Devo Security Data Platform

Ingest anything and defend everything.

SOLUTION BRIEF

SECURITY TEAMS CONFRONT DATA, TECHNOLOGY, AND RESOURCE CHALLENGES

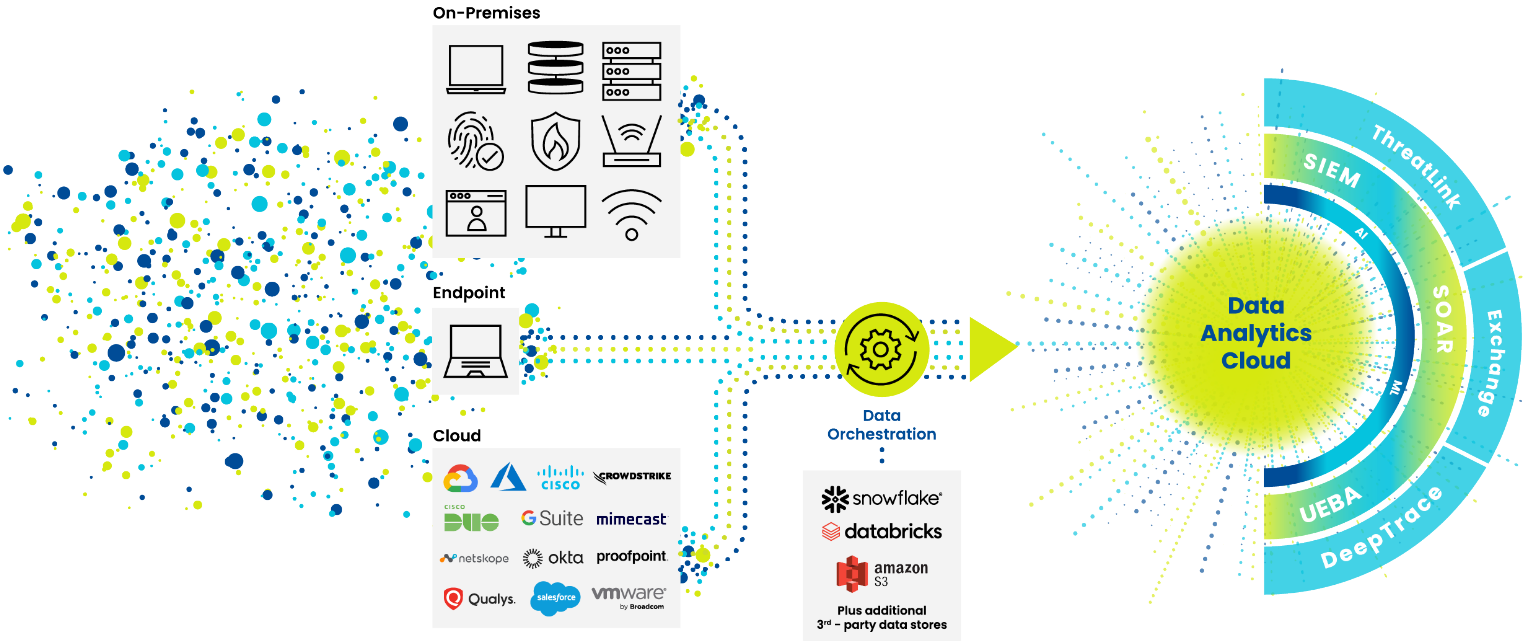
Security teams today are facing a perfect storm of challenges. The explosion of data, coupled with an ever-expanding attack surface, is overwhelming traditional security tools and processes. Legacy SIEM solutions, designed without a data-at-scale mindset, struggle to manage diverse data sources and an increasing volume of events.

With ever-expanding volumes of data, organizations are forced to make difficult tradeoffs. Either they discard potentially valuable data to save on costs, or they overspend on trying to ingest and analyze everything.

To overcome this challenge, a new approach is needed: a cutting-edge security data platform capable of handling massive data volumes, ingesting diverse data sources, performing real-time analysis, and leveraging AI-powered automation to help security teams detect and respond to threats faster.

TRANSFORM SECURITY OPERATIONS WITH THE DEVO SECURITY DATA PLATFORM

The Devo Security Data Platform is a cloud-native security analytics platform that empowers organizations to gain deeper insights into their security data, enabling them to detect, investigate, and respond to threats more effectively. It provides limitless visibility by orchestrating and ingesting data from unlimited data sources and improves MTTD and MTTR up to 90% with its integrated security capabilities, including advanced SIEM, SOAR, UEBA, automated case management, and autonomous investigation and threat hunting.

