

# The Hidden Dangers of Zombie and Shadow APIs: A Comprehensive Security Approach

.....

Over 40% of organizations have no processes in place to discover APIs.

## Executive Summary

In today's complex digital environment, APIs are crucial for business operations and innovation, but they also pose significant security risks, especially from zombie and shadow APIs. These concealed or undocumented endpoints can be exploited by attackers, leading to data breaches, unauthorized access, and compliance violations. Traditional security tools fail to address these threats because they rely on manual processes and limited visibility. Salt Security offers a comprehensive API Protection Platform that automatically discovers, monitors, and secures all APIs, including zombie and shadow APIs, providing complete visibility and proactive threat detection.

## The Challenge of Zombie and Shadow APIs

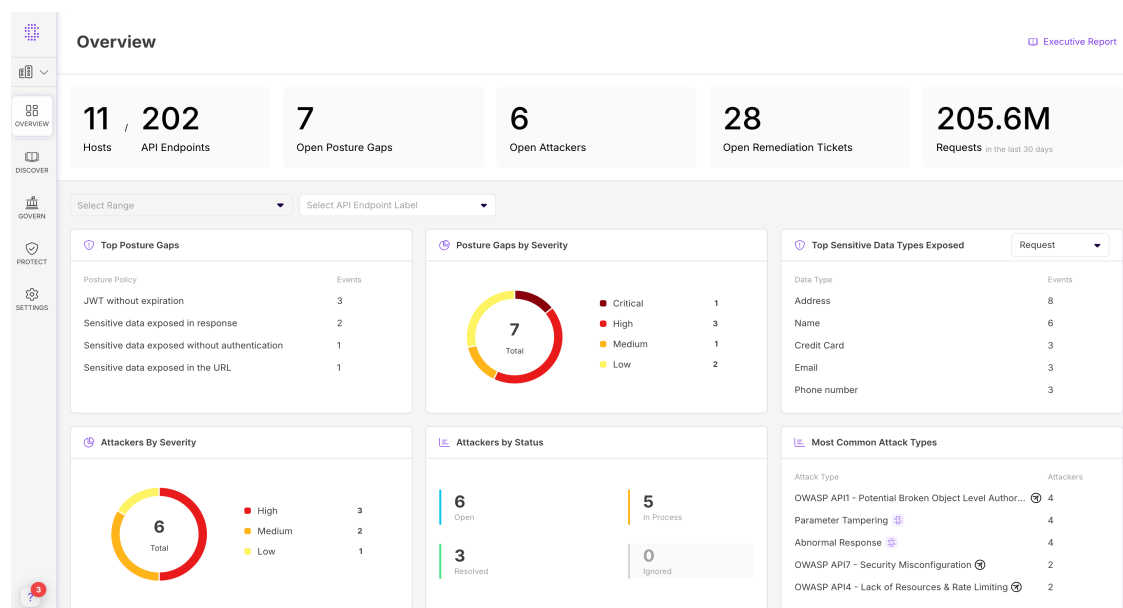
- **Zombie APIs:** These are outdated or deprecated endpoints that still exist in the environment, posing potential vulnerabilities.
- **Shadow APIs:** Created without the security team's knowledge or approval, shadow APIs often emerge from rapid development cycles (including AI-generated APIs) and lack proper documentation.

The presence of these concealed APIs presents considerable risks due to their lack of visibility, inconsistent security posture, compliance risks, and operational inefficiencies. Conventional tools are ineffective in addressing these issues because they rely on manual processes and static documentation and offer limited visibility into the dynamic API landscape.



# Salt Security's API Protection Platform

Salt Security provides a complete solution to tackle the challenges posed by zombie and shadow APIs.



- 1. Comprehensive API Discovery:** Continuous and automatic discovery of all APIs, including zombie and shadow APIs, provides complete visibility into the API landscape.
- 2. API Posture Governance:** Apply posture governance rules to discovered APIs to ensure compliance with organizational and industry-specific guidelines, reducing risk.
- 3. Advanced Behavioral Analysis:** Utilizes machine learning and AI to identify anomalies, outdated endpoints, and undocumented activity, enabling proactive issue detection.
- 4. Real-time Threat Detection and Response:** Our system actively monitors and secures all APIs, even obscure ones, against attacks. It provides deep insights into API behavior, enabling quick threat identification and mitigation.
- 5. Extend API Security Left:** Our system integrates into the development pipeline to address zombie and shadow APIs early in the development process, preventing the creation of risky, undocumented APIs.



## Why Choose Salt

Salt Security is the only solution that provides the comprehensive capabilities needed to fully secure zombie and shadow APIs. It integrates deep discovery, continuous monitoring, governance, and proactive threat detection into a single, AI-infused platform. By selecting Salt Security, organizations can guarantee that their entire API landscape is resilient, compliant, and secure, allowing for innovation without any compromise.

## Conclusion

Zombie and shadow APIs pose a significant threat to organizational security. Conventional tools are inadequate in addressing these issues, making Salt Security's comprehensive API Protection Platform the optimal solution for ensuring complete API security.

