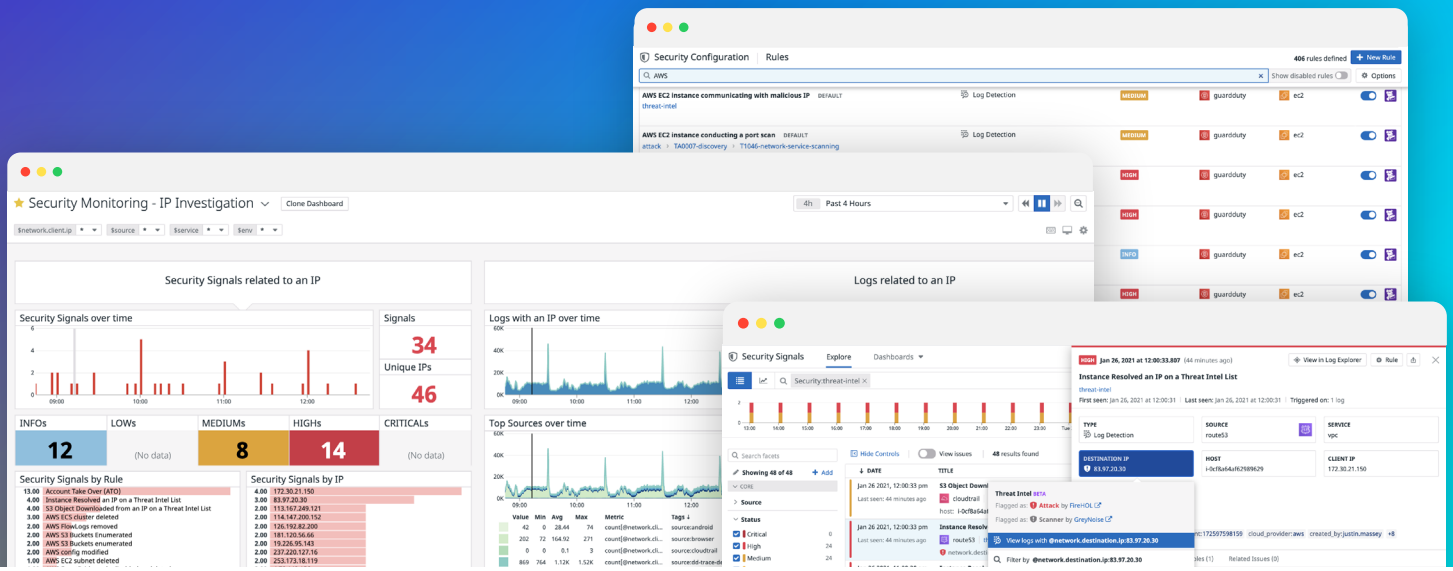
Datadog Cloud SIEM

Detect, investigate, and respond to threats across your applications, networks, and infrastructure.



Introduction

As dynamic, cloud-native environments face increasingly sophisticated security threats, the boundaries between security, development, and operations teams are beginning to fade. Security teams need visibility into their applications, infrastructure, and network, while development and operations teams need the ability to secure the services they own. Entire engineering organizations therefore need access to a unified platform for their monitoring and security data so they can protect their environments from breaches and attacks.

Limitations of threat detection tools in the cloud

Businesses face mounting pressure with each new breach or attack, so it's essential that they have the tools they need to proactively detect potential threats before they escalate. The inherent complexity of cloud-native environments, however, poses several challenges for teams that are trying to fortify their security posture:

SILOED TOOLS LIMIT VISIBILITY

Cloud-native environments are fast-paced, and it's important to capture all activity in order to identify security threats and remain compliant. Historically, teams have relied on multiple siloed tools to monitor these dynamic systems, but this process creates blindspots and slows down the investigation process.

LOGGING INCONSISTENCIES COMPLICATE THREAT DETECTION

Authentication logs come from many different sources in your environment, which results in formatting inconsistencies. They may also be managed by different teams and implemented with different third-party services, such as Google, Okta, and Auth0. This can make it difficult to perform meaningful analysis of all authentication activity.

INVESTIGATIONS ARE MISTAKE-PRONE

Organizations often struggle to assess the impact of security attacks across ephemeral entities and unknown users, and undetected attacks can lead to major security breaches. It's therefore critical that the teams responsible for securing cloud services can identify and respond to threats as soon as they occur.

MISCONFIGURATIONS CAN HAVE SEVERE CONSEQUENCES

A single misconfigured security group in a cloud environment can have cascading consequences and lead to a serious data breach. This puts a lot of pressure on development and operations teams to properly secure their services.

Detect and analyze security threats anywhere in your stack

Datadog Cloud SIEM provides end-to-end security coverage of dynamic, distributed systems in a unified platform. This enables DevOps, SecOps, and GRC teams to work together to detect and respond to threats and misconfigurations in real time, without having to switch contexts. Cloud SIEM is fully integrated with all of Datadog's application and infrastructure monitoring products, which allows users to seamlessly pivot from a potential threat to associated monitoring data in order to quickly triage security alerts.

With Datadog Cloud SIEM, you can:

UNIFY YOUR OBSERVABILITY AND SECURITY EFFORTS

See all of your data in one place. Easily correlate security data with runtime events, application and service logs, and more.

Break down silos between teams. Development, security, and operations teams can access the same observability data and drive security investigations in a single, unified platform.

VISUALIZE YOUR SECURITY DATA WITH OUT-OF-THE-BOX DASHBOARDS

Get a high-level overview of your security posture. The Security Overview dashboard allows anyone in your company to review system-wide security signals at a glance.