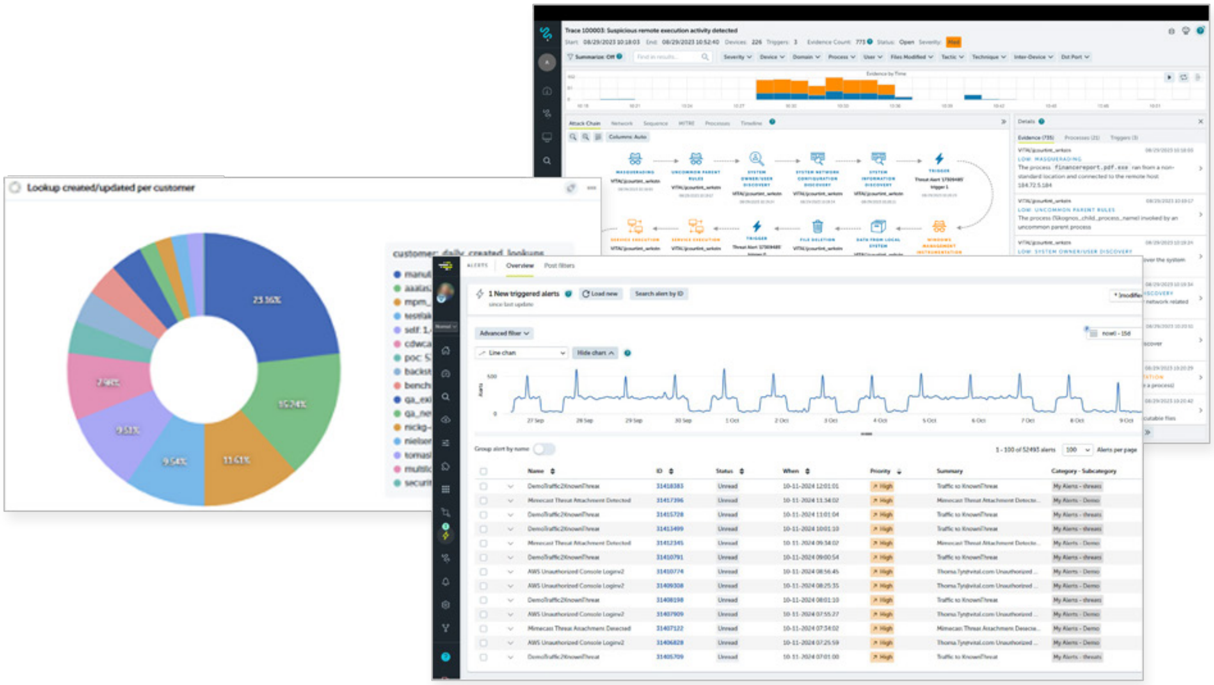


The Devo Security Data Platform protects evolving environments from relentless cyber attacks while optimizing costs.

SEE MORE, KNOW MORE, AND ACT FASTER

The Devo Security Data Platform sets itself apart with its unparalleled speed, scalability, and advanced security analytics capabilities, empowering organizations to transform massive amounts of security data into actionable insights.

Speed and Scale	Real-Time Analytics	Actionable Intelligence
Achieve unmatched visibility as your infrastructure scales and evolves **Filter and route data** to ensure the right data is accessible **Find the signal** over an extended time horizon with always-hot data	**Find threats with zero lag** with streaming alerts **Automate alert triage** by correlating and enriching alerts into high-fidelity cases **Identify anomalous activity** with tunable risk-based alerting	**Get the full attack story** within minutes with attack-tracing AI **Visualize your threat posture** with customizable Devo Activeboards and Grafana dashboards **Pinpoint attacks and assess threat coverage** with the MITRE ATT&CK Framework



Trace 100003: Suspicious remote execution activity detected

Start: 08/29/2023 10:18:03 End: 08/29/2023 10:52:40 Devices: 226 Triggers: 3 Evidence Count: 773 Status: Open Severity: Med

The process financereport.pdf.exe ran from a non-standard location and connected to the remote host 184.72.5.184

The process {$kognos_child_process_name} invoked by an uncommon parent process

1 - 100 of 52493 alerts

	Name	ID	Status	When	Priority	Summary	Category - Subcategory
□	DemoTraffic2KnownThreat	31418383	Unread	10-11-2024 12:01:01	↗ High	Traffic to KnownThreat	My Alerts - threats
□	Mimecast Threat Attachment Detected	31417396	Unread	10-11-2024 11:34:02	↗ High	Mimecast Threat Attachment Detecte...	My Alerts - Demo
□	DemoTraffic2KnownThreat	31415728	Unread	10-11-2024 11:01:04	↗ High	Traffic to KnownThreat	My Alerts - threats
□	DemoTraffic2KnownThreat	31413499	Unread	10-11-2024 10:01:10	↗ High	Traffic to KnownThreat	My Alerts - threats
□	Mimecast Threat Attachment Detected	31412345	Unread	10-11-2024 09:34:02	↗ High	Mimecast Threat Attachment Detecte...	My Alerts - Demo
□	DemoTraffic2KnownThreat	31410791	Unread	10-11-2024 09:00:54	↗ High	Traffic to KnownThreat	My Alerts - threats
□	AWS Unauthorized Console Loginv2	31410774	Unread	10-11-2024 08:56:45	↗ High	Thoma.Tyr@vital.com Unauthorized ...	My Alerts - Demo
□	AWS Unauthorized Console Loginv2	31409308	Unread	10-11-2024 08:25:35	↗ High	Thoma.Tyr@vital.com Unauthorized ...	My Alerts - Demo
□	DemoTraffic2KnownThreat	31408198	Unread	10-11-2024 08:01:10	↗ High	Traffic to KnownThreat	My Alerts - threats
□	AWS Unauthorized Console Loginv2	31407909	Unread	10-11-2024 07:55:27	↗ High	Thoma.Tyr@vital.com Unauthorized ...	My Alerts - Demo
□	Mimecast Threat Attachment Detected	31407122	Unread	10-11-2024 07:34:02	↗ High	Mimecast Threat Attachment Detecte...	My Alerts - Demo
□	AWS Unauthorized Console Loginv2	31406828	Unread	10-11-2024 07:25:59	↗ High	Thoma.Tyr@vital.com Unauthorized ...	My Alerts - Demo
□	DemoTraffic2KnownThreat	31405709	Unread	10-11-2024 07:01:00	↗ High	Traffic to KnownThreat	My Alerts - threats

