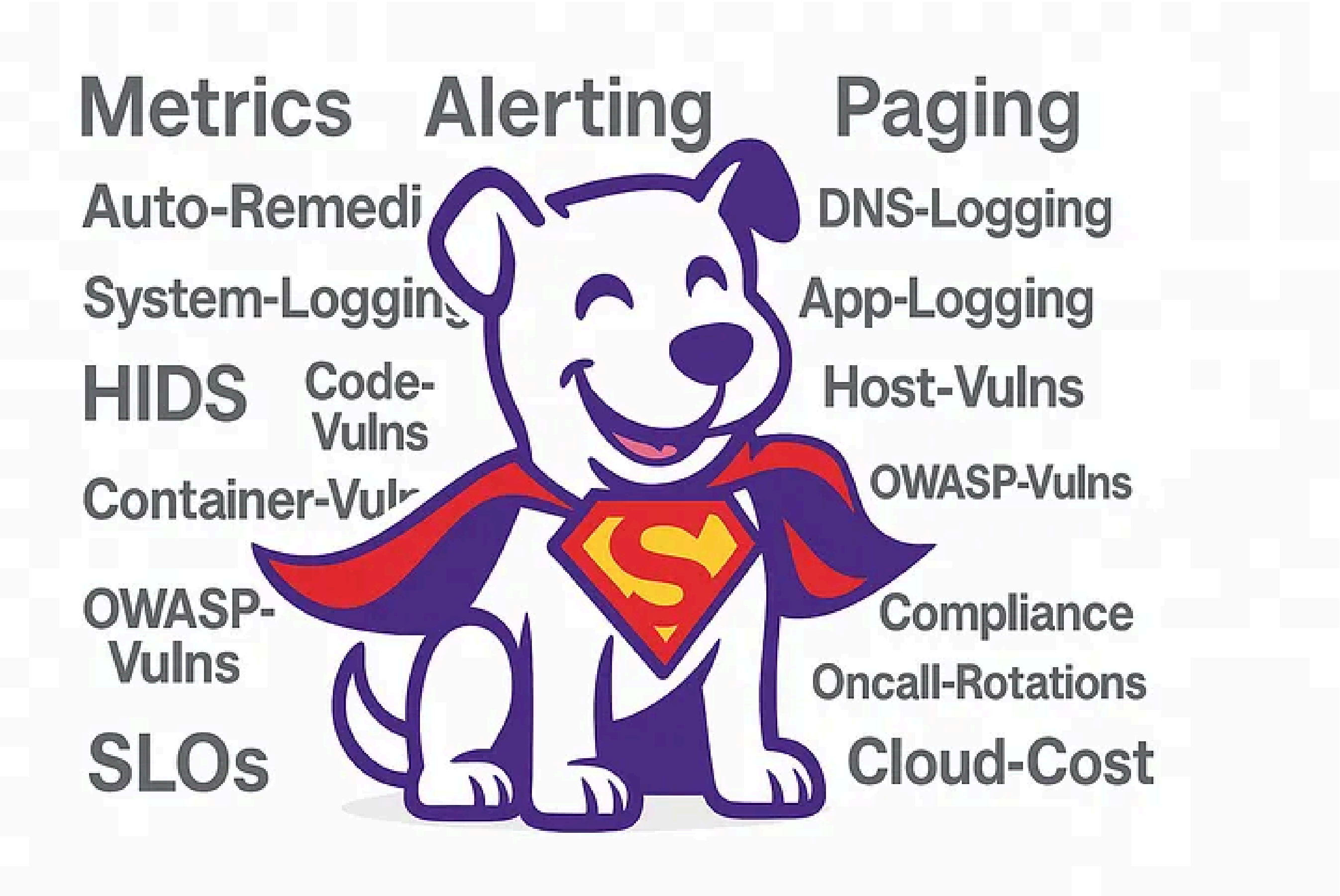
Wait... Since When Did Datadog Replace PagerDuty?

Datadog's expansion into a multifaceted operations platform

8 min read · 2 days ago

Elliot Graebert Follow

Listen Share More



Datadog is no longer just a monitoring platform.

I've always been a Datadog fan, but with their expansion into new products, allowing me to replace tools like Splunk, Tenable, PagerDuty, OSQuery, Dome9, Sentry, Mixpanel, custom FIM scripting, Snyk, and Burp, into a single enterprise Datadog contract — well, now I'm a fanatic.

