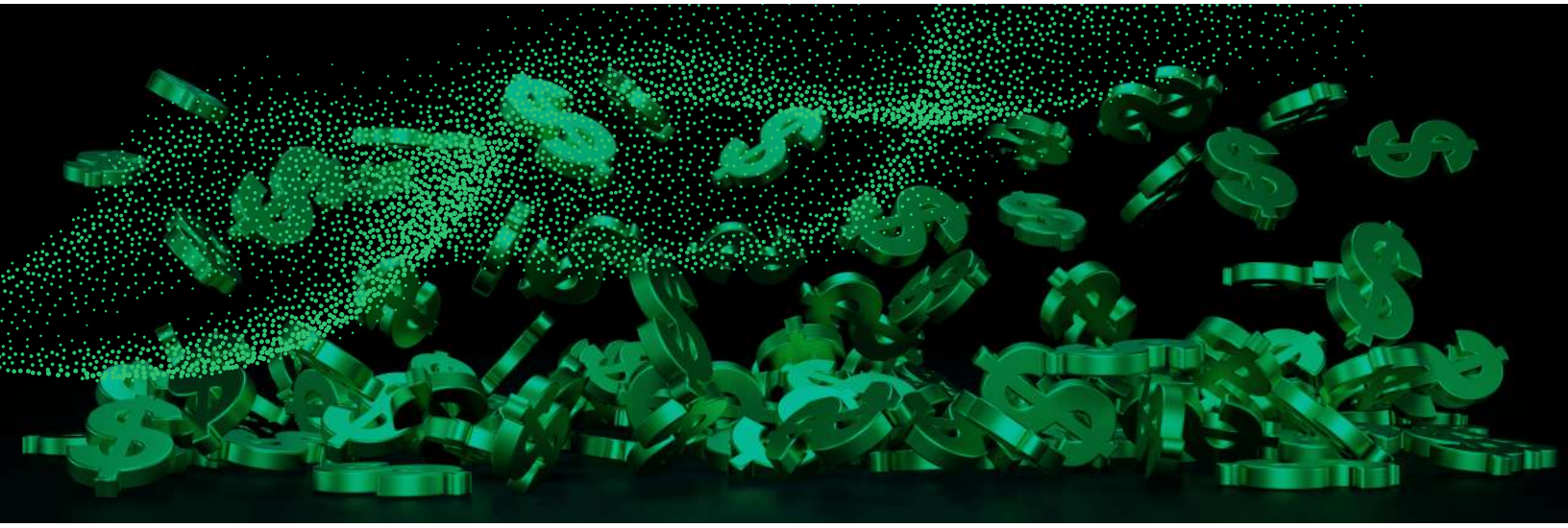
As a result, constant metrics outages plagued the infrastructure team tasked with managing observability, and resource limitations impacted triaging and management. “If you cannot trust your metrics, it creates a very challenging environment. It means several layers of engineering investigation need to be dedicated to figuring out an issue, even if it’s a tiny issue,” said Elder Yoshida, a Software Engineering Tech Lead Manager on Abnormal’s cloud infrastructure team.

For Abnormal, the challenge became finding an observability solution that could keep pace with over 300% business growth experienced over the past year, while achieving its targeted 99.9% SLA.

“When running such a big host – one of the largest ECS instances provided by AWS – you cannot scale vertically anymore,” said Yoshida. “We had to figure out a better solution.”

Solution

Before partnering with Chronosphere to solve observability challenges, the Abnormal team ruled out several monitoring alternatives, including running Thanos themselves in-house or another SaaS solutions like Grafana Labs. Cost savings – engineering and infrastructure - was a key driver behind why Abnormal chose Chronosphere for observability:



Visibility and control over usage:

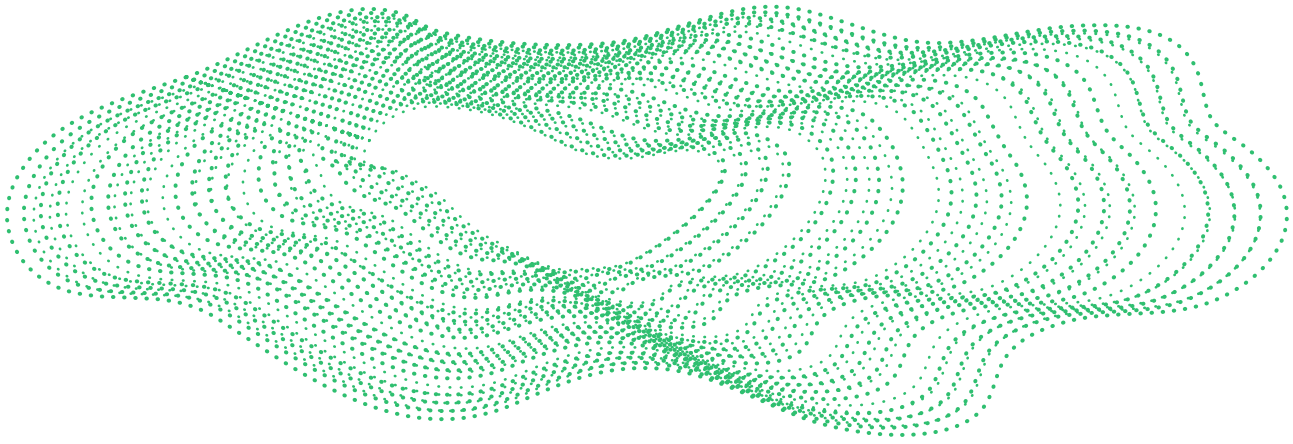
With Chronosphere, Abnormal gained visibility into how the observability system is being used, as well as gained control over how it behaves when it reaches its limits. No longer would small code changes cause the metrics system to slow down or crash.

Flexibility in metric retention:

With Chronosphere, Abnormal can make easy adjustments to retention times, such as choosing both the time interval as well as the retention time. For example, Abnormal could choose to roll up its metrics in five-minute increments for six months.

Data aggregation:

Chronosphere's unique control plane allowed Abnormal to aggregate 98% of their metrics, which resulted in it being 10x more cost-effective than alternative SaaS and self-managed options. By doing so, Abnormal aligns their metrics data to the business value. "The most compelling feature Chronosphere offered is the data point aggregation. This helps us reduce the cardinality that we don't need and only store the data that is critical to us. That was the differentiating factor that helped us save costs in the long run, " said Yoshida.



Reduced management overhead:

Abnormal decreased the number of times engineers and admins had to work on their internal solution prior to Chronosphere, freeing them up to work on problems that drive their business. “We knew if we were to build it ourselves, we would have to fund a dedicated team. This was a non-starter because at the time we were really focused on using engineering time to tackle other issues, like expanding our customer base and continuing our growth,” said Yoshida.

Open source compatible:

Abnormal needed a SaaS solution that can natively ingest Prometheus so it wouldn't have to change any of its instrumentation. “We needed to figure out a way to move quickly, which meant not having to do a lot of engineering work to ingest. We didn't want to spend time rewriting our alerts or rewriting the actual code around our metrics,” said Yoshida.

Outcome

Abnormal’s move from a self-managed Prometheus monitoring tool to a full observability platform supported a top-level company metric. As a provider of email security, the company always needs to have enough capacity to support its customers and increase growth. To do this, it needs to know about incidents when they happen and before they become a problem.

“Chronosphere observability is making it so we never say no to customers.”

Key results

As an engineering team, Abnormal is experiencing with Chronosphere:

- Improved overall Prometheus stability: With the Chronosphere collector running in ECS, Abnormal has a clear, predictable scale of resources and improved uptime.
- Mean Time to Detection (MTTD) and Mean Time to Resolution (MTTR) were reduced by at least 80% based on SLOs (Service Level Objectives). Abnormal is able to average >5 minutes for MTTD starting out and lower it to <1 minute with Chronosphere.
- Improved query performance: Abnormal is able to load dashboards 8-10x faster, including dashboards with longer time frames (i.e. greater than six months).
- Flexible metric resolution and retention is enabling Abnormal to keep the most important metrics for the duration of its business requirements.
- Improved reliability and stability of its metrics system: Leveraging Chronosphere's control plane is flattening large spikes in metric volume and improving overall stability to greater than 99.9% uptime.
- Real-time visibility into metrics increased Abnormal's ability to understand problems that can be addressed by high cardinality metrics.
- Empowered the SRE team to shift focus from monitoring to tackling problems that move the needle for the business.

Abnormal

"The long-term impact of switching to Chronosphere is freeing up headspace to tackle the hard problems and deliver business value and a better experience for our customers."