DEVO DATA ANALYTICS CLOUD: THE FOUNDATION OF THE DEVO SECURITY DATA PLATFORM

Data Analytics Cloud fuels the end-to-end security capabilities of the Devo Security Data Platform. It is the only data-agnostic, real-time analytics foundation purpose-built for advanced security teams and MSSPs. It empowers organizations to seamlessly orchestrate, ingest, and analyze unlimited volumes of data from diverse sources, regardless of format. Open APIs facilitate custom integrations and applications, providing the flexibility to build tailored security solutions.

DETECT, INVESTIGATE, AND RESPOND TO THREATS WITH UNPRECEDENTED SPEED AND ACCURACY

The Devo Security Data Platform leverages unparalleled speed, unlimited scalability, and advanced analytics to help organizations revolutionize their security operations.

Intelligent SIEM: Devo Intelligent SIEM delivers a SaaS-based, scalable, high-performance SIEM integrated with SOAR, UEBA, automated case management, and autonomous threat detection, investigation, and response (TDIR).

Intelligent SIEM provides a singular view of your risk posture, security operations, and threat detection by leveraging MITRE ATT&CK framework context, Devo Exchange security content, and automated enrichment and correlation across cloud, hybrid, and on-premises security environments.

User and Entity Behavior Analytics (UEBA): Devo Behavior Analytics is an AI-powered UEBA solution that uncovers anomalous activity and quantifies risks across users, devices, and domains within multi-petabyte data sets. It employs an extensive library of AI models to detect unusual behaviors and quantify risks to streamline investigations.

Security Orchestration, Automation, and Response (SOAR): Devo SOAR streamlines incident management by automating workflows and integrating security tools, leading to more efficient response. Its enhanced collaboration capabilities enable security teams to pivot and quickly gather new information, resolving security incidents faster and more effectively.

Devo SOAR uses AI-powered playbooks and decision automation to handle any volume of alerts while reducing response times from hours to minutes.

Automated Alert Triage and Case Management: Devo ThreatLink™ is the centralized, automated case management solution that helps security teams track and collaborate on security incidents and alerts. It automates alert triage by correlating and enriching alerts into high-fidelity cases, reducing analyst workload from thousands of alerts to tens of cases per day. Its extensible automation enables teams to streamline triage and investigation workflows and act more quickly against threats.

AI-Powered, Autonomous Alert Investigation and Threat Hunting: Devo DeepTrace autonomously performs investigations at machine speed with attack-tracing AI, relieving analysts from mundane, repetitive tasks so they can focus on the more complex aspects of threat detection, investigation, and response.

BUILD YOUR SOC ON THE DEVO SECURITY DATA PLATFORM

The Devo Security Data Platform provides a comprehensive and unified solution for security operations, simplifying workflows and empowering organizations with complete visibility and control.

The single, unified platform that simplifies security operations

The Devo Security Data Platform combines data-agnostic SIEM, SOAR, UEBA, automated case management, and autonomous investigation and threat hunting to streamline workflows throughout the entire threat detection, investigation, and response lifecycle.

Self-service multitenancy that offers full visibility and control

Devo offers native, self-service multitenancy, enabling customers and partners to securely manage data access, content, and configuration across globally distributed operations while meeting data residency and compliance requirements at no extra cost.

All-inclusive packaging with varying levels of automation

Devo delivers simple, all-inclusive packaging, offering several easy-to-license SaaS options with varying levels of automation. Pricing for all packages is calculated based on a TB per day ingestion metric, making it easy to understand, predict, and budget.

Devo
3 Center Plaza
Suite 302
Boston, MA 02108

Devo replaces traditional SIEMs with a real-time security data platform. Devo's integrated platform serves as the foundation of your security operations and includes data-powered SIEM, SOAR, and UEBA. AI and intelligent automation help your SOC work faster and smarter so you can make the right decisions in real time. Learn more at **www.devo.com**.