Salt Security Platform: Reducing Risk In the Age of Rapidly Expanding API Utilization

The Benefits of Salt Security Platform

- **API Ecosystem Visibility:** Rapidly understand the scope of APIs deployed across your organization.
- **Reduced Risk:** Proactively identifying and mitigating API security threats significantly reduces the likelihood of successful attacks.
- **Improved Compliance:** Automated policy enforcement and real-time alerts ensure adherence to industry standards and internal regulations.
- **Faster Time to Value:** Rapid deployment and immediate insights into your API landscape accelerate your security journey.
- **Enhanced Operational Efficiency:** Automation eliminates manual tasks, streamlines security processes, and frees up valuable resources.
- **Reduced Costs:** Mitigating data breaches and other security incidents minimizes financial losses and reputational damage.

The Looming Threat

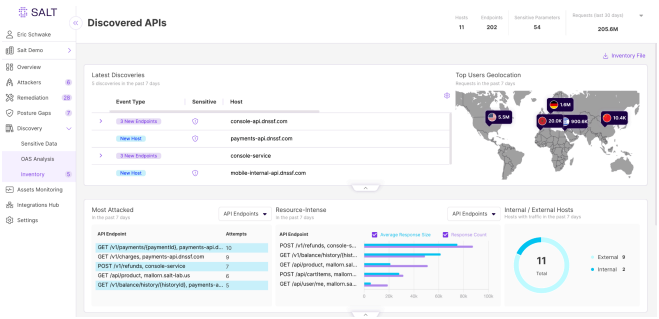
APIs are essential to modern applications and digital transformation, from mobile experiences to complex enterprise integrations. However, their increasing growth has created a new complex and vulnerable attack surface for threat actors to take advantage of. Traditional security tools, which are challenged to detect new threats targeting APIs, need help understanding and protecting APIs. This leaves organizations open to a wide range of threats, including:

- Data Breaches: Hackers can exploit insecure APIs to steal sensitive data like customer information, intellectual property, and financial records.
- Account Takeovers: Malicious actors can gain unauthorized access to accounts or applications by compromising API credentials or exploiting vulnerabilities.
- Denial-of-Service Attacks: Attackers can overwhelm APIs with traffic, rendering applications and services unavailable.
- Logic Flaws and Business Logic Attacks: Exploiting vulnerabilities in API logic can lead to unauthorized access, data manipulation, or even complete system compromise.

The Salt Solution

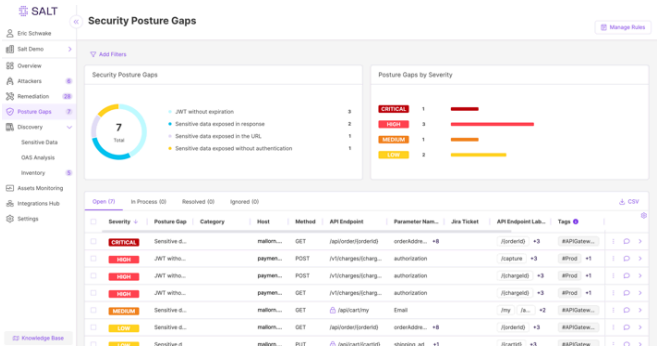
The Salt Security Platform offers a comprehensive solution for API risk reduction, empowering organizations to secure their APIs proactively and confidently. Unlike traditional tools, Salt is built from the ground up for APIs, providing deep visibility, robust protection, and seamless integration with existing security ecosystems. Salt's platform has been built from the ground up to provide security practitioners with easily accessible and actionable information to quickly understand their API ecosystem and act upon any threats that may be attacking them.

Unveiling the Hidden Landscape: API Discovery



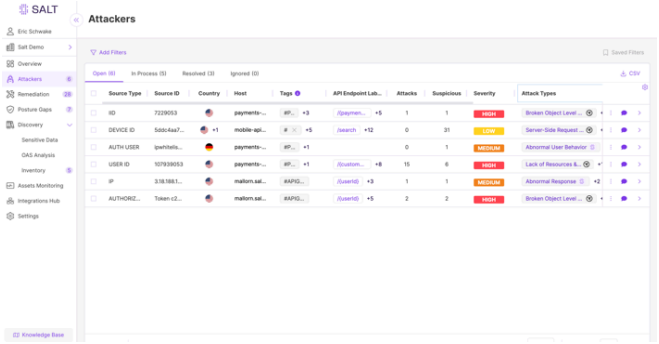
The journey to securing APIs starts with **uncovering all APIs** within your infrastructure, including even the elusive "shadow APIs" that may have been developed outside of formal processes. This comprehensive discovery, utilizing various techniques like API traffic analysis and protocol identification, ensures no API escapes scrutiny. Salt goes beyond mere identification, **analyzing API traffic** to understand functionality, data sensitivity, and potential attack vectors, providing valuable context for informed security decisions.

Enforcing Policies: API Posture Governance



Once your API landscape is mapped, Salt helps you **define and enforce security policies**. These policies can be tailored to specific API types, functions, and data sensitivity levels, ensuring consistent security practices across your organization. Salt provides many prebuilt policies but allows for the manual creation of policies to suit organizational needs. Salt automates policy enforcement, eliminating manual intervention and reducing human error. Real-time alerts for policy violations and misconfigurations keep you vigilant, allowing for swift remediation before attackers exploit weaknesses.

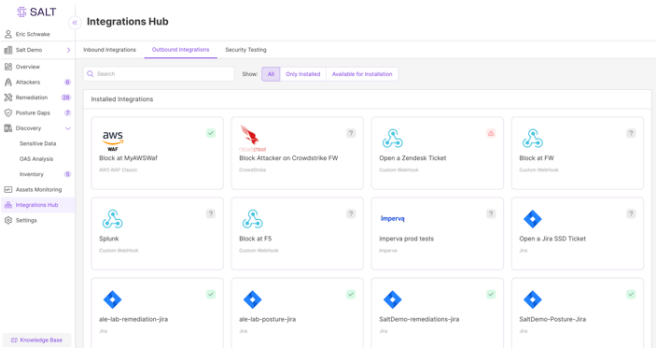
Shielding Against Advanced Threats: API Behavioral Threat Protection



Protecting your APIs requires more than just static policies. Salt employs advanced **behavioral threat protection** powered by AI and machine learning. This dynamic approach analyzes user behavior within the context of normal API usage patterns, identifying **anomalous activities** that

could indicate malicious intent. Salt's advanced detection techniques go beyond traditional signatures, safeguarding you even against zero-day attacks and novel threats. When suspicious activity arises, Salt **immediately shares threat intel** with the rest of your ecosystem, helping prevent damage before it occurs.

Beyond the Platform: API Security Ecosystem Enrichment



Salt doesn't operate in isolation. It seamlessly **integrates with your existing security tools**, including API gateways, web application firewalls (WAFs), security information and event management (SIEM) systems, and dynamic application security testing (DAST) tools. This **unified approach** provides a holistic view of your security posture and enables comprehensive threat intelligence sharing across platforms. Our ecosystem enrichment capabilities allow SOC analysts to continue working in the tools they are used to while taking advantage