



## **GEMINI DATA:**

Intelligent security analysis  
for the modern enterprise

---



## GEMINI SOLUTION

Gemini for Security Operations delivers actionable Stories that connect incidents and events to higher-level problems by leveraging AI/ML algorithms, intelligent data interpretation and data mapping to business context. Data that is relevant for security posture and threat exposure — including network and user activity, malware detections as well as information from Identity and Access Management solutions — is autonomously analyzed and delivered to respective key stakeholders in the organization.

Gemini's Autonomous Data Infrastructure (ADI) enables analysts to easily and rapidly access data that is stored in enterprise data platforms and topological systems, such as SIEMs, HDFS, RDBMs, CMDBs and Centralized Log Management tools by virtualizing these different technologies with open standards. A single unified query gives the power of converging massive amounts of data that is critical for full contextual analysis based on true facts at scale. Data virtualization additionally reduces dramatically the amount of data movement over the network.

Gemini's ADI uses a single microservices architecture with optimization for Zero Trust networks for maximum enterprise security and autonomous

resource management. It offers GPU support to deliver the promise of an AI/ML-ready data infrastructure for real cognitive analysis at scale.

The high degree of data management and interpretation automation of Gemini's ADI enables human analysts to focus on higher level intelligent analysis assisted by machine intelligence for joint collaboration and substantial reduction of Mean Time to Action (MTTA).

In summary, Gemini's ADI delivers a complete stack for future-oriented security operations and analysis:

- Action-driven analysis with machine-generated Gemini Stories
- Data availability across all enterprise data with AI/ML optimization
- Data exploration with facts and full context and single query across all data platforms at scale
- Unified data across all enterprise silos or platforms with open standards architecture
- Zero Trust network optimization for maximum enterprise security

### Automate Your Data Platform:

Automate the deployment and management of data platforms like Splunk, Hadoop, and Elastic, removing the daunting complexity of deploying and scaling data solutions while ensuring performance is maintained. We make it easy to deploy and manage across complex architectures, multiple locations, and hybrid environments.

### AI Accelerated Analysis:

Apply AI across your unified data model for accelerated analysis across Enterprise IT, reducing IT noise to meaningful stories understood by all. Link datasets from disconnected systems with an intuitive interface, breaking down data silos to achieve meaningful contextual intelligence that accelerates problem solving and incident remediation.

### Support for Your Data Journey:

Gemini Enterprise is delivered on premise or in the cloud, managed or unmanaged, to meet you where you are on your data journey and grow with you. The best part - with Gemini Care, our global team of certified experts are here to help you 24/7.



**Security**



**Compliance**



**IT Operations**

## USE CASES

### AI/ML-Driven Incident Correlation

Reduce Mean Time to Action with machine generated Gemini Stories that indicate higher-level problems. With use of AI/ML algorithms, security events and alerts from SIEMs and other data sources are connected with topological information from Configuration Management Databases (CMDB) or Identity and Access Management (IAM) systems. Stories provided by Gemini's Autonomous Data Infrastructure reduce manual error-prone aggregation and incident drill down dramatically.

