Devo Platform

Cloud-native logging, SIEM, and security analytics

Key benefits

• Get full visibility into all your data—400 days hot—for faster, more accurate threat investigations.
• Embedded threat intelligence platform to enrich with threat context and guide analysts.
• Entity analytics point analysts to anomalous behaviors, surfacing threats to your organization automatically.
• Complete incident response and investigation workflow enables your team to respond rapidly.
• Devo is a true cloud-native solution for businesses that already operate in the cloud or are making the shift to the cloud.
• Automated Devo enrichments inform your security operations center (SOC) analysts, enabling them to streamline their triage, investigation, and hunting workflows.

Product overview

The Devo Platform enables security and operations teams to address common use cases including centralized logging, SIEM, compliance, fraud detection, and more. The Platform includes tightly integrated applications for security and IT teams.

Product features

Full visibility without compromise
Devo allows you to ingest data from all your data sources closing the visibility gap that puts your organization at higher risk, it lets you integrate with your existing security products with seamless enrichment integrations, and connects with flexible APIs to your preferred SOAR platform to accelerate incident response.

Real-time detections and enriched investigations
Free up analyst’s valuable time spent on getting their logging and SIEM to work and instead spend it on the investigations that pose the highest risk to your organization with automated enrichments, machine learning powered analytics, and advanced alerting to investigate and detect threats faster than ever. Devo also maps to the MITRE ATT&CK framework across alerts and investigations, adding additional context.

Maximize analyst productivity
Up-level analysts’ performance with capabilities that empower them to perform beyond their level of expertise with analyst-centered workflows, dynamic visual analysis, enriched investigations, and other confidence building capabilities.

Additional Resources

• Devo Data Sizing Tool
• Evaluation Toolkit
• Devo Support and Training
• Devo FAQ
How it works

Devo has engineered a solution to empower enterprise security teams and provide them the ability to view their entire attack surface. The Devo Platform, combined with the Devo Security Operations application, provides advanced analytics for SOC teams to detect, investigate, and hunt for attacks in real-time—24/7/365—enabling a robust defense against all cybersecurity threats that modern enterprises face. And, with alert categorizations from Devo mapped to the specific tactics, techniques, and procedures (TTPs) found in the MITRE ATT&CK framework, analysts can act quickly to respond to the most critical techniques being triggered.

Differentiators

- Handles terabytes of ingest volume while analyzing petabytes of data
- Delivers insights from log and metric data, providing business, security, and operations teams with no-code visual analytics
- No-compromise architecture that delivers both scale and speed at lower costs
OneMain Financial Gets More Visibility and Context with Devo

**Challenge**
In an industry where security is always top of mind, OneMain Financial needed more transparency and optics on understanding vulnerabilities, threats, and issues across the enterprise.

**Solution**
Devo was able to approach security monitoring by solving the data problem. Devo helped OneMain Financial to create a clear picture of what’s happening internally with all asset behaviors, connectivity, and data flows at any given time.

**Benefits**
- Took away the concern of how to ingest and regulate data
- Increased visibility on security monitoring across the enterprise
- Enabled a way to protect data and solve real business challenges

“OneMain Financial had a goal of making our SOC more effective while being able to increase visibility into all environments. By working with Devo and AWS, OneMain has been able to achieve these goals by ingesting more data from a variety of sources, positively impacting functionality between our Search, Alerts, and Dashboards.”

Tunde Oni-Daniel, VPsMD Head of Security Architecture, Engineering and Operations, OneMain Financial

Solution available in [AWS Marketplace](https://aws.amazon.com/marketplace/)