DEVO
Data. Evolved.

Devo Security Operations

Cyber Security for the Modern Enterprise

SEE ALL THREATS
across the enterprise,
in real time

SECONDS, NOT HOURS OR DAYS
surface threats faster
to start remediation

DISRUPT DATA ECONOMICS
50% reduction in TCO
with no risk, no tradeoffs

All Data is Security Data

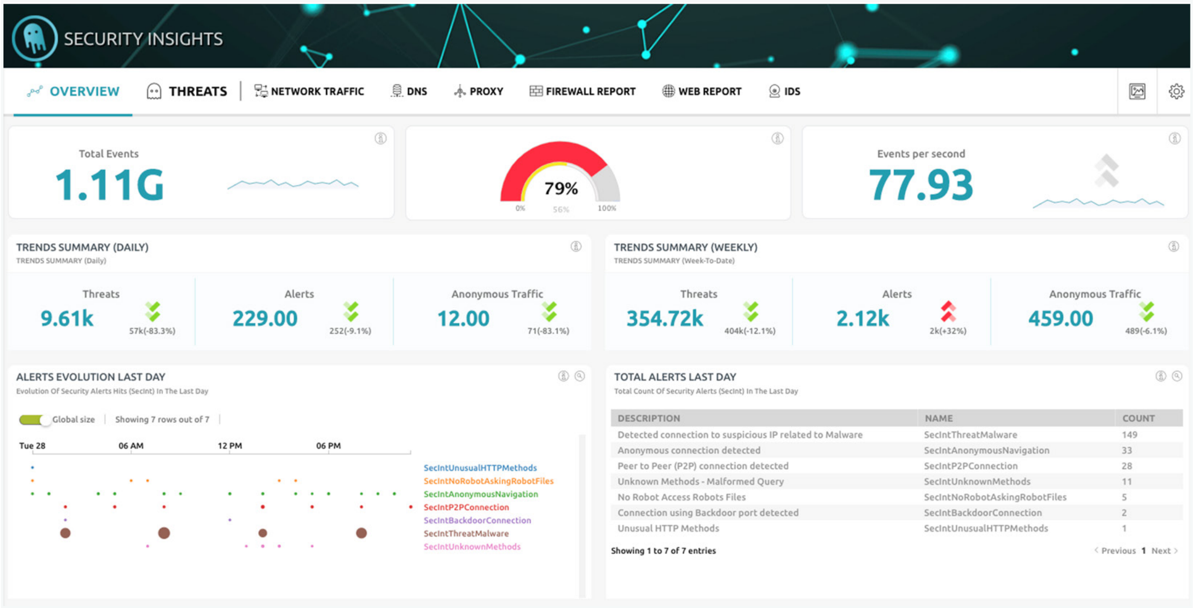
Growth in cloud technologies and new business applications in the modern enterprise is driving exponential security-related data growth and expanding the attack surface. Adversaries continue to evolve and adapt their methods. Malware has begun to incorporate AI, automating many aspects of an attacker's work and exploiting vulnerabilities in new and old technologies. Traditional rules-based security solutions and analytics tools are failing to keep up with evolving attacks and advanced threats.

In addition, increasing coverage for security is becoming cost-prohibitive from all aspects - infrastructure, data management and people. As the need to find new threats increases, security teams are faced with an untenable tradeoff – incur the high costs of data overhead, or accept risk in deciding which areas of the business to cover.

The need for speed compounds this risk. Security teams need to be able to hunt and see all threats in context, both across real-time events and historical data, while also performing retrospective forensic analysis. But security teams are spending too much time collecting and managing data when real-time analytics and timely remediation are necessary.

Devo Security Operations

Devo Security Operations, built on top of the Devo Data Operations Platform, is a highly scalable security analytics solution that frees security analysts from the burden of data management to focus on what matters most - fast identification and remediation of security threats at petabyte scale. The Devo Data Operations Platform is a full stack, multi-tenant, distributed analytics platform that provides the industry's most scalable and efficient cloud-native platform for real-time operational intelligence. Devo collects, enhances, analyzes, and visualizes all of an enterprise's machine data in a single, unified platform. Unlike traditional SIEMs, which sacrifice query performance or require vast investments in infrastructure and staffing, Devo is architected to access raw data, eliminating costly transformations and indexing to achieve speed, scale and superior TCO that keeps pace with exponential data growth.



