Salt Security: Discover and Secure Sensitive API Data

Introduction

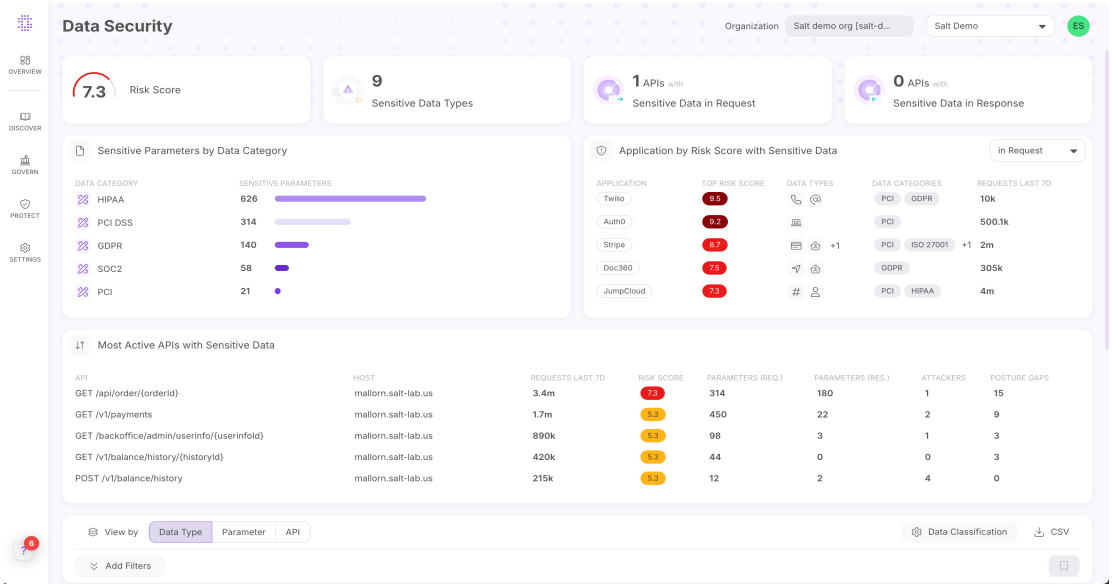
APIs play a crucial role in modern business by enabling vital data exchanges, including the exchange of sensitive information. Effectively managing and securing this data during its transmission through APIs poses significant challenges. Organizations require clear insights into the locations of sensitive data, its flow, and the associated risks to ensure security and compliance.

Salt Security's Data Security capability offers vital oversight and control over sensitive data handled by your APIs. By examining data in transit, security teams can gain a deeper understanding of their sensitive data environment, assess risks, and improve API security. This functionality is further improved by new Widgets in the Data Security Interface, which simplify monitoring and risk evaluation.

Key Capabilities

The Data Security capability offers powerful capabilities for discovering and securing sensitive API data:

- **Comprehensive Sensitive Data Insights:** Get a consolidated view of sensitive parameters and their presence across data categories defined in your environment. Widgets and the interface provide application-level insights (via API labels), offering business context for your API landscape and sensitive data locations.
- **Granular Visibility of Sensitive Data Types and Categories:** Understand specific sensitive data types and categories associated with your APIs. This visibility extends to APIs triggering posture gaps, clarifying risks linked to vulnerable APIs handling sensitive data.



- **Contextual Risk Evaluation Integrated with Posture Gaps:** Sensitive Data Types and Categories are displayed in the Posture Gaps table for triggering APIs. This context enables security teams to better assess risk by understanding whether vulnerabilities are associated with APIs handling sensitive information, thereby highlighting the urgency of remediation.
- **Streamlined Analysis within the Data Security Interface:** The interface offers views (by Data Type, Parameter, API) where Data Categories are visible. This provides a single snapshot to correlate sensitive parameters, data types, and processing APIs, streamlining analysis of sensitive data flow.

- **Enhanced Visibility with Data Security Widgets:** New Widgets in the Data Security Interface provide high-level assessments of sensitive data flows, showing APIs handling sensitive data in requests vs. responses. Gain insights into active APIs with sensitive data, associated Posture Gaps, and attackers. These widgets simplify monitoring and highlight critical areas.
- **Targeted Analysis with Filtering:** Utilize data types and Data Categories as filters in the Posture Gaps table for targeted analysis. Prioritize remediation efforts based on the sensitivity of the data involved.

Business Value

The Salt Security Data Security capability with its new widgets delivers significant value:

- **Enhanced Visibility and Observability:** Gain consolidated visibility into sensitive data, its categories, and its presence across applications and APIs, improving understanding of data movement.
- **Improved Risk Assessment and Prioritization:** Better evaluate posture gaps and sensitive data exposure by understanding the type and category of sensitive data an API handles, aiding in prioritizing remediation.
- **Streamlined Analysis:** Simplify analyzing sensitive data flow and exposure through correlated views and widget summaries, enabling faster incident response.
- **Simplified Risk Management for Sensitive Data:** Widgets provide high-level assessments and insights into sensitive data flows, simplifying risk understanding and management for sensitive API information.

Conclusion

The Data Security capability, enhanced by new Data Security Widgets, is crucial for organizations that monitor and secure sensitive data processed by APIs. By providing enhanced observability into data flow, simplified risk assessment via high-level insights, and correlating sensitive data context with API posture gaps and attacker activity, Salt Security helps customers strengthen security, manage risk, and maintain compliance against evolving API threats.