This blog post is for my fellow infrastructure engineers, who may not have realized the scope of Datadog's expansion over the past couple of years. While Datadog has a reputation for being very expensive, it is cheaper (for Skydio) than paying for all these other vendors independently.

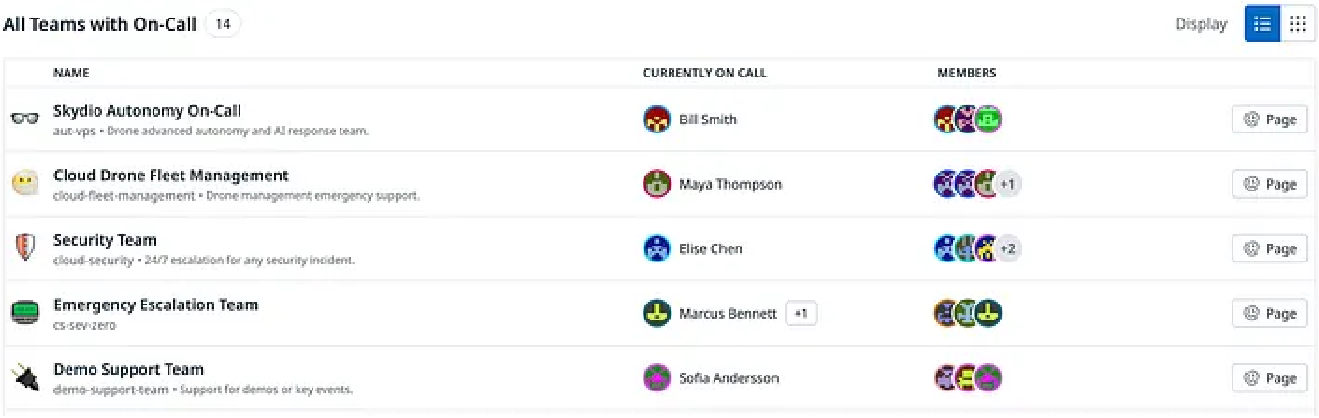
In my first-ever blog post (Many Facets of Infrastructure), I highlighted 60 facets that go into running a highly available and secure cloud-based application. I went back and updated it, and Datadog now covers 18 of the 60 facets. With their upcoming FedRAMP High certification, it's an excellent time to revisit your current portfolio of vendors that support your application.

. . .

It's time to dump PagerDuty.

PagerDuty has been a staple in the industry, but in the 10 years I've been a customer, they have not delivered a single new feature that I find compelling. I just always assumed that the tradeoff was between PagerDuty and some other alerting framework (like OpsGenie).

Recently, Datadog has reached general availability with their PagerDuty replacement: On-Call.



All Teams with On-Call 14

NAME	CURRENTLY ON CALL	MEMBERS	
Skydio Autonomy On-Call aut-vps • Drone advanced autonomy and AI response team.	Bill Smith		Page
Cloud Drone Fleet Management cloud-fleet-management • Drone management emergency support.	Maya Thompson	+1	Page
Security Team cloud-security • 24/7 escalation for any security incident.	Elise Chen	+2	Page
Emergency Escalation Team cs-sev-zero	Marcus Bennett +1		Page
Demo Support Team demo-support-team • Support for demos or key events.	Sofia Andersson		Page

Datadog Teams can now go on-call and be directly paged.

Datadog On-Call schedules work similarly to PagerDuty's.

When we were using PagerDuty, we ended up needing to duplicate our concept of “teams” and “services” into both Datadog and PagerDuty. We needed it in Datadog so that we could tag dashboards and monitors with their team owner, and we needed it in PagerDuty so we could establish on-call schedules. Condensing this down to just Datadog allowed us to remove unnecessary automation and focus on a single tool.

In addition, Datadog's On-Call is cheaper than PagerDuty. **Saving money by switching to Datadog? Hell may have finally frozen over.**

. . .

Datadog can now do vulnerability management

Vulnerability management means:

1. The live scanning of assets in your production environment.
2. Mapping scan results to known vulnerabilities
3. Tracking the remediation of vulnerabilities within the appropriate patching window (e.g., 14/30/60/90 days for critical/high/medium/low vulnerabilities).