Total Events 1.11G

Events per second 77.93

TRENDS SUMMARY (DAILY)
TRENDS SUMMARY (Daily)

Threats 9.61k 57k(-83.3%)
Alerts 229.00 252(-9.1%)
Anonymous Traffic 12.00 71(-83.1%)

TRENDS SUMMARY (WEEKLY)
TRENDS SUMMARY (Week-To-Date)

Threats 354.72k 404k(-12.1%)
Alerts 2.12k 2k(+32%)
Anonymous Traffic 459.00 489(-6.1%)

ALERTS EVOLUTION LAST DAY
Evolution Of Security Alerts Hits (SecInt) In The Last Day

Showing 7 rows out of 7

TOTAL ALERTS LAST DAY
Total Count Of Security Alerts (SecInt) In The Last Day

DESCRIPTION	NAME	COUNT
Detected connection to suspicious IP related to Malware	SecIntThreatMalware	149
Anonymous connection detected	SecIntAnonymousNavigation	33
Peer to Peer (P2P) connection detected	SecIntP2PConnection	28
Unknown Methods - Malformed Query	SecIntUnknownMethods	11
No Robot Access Robots Files	SecIntNoRobotAskingRobotFiles	5
Connection using Backdoor port detected	SecIntBackdoorConnection	2
Unusual HTTP Methods	SecIntUnusualHTTPMethods	1

Showing 1 to 7 of 7 entries

Figure 1: Overview Tab

See All Threats: Industry Leading Threat Management Framework and Interactive Analytics

Devo Security Operations ingests data from both traditional security sources and the growing number of non-traditional data sources. Sources can include proprietary data feeds, IT systems, security systems, identity and access solutions, manufacturing systems, and real-time machine data. Non-tranditonal data services can indlude cloud environments, business applications, SaaS applications, IoT device data and microservices. All data, both real time and historical, is easily correlated to enhance situational and security awareness.

Devo integrates real-time data from open or proprietary intelligence feeds with enterprise data and provides a collection of out-of-the-box threat intelligence feeds to enrich data sources.

Devo provides a visually-driven, interactive drag-and-drop interface to organize and correlate multiple data sources for security insight across the entire threat landscape. Users can easily create customized dashboards and views. A library of dashboards and widgets can be used to easily build new security applications, including attack detection, user & system activity tracking, and behavioral analysis, all wthout the need for advanced coding. The Devo interface speeds exploration and drill-down to raw data to quickly understand hidden relationships, reveal advanced threats, and enable quick detection and response. All workflow activity can be captured and stored for automation, auditing or reporting.

Flexible role-based access control ensures only specified users have access to applications as well as data, whether performing forensic analysis or threat hunting across the full repository of security data.

Act in Seconds, Not Hours with Advanced Analytics and Incidents Detection

Analytics and insight are useless without timely action. Devo pairs raw speed of analysis with advanced analytics and ML, empowering users to predict, identify, and act on threats in real time. Existing security solutions take too long to collect, query and analyze data necessary to detect intrusions and threats, leaving enterprises at risk from real-time attacks as well as unrevealed breaches.

Unlike traditional security solutions, Devo does not normalize, index or otherwise transform data at ingest, speeding incident detection and response. Data is stored in its raw format and is available for query as soon as it's written to disk. Devo ingests data at the rate of 150,000 events per second, per core, while simultaneously analyzing 1 million events per core. The platform scales vertically as well as horizontally.

Disrupt the Economics of Security Data

Devo fundamentally changes the way organizations collect, analyze, alert on and visualize growing volumes of security and operational data. Architected for organizations with terabytes of streaming data coming in every day and with petabyte-scale data stores, the Devo architecture offers significant savings in both direct operational costs and resources while ensuring real-time visibility across the entire threat landscape. All operations on data are parallelized, ensuring Devo delivers performance up to 50 times faster than competing solutions using 80 percent less infrastructure.

Improve Security Operations with Devo

Devo Security Operations can function as a complete stand-alone security analytics solution, or it can extend and complement existing security solutions and tools, such as SIEM. This integration with the platform extends the value of existing investments in security infrastructure.

Enterprises in financial services, manufacturing, telco, and more use Devo Security Operations to increase business efficiency and security, reduce cyber threats and operational costs, and make real-time decision-making a competitive advantage. For more information on getting started with Devo, contact **sales@devo.com**.

CAIXABANK ACCELERATES AND SECURES DIGITAL TRANSFORMATION WITH DEVO

- □ Significantly accelerate forensic analysis and incident response
- □ Enrich the entire CaixaBank security stack with real-time security analytics
- □ Extend and enhance the effectiveness of its SIEM and security operations

10 TB/DAY COLLECTED

5 PB/DAY ANALYZED

TECHNICAL USERS

ABOUT DEVO

Devo delivers real-time operational and business insights from analytics on streaming and historical data to operations, IT, security and business teams at the world's largest organizations. The Devo Data Operations Platform collects, enhances and analyzes machine, business and operational data, at scale, from across the enterprise.