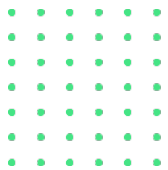


Solution Brief: Salt Security API Posture Governance

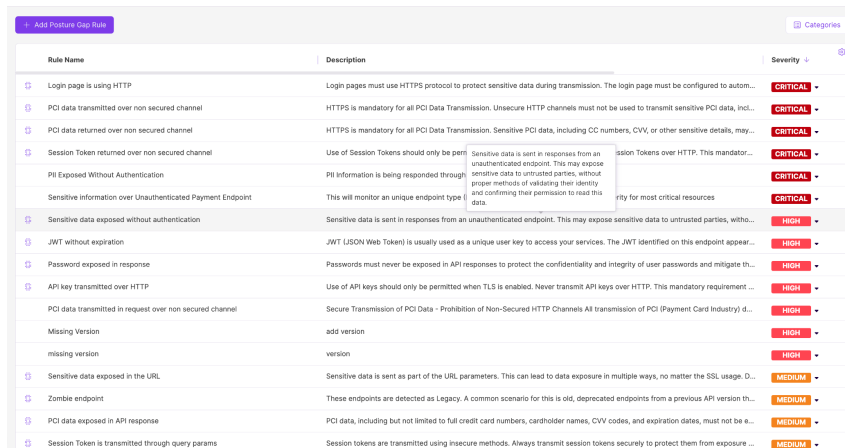
The Challenge: Securing APIs as Critical IT Assets



APIs have become indispensable IT assets, powering data exchange, business processes, and seamless 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 need help integrating APIs into their broader IT asset management and posture governance strategies. This creates security blind spots, leaving critical data and applications vulnerable to attacks.

The Salt Security Solution: Proactive, Integrated API Posture Governance

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. 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 and can prioritize remediation efforts to optimize the security of your most valuable resources.



Rule Name	Description	Severity
Login page is using HTTP	Login pages must use HTTPS protocol to protect sensitive data during transmission. The login page must be configured to autom...	CRITICAL
PCI data transmitted over non secured channel	HTTPS is mandatory for all PCI Data Transmission. Unsecure HTTP channels must not be used to transmit sensitive PCI data, incl...	CRITICAL
PCI data returned over non secured channel	HTTPS is mandatory for all PCI Data Transmission. Sensitive PCI data, including CC numbers, CVV, or other sensitive details, may...	CRITICAL
Session Token returned over non secured channel	Use of Session Tokens should only be permitted over secure channels. Sensitive data is sent in responses from an unauthenticated endpoint. This may expose sensitive data to untrusted parties, without proper methods of validating their identity and confirming their permission to read this data.	CRITICAL
PII Exposed Without Authentication	PII information is being responded through unauthenticated endpoints. This may expose sensitive data to untrusted parties, without proper methods of validating their identity and confirming their permission to read this data.	CRITICAL
Sensitive information over Unauthenticated Payment Endpoint	This will monitor a unique endpoint type for most critical resources	CRITICAL
Sensitive data exposed without authentication	Sensitive data is sent in responses from an unauthenticated endpoint. This may expose sensitive data to untrusted parties, witho...	HIGH
JWT without expiration	JWT (JSON Web Token) is usually used as a unique user key to access your services. The JWT identified on this endpoint appear...	HIGH
Password exposed in response	Passwords must never be exposed in API responses to protect the confidentiality and integrity of user passwords and mitigate th...	HIGH
API key transmitted over HTTP	Use of API keys should only be permitted when TLS is enabled. Never transmit API keys over HTTP. This mandatory requirement ...	HIGH
PCI data transmitted in request over non secured channel	Secure Transmission of PCI Data - Prohibition of Non-Secured HTTP Channels All transmission of PCI (Payment Card Industry) d...	HIGH
Missing Version	add version	HIGH
missing version	version	HIGH
Sensitive data exposed in the URL	Sensitive data is sent as part of the URL parameters. This can lead to data exposure in multiple ways, no matter the SSL usage, D...	MEDIUM
Zombie endpoint	These endpoints are detected as Legacy. A common scenario for this is old, deprecated endpoints from a previous API version th...	MEDIUM
PCI data exposed in API response	PCI data, including but not limited to full credit card numbers, cardholder names, CVV codes, and expiration dates, must not be e...	MEDIUM
Session Token is transmitted through query params	Session tokens are transmitted using insecure methods. Always transmit session tokens securely to protect them from exposure ...	MEDIUM



How API Posture Governance Strengthens Overall IT Security

- Treat APIs as First-Class IT Assets:** It's important to consider APIs as any other IT asset, and as with other assets, getting visibility into your API ecosystem is a critical first step. Salt provides you with this capability quickly through our integrated API discovery. This is essential for a holistic understanding of your attack surface.