Pivot from a bird's-eye view to granular details. The IP Investigation and User Investigation dashboards enable users to correlate specific IP addresses and users with security signals, events, and logs, so they can quickly hone in on malicious activity patterns.

LEVERAGE THREAT DETECTION RULES THAT DON'T REQUIRE A QUERY LANGUAGE

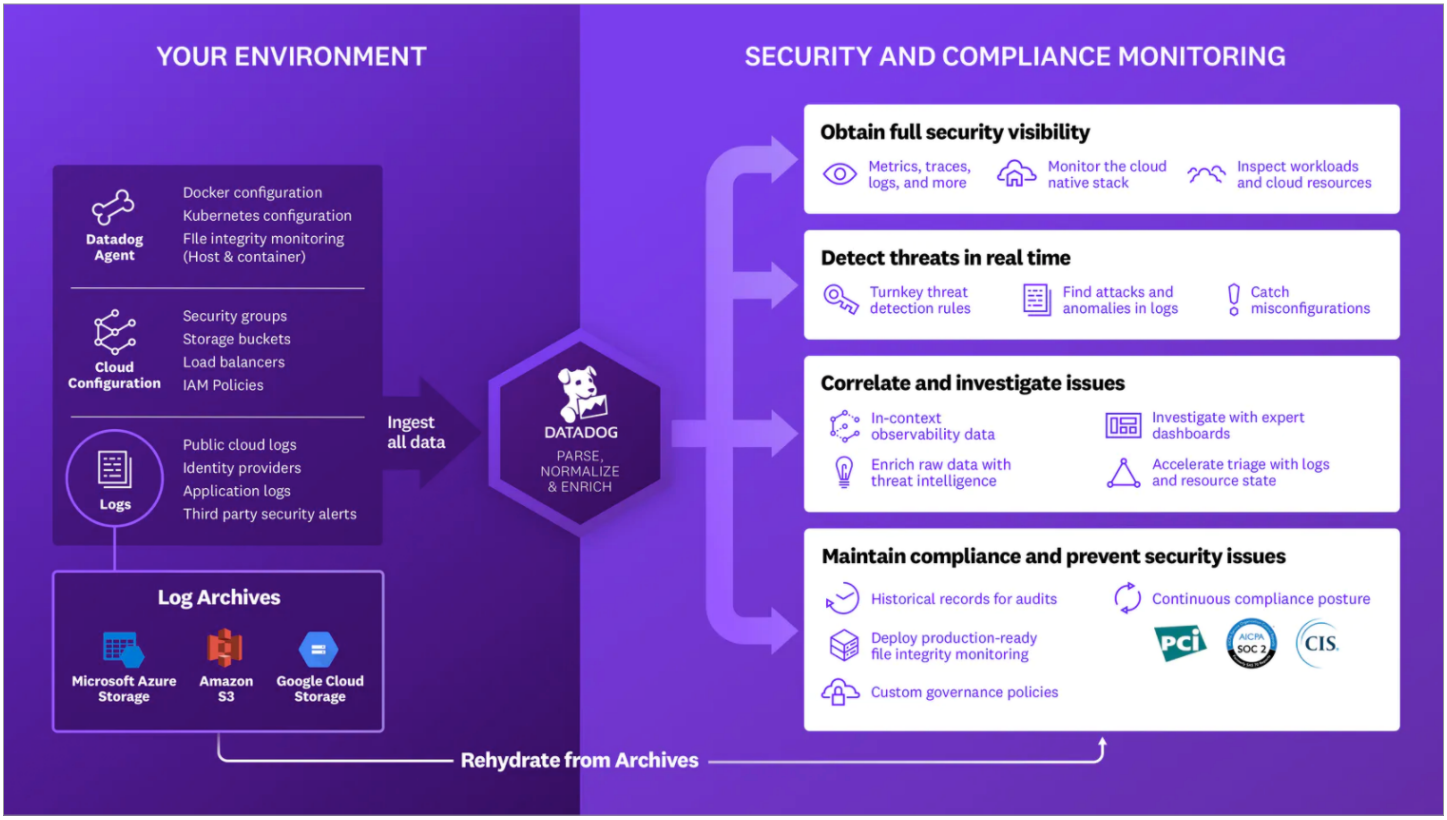
Get started quickly with turnkey detection rules. Datadog Cloud SIEM comes equipped with out-of-the-box threat detection rules for widespread attacker techniques and misconfigurations that are mapped to the MITRE ATT&CK® framework. This means you can improve your security posture in minutes, without any subject matter expertise. Out-of-the-box rules can also be customized to fit your organization's needs.

Create custom rules in a code-free editor. Users can create their own sophisticated rules for account takeovers, root user activity, and more with a flexible yet powerful editor. Rule creation is intuitive and does not require knowledge of a query language.

JUMPSTART YOUR INVESTIGATIONS WITH MORE THAN 400 VENDOR-BACKED INTEGRATIONS

Collaborate easily during investigations. Datadog integrates with Slack and PagerDuty allow you to automatically loop in relevant teams when a high-severity rule detects a threat. You can also export security signals to collaboration tools like JIRA or ServiceNow.

Security integrations provide additional context. Built-in security integrations with AWS CloudTrail, Okta, G Suite, and more enable users to ingest additional security data in minutes, which provides deeper context and helps accelerate investigations.



Security for dynamic environments

Security threats in cloud-native environments move fast, which means that security, development, and operations teams all need visibility into their infrastructure, network, and applications. Datadog Cloud SIEM is a SaaS solution that provides end-to-end security coverage of dynamic, distributed systems. It enables real-time threat detection across the entire stack, as well as deeper collaboration between teams.

MITRE | ATT&CK®


DATADOG