In the past, I've recommended tools like Tenable as a single-purpose tool for performing vulnerability scanning. Where I've run into friction is trying to integrate Tenable into my infrastructure team's routine workflows. I swapped Skydio over to using Datadog's vulnerability scanning tool, and the flow is awesome.

Datadog’s query language and grouping make vulnerability analysis much easier.

Since we were already using Datadog, adding the container image and host vulnerability scanning was just a couple of lines of configuration. After that, we had a list of findings that we could filter and sort in the typical Datadog fashion. From there, I used their Findings Automation Pipeline to automatically set due dates for any vulnerability that was close to breaching its SLA.

The due date is also tagged in the data model.

Once the vulnerabilities had due dates, it was easy to create a monitor that would alert my team any time there was a vulnerability that wasn’t fixed by our automated patching:

These alerts are then piped into Slack.

And presto: I now have continuous vulnerability monitoring! If you aren't familiar with vulnerability management, this might not seem exciting. However, if you've had to maintain a FedRAMP, CJIS, or equivalent system, maybe you're nerding out with me.

You can then expand this to include:

- Cloud Security Posture Management — scan your cloud environment for unencrypted drives or missing MFA configurations. Replaces tools like Dome9.
- Code vulnerabilities — static application security testing (SAST). Replaces tools like Snyk or Semgrep.
- Web vulnerabilities — dynamic application security testing (DAST). Replaces tools like Burp Suite.

Having all your vulnerabilities in one place? Chef's kiss!

. . .

Datadog is a SIEM now?!?!?

That's right, Datadog is now a SIEM *and* SOAR!

Infrastructure engineers want their logs in the same application as their metrics and monitors (i.e., Datadog), but security professionals want all the logs in their SIEM (i.e., Splunk). I've always found myself paying twice for these as separate tools. However, with Datadog now having dedicated products for SIEM and SOAR, you can now avoid double-paying.

Datadog doesn't just act as a simple log ingestion engine, but it comes prepackaged with alert detection strategies and SOAR automation for auto-response. For example, when you think “Datadog”, do you think: “comes prebuilt with alert detection strategies for Meraki firewalls”.

This image is copied straight from Datadog’s documentation.

I don’t think most people have seen Datadog’s dramatic transformation from “observability” to an observability/security hybrid. Every month, they seem to add another tool or integration that formerly was its own company:

- File integrity monitoring and SBOM analysis
- Network analysis and investigation tools
- eBPF agents for kernel-level inspection.

Now it’s worth noting that Datadog’s SIEM and SOAR products are much newer and might not have all the integrations that your organization requires. I’d recommend taking a cautious but optimistic look at what they offer today.

. . .

Honorable mentions

The point of the post was to highlight some of the more interesting Datadog products that have emerged over the past couple of years. The following weren't in my top three of "most intereating", but still worth a brief mention:

Datadog Error Tracking to replace Sentry.io

Datadog now treats errors as their own data model. Integrates with services and teams.

Datadog treats errors as it's own data model, with the idea that it's more than just "a log with a error code". By treating errors as their own data model, you can track and resolve them across deploys. It's not a complex idea, but it was a genuinely a nice addition.

You can get errors linked with your source code, making it easier to go from the error, to where in the code you need to look. It's not earth shattering, but I'm glad they have it.

Datadog Synthetic Testing to replace BrowserStack

We leverage browser-driven tests as both regression tests and as an advanced form of monitoring

Datadog synthetic testing is surprisingly simple and reliable. We deployed it three years ago with only a couple days worth of work. It has run reliably since then as a pre-deploy check in both our staging and production environments. We've since gone ahead and started replacing it with Playwright testing, but I thought it was worth a callout — the tool has provided surprisingly good results for the amount of effort we put into it.

Datadog RUM and Product Analytics to replace Mixpanel and Google Analytics

Datadog has been instrumental in learning our user flows.

Datadog's RUM and Product Analytics products probably deserve their own blog post. To me, they are essentially for tracking your users' journey throughout the app and seeing what was happening when they experienced an error. They also have excellent masking capabilities such that you can easily capture your users' interactions, without revealing any of the data that needs to be kept sensitive.

The reason I didn't include it is because I don't think anyone would find it surprising that Datadog has these features. It's kind of expected at this point.

. . .

The negatives I didn't put above

The amount of products is overwhelming

Similar to AWS, the breadth of Datadog is massive, and neither their product or support do a good job at shepherding you through the product. There are so many parts of the app, it’s hard to tell whether you’re optimally using the product. If you are feeling overwhelmed by the amount of options, you’re not alone.

New Datadog’s products stay in a half-developed state for too long.

Datadog’s Incident Management was missing a Google Meet integration for at least a year — but they had Teams and Zoom. Unfortunately, Skydio is a Google Meet shop, so this was a big killer.

Datadog On-Call doesn’t have a Slack integration for updating a `@current-oncall` style handle. We rely heavily on this integration to help direct people to the correct team’s on-call engineer.

Over time, these issues keep getting addressed, but it leaves me with low trust that a new Datadog product is ready for enterprise use in the first 6 months of it launching. That’s not too surprising.

Datadog’s pricing structures are too complicated

As Datadog’s products have exploded in quantity, it’s become a nightmare to try and maintain an enterprise billing model that makes sense. They charge for usage for each individual product, and you never know which feature is priced poorly and will blow out the budget. From experience, I can say that it’s possible to get to a reasonable price where the value of all the functionality greatly exceeds the cost — but you have to spend more time than you want reading pricing charts.

. . .

Wrap-up

Datadog has rapidly expanded into many new verticals, which has been transformational. Being able to condense down a dozen different vendors into oneapplication has been a huge relief for me. On top of that, their FedRAMP compliance means that I can use them, even in the most stringent of US Government compliance.

My hope with this blog post is that at least one of the use cases above was new for you, and maybe one of these tools will make your life easier.

> *This blog post was written entirely by a human (me)! Excluding spell checking, all ideas, content, and prose were generated by me, and no AI! All run-on sentences, extra commas, and nonsensical phrasings are from me. Also, the ideas presented in this post are of my own personal opinion, and not as a representative of Skydio.*

Software Development Site Reliability Engineer DevOps Datadog

Observability

Follow

Written by Elliot Graebert

4.7K followers · 0 following

Sr Director of Engineering at Skydio, Ex-Palantir, Infrastructure and Security Nerd, Gamer, Scuba Diver, Dad

No responses yet

Bgerby

What are your thoughts?

More from Elliot Graebert

Elliot Graebert

Comparing the Top Eight Managed Kubernetes Providers

My experience deploying Helm charts on eight cloud providers.

Feb 1, 2023 👏 877 💬 25

Elliot Graebert

Laptop development is dead: why remote development is the future

Using Coder-OSS to demonstrate the power of Kubernetes-based development environments.

Nov 15, 2022 👏 3.3K 💬 69

Elliot Graebert

How I replaced Google with ChatGPT

Incorporating AI into my daily engineering workflows.

Sep 18, 2023 714 7

In Better Programming by Elliot Graebert

Designing a Backup and Disaster Recovery Plan

A comprehensive disaster recovery guide takes time, planning, and automation

May 8, 2022 101

See all from Elliot Graebert

Recommended from Medium

Neal Davis

Cloud Skills that will soon be obsolete—and what to learn instead

If you're learning cloud right now—pay attention. Some of the most common skills people still spend hours practicing are already...

Oct 13 17 2

In Stackademic by Mohab AbdelKarim

AWS Just Fired 40% of Its DevOps Team — Then Let AI Take Their Jobs!

Leaked internal tools show how Amazon's cloud is now self-healing, self-scaling, and self-negotiating — no humans required.

✦ 4d ago 👏 53 💬 9

Alex Suzuki

Cretaceous Software Engineering — Why I don't use AI to write code.

👋 Hi! I'm a Cretaceous Software Engineer.

6d ago 641 28

Devansh

Why Jensen Huang Loves the “AI Bubble” Stories

Answering why AI is not a Bubble and the Deeper Story at play

5d ago 273 8

In The Context Layer by Jannis

Claude’s New “Skills” Show How Anthropic Is Layering Intelligence on Top of MCP

✦ 4d ago 240 1

In AI Advances by Pooja Kashyap

Speech-to-Meaning: Why the Future of Voice AI Isn’t About Better Microphones

“Tea, Earl Grey, Hot”, remember this line by Picard from Star Trek?

4d ago 396 10

See more recommendations