

## Salt Security API Posture Governance

### The Challenge: Securing APIs as Critical IT Assets — And Meeting Compliance Mandates

APIs have become indispensable IT assets, enabling seamless data exchange, streamlined business processes, and enhanced digital experiences. Just like traditional IT infrastructure, APIs require careful management and protection. With rapidly developed APIs through the power of AI, the challenges will become even greater. Yet, many organizations struggle to integrate APIs into their broader IT asset management and posture governance strategies. This creates security blind spots, leaving critical data and applications vulnerable to attacks, and significantly complicates the ability to meet stringent regulatory and industry compliance requirements.

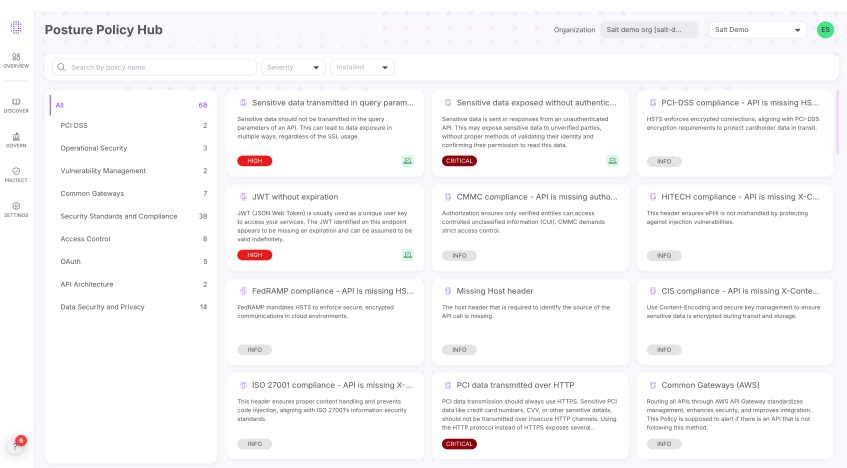
### The Salt Security Solution:

#### Proactive, Integrated API Posture Governance for Enhanced Security and Compliance

Salt's API Posture Governance engine enables organizations to manage APIs with the same level of rigor as any other IT asset. The solution assists in comprehensive risk management and proactive security, ensuring that your API landscape aligns seamlessly with your overall Posture Governance strategies and strengthens your compliance posture. This entails extending existing IT asset management practices to include APIs. It involves inventorying all APIs, both internal and external-facing ones, alongside traditional IT infrastructure components. Classifying APIs based on their business criticality and the sensitivity of the data they access, and regularly evaluating API security posture against industry best practices and your organization's internal security policies. By treating APIs as IT assets, you gain a comprehensive understanding of your security landscape. You can prioritize remediation efforts to optimize the security of your most valuable resources, directly contributing to a stronger compliance position.

### How API Posture Governance Strengthens Overall IT Security and Compliance

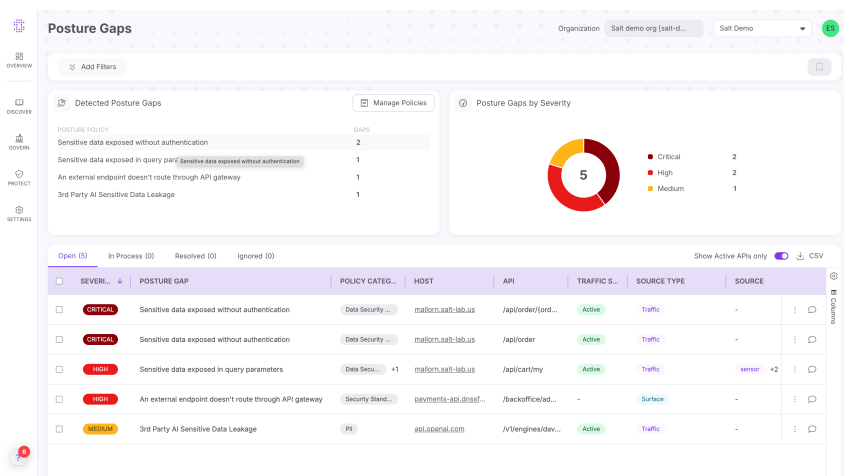
- **Treat APIs as First-Class IT Assets:** It's essential to consider **APIs as any other IT asset**. As with other assets, gaining visibility into your API ecosystem is a critical first step. Salt provides you with this capability quickly through our **continuous API discovery**. This is essential for a holistic understanding of your attack surface.
- **Consistent Policy Enforcement:** Extend established IT security policies and access controls to your APIs. Use pre-built policies or easily create customized, granular API-specific policies to ensure that authentication, authorization, input validation, and other security measures are consistently applied across the entire API ecosystem. Salt provides nearly **70 pre-defined out-of-the-box policies**, readily available in the Posture Policies Hub, to accelerate your governance efforts and ensure adherence to common compliance frameworks. The **unique Posture Policies Hub** serves as a central place for Security Managers to discover, deploy, and maintain the API Governance policies that safeguard the organization's security frameworks.



- **Centralized Risk Prioritization:** Salt's Posture Governance engine analyzes API risks as they are tied into your broader IT ecosystem. Prioritization is based on the potential impact to your business, empowering you to focus remediation efforts where they matter most from both a security and compliance perspective.
- **Build Security into API Design:** With ecosystem enrichment, you can embed **API posture checks into CI/CD pipelines**, shifting API security left for faster remediation.

This aligns with DevSecOps practices, enabling you to treat APIs as integral components of secure application development, thereby helping to integrate compliance requirements into the development lifecycle.

- **Compliance Through Continuous Assessment:** Salt provides API Posture Governance visibility, simplifying the process of demonstrating **adherence to regulations such as PCI DSS, HIPAA, and GDPR**. Treating APIs as core assets provides the tracking and proof necessary for IT governance and compliance audits. Consistent API posture governance is key to providing the continuous assessment and documented evidence required by auditors.



## The Bottom Line:

### A Stronger API Security Posture, End-to-End, with Enhanced Compliance

Salt Security's API Posture Governance helps you:

- **Maximize Asset Value:** Secure your API assets to ensure they continue to provide business value without introducing undue risk.
- **Reduce Risk:** Identify and mitigate API vulnerabilities before they're exploited, protecting your organization's data and reputation.
- **Streamline Compliance:** Manage APIs as IT assets, meeting regulatory requirements, and easing the burden of audit processes. Proactive posture governance simplifies demonstrating compliance.
- **Accelerate, Secure Innovation:** Empower developers with guardrails that promote secure API development, enabling agility while building trust.

## Why Choose Salt Security?

Salt Security uniquely combines API-specific security expertise with an understanding of broader IT security principles. Our dedicated API Posture Governance engine integrates seamlessly into your existing IT asset management and security frameworks. Using our AI-powered platform, elevate the protection of your API assets, strengthening your overall IT security posture to meet the challenges of a rapidly evolving threat landscape and ensuring continuous compliance.