Rule Name	Description	Severity
Login page is using HTTP	Login pages must use HTTPS protocol to protect sensitive data during transmission. The login page must be configured to autom...	CRITICAL
PCI data transmitted over non secured channel	HTTPS is mandatory for all PCI Data Transmission. Unsecure HTTP channels must not be used to transmit sensitive PCI data, incl...	CRITICAL
PCI data returned over non secured channel	HTTPS is mandatory for all PCI Data Transmission. Sensitive PCI data, including CC numbers, CVV, or other sensitive details, may...	CRITICAL
Session Token returned over non secured channel	Use of Session Tokens should only be permitted over secure channels. Sensitive data is sent in responses from an unauthenticated endpoint. This may expose sensitive data to unauthorized parties, without proper methods of validating their identity and confirming their permission to read this data.	CRITICAL
PII Exposed Without Authentication	PII information is being responded through unauthenticated endpoints. This may expose sensitive data to unauthorized parties, without proper methods of validating their identity and confirming their permission to read this data.	CRITICAL
Sensitive information over Unauthenticated Payment Endpoint	This will monitor a unique endpoint type that is used for payment processing. Sensitive data is sent in responses from an unauthenticated endpoint. This may expose sensitive data to unauthorized parties, without proper methods of validating their identity and confirming their permission to read this data.	CRITICAL
Sensitive data exposed without authentication	Sensitive data is sent in responses from an unauthenticated endpoint. This may expose sensitive data to unauthorized parties, without proper methods of validating their identity and confirming their permission to read this data.	HIGH
JWT without expiration	JWT (JSON Web Token) is usually used as a unique user key to access your services. The JWT identified on this endpoint appears to be missing an expiration date. This may allow an attacker to use the token indefinitely.	HIGH
Password exposed in response	Passwords must never be exposed in API responses to protect the confidentiality and integrity of user passwords and mitigate the risk of credential theft.	HIGH
API key transmitted over HTTP	Use of API keys should only be permitted when TLS is enabled. Never transmit API keys over HTTP. This mandatory requirement is in place to protect the confidentiality and integrity of API keys.	HIGH
PCI data transmitted in request over non secured channel	Secure Transmission of PCI Data - Prohibition of Non-Secure HTTP Channels All transmission of PCI (Payment Card Industry) data must be over a secure channel (HTTPS).	HIGH
Missing Version	add version	HIGH
missing version	version	HIGH
Sensitive data exposed in the URL	Sensitive data is sent as part of the URL parameters. This can lead to data exposure in multiple ways, no matter the SSL usage. Data exposed in the URL is not encrypted and is easily accessible to anyone who can intercept the traffic.	MEDIUM
Zombie endpoint	These endpoints are detected as Legacy. A common scenario for this is old, deprecated endpoints from a previous API version that are still accessible.	MEDIUM
PCI data exposed in API response	PCI data, including but not limited to full credit card numbers, cardholder names, CVV codes, and expiration dates, must not be exposed in API responses.	MEDIUM
Session Token is transmitted through query params	Session tokens are transmitted using insecure methods. Always transmit session tokens securely to protect them from exposure to unauthorized parties.	MEDIUM

- Consistent Policy Enforcement:** Extend established IT security policies and access controls to your APIs. Use pre-built rules or easily create customized granular API-specific rules, ensuring authentication, authorization, input validation, and other security measures are consistently applied across the full API ecosystem.
- 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.
- 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 mirrors DevSecOps practices, enabling you to treat APIs as integral components of secure application development.
- Compliance Through Continuous Assessment:** Salt provides API Posture Governance visibility, simplifying the process of demonstrating adherence to regulations (PCI DSS, HIPAA, GDPR, etc.). Treating APIs as core assets gives you the tracking and proof required for IT governance and compliance audits.

PCI data transmitted over non secured channel

Rule Name: PCI data transmitted over non secured channel

Status: Active

Severity: CRITICAL

Description: HTTPS is mandatory for all PCI Data Transmission. Unsecure HTTP channels must not be used to transmit sensitive PCI data, including CC numbers, CVV, or other details.

Remediation: 1. All communication channels involved in transmitting PCI data must utilize HTTPS, which employs SSL/TLS encryption protocols. 2. Disable non-secured protocols on systems and applications involved in the processing or transmission of PCI data to prevent accidental usage.

Category: Data Security and Privacy, PCI DSS, Security Standards and Compliance

Rule Conditions: Find Request Anywhere with Sensitive Data Type is Credit Card Details and Protocol is HTTP

[View in the Inventory](#)



The Bottom Line: A Stronger API Security Posture, End-to-End

Salt Security's API Posture Governance helps you:

- **Maximize Asset Value:** Secure your API assets to ensure they provide continued 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.
- **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.