### Visual-Aided Data Investigation

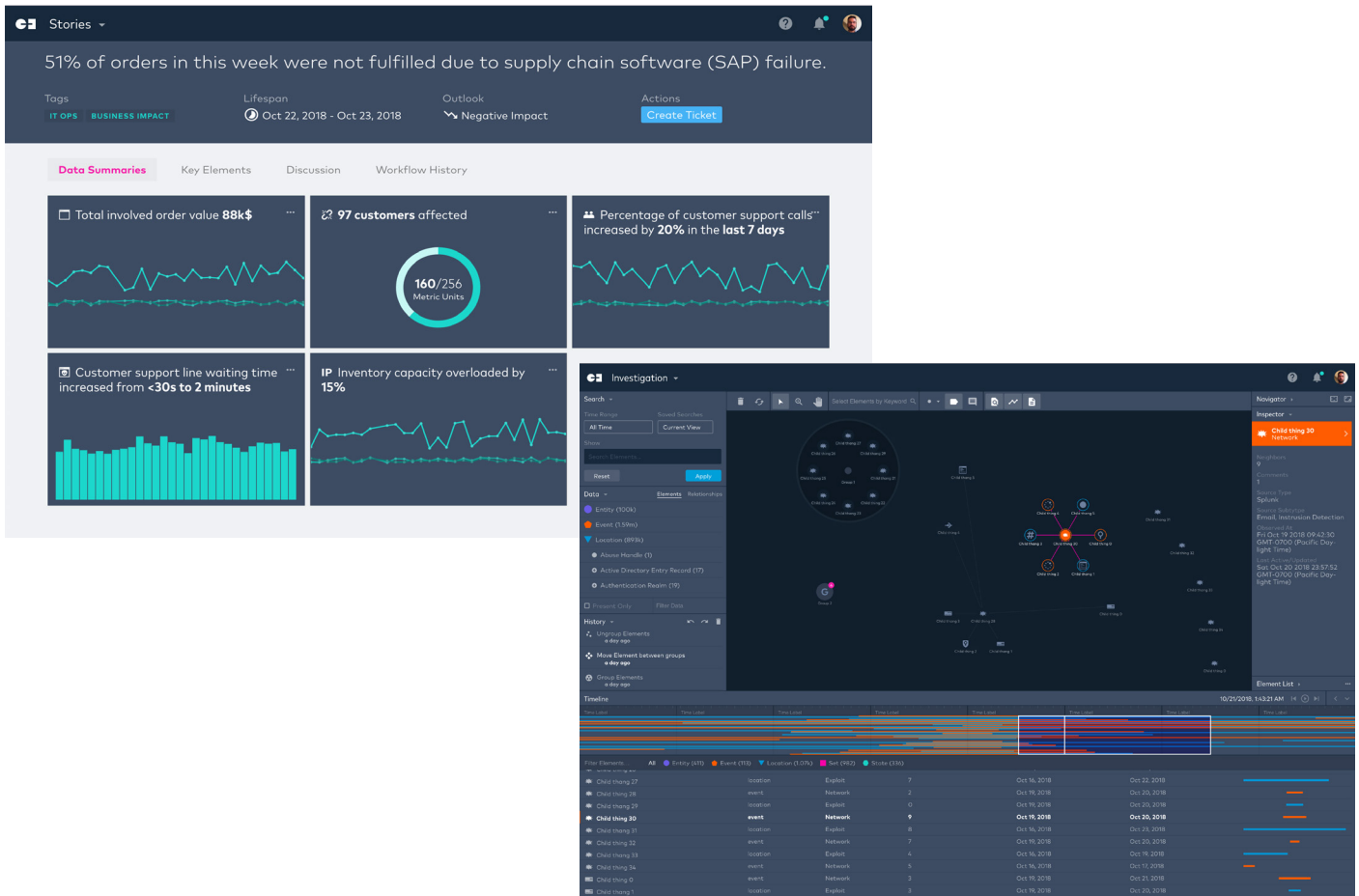
Understand the context of data elements and pivot relationships of each neighbor without being limited by static reports. Use Gemini's simplified vocabulary to identify and understand data easily.

### Data Hub for Rapid Analysis

Run a single unified query across all enterprise data sets to analyse data from different angles without need to know the specifics of each data typologies. Proof and enrich facts observed in machine data by automatic augmentation with topological data.

### Fact-Based Data Exploration

Get a quick overview of the current security situation by analysing true facts and their full context. Gemini's Autonomous Data Infrastructure works assumption-free and reduces analysis overhead by connecting all data to business context and separating real issues that require human attention from noise.



## GEMINI ENTERPRISE - FULL STACK ANALYSIS SOLUTION BUILT FOR THE FUTURE

Gemini's Autonomous Data Infrastructure delivers the promise of analysis with business context by leveraging AI/ML technologies. The architecture is built for today's scalability requirements to rapidly analyse massive amounts of data from any type of source with intelligent resource management. It is designed to increase the range of data and knowledge with open standards. Analysts can focus on their highly demanding analytical tasks and let Gemini's Autonomous Data Infrastructure do the heavy labor.



### Converge

Data availability across all enterprise data with AI/ML optimization.

### Virtualize

Unified data across silos or platforms with open standards architecture.

### Analyze

Action driven analysis and machine generated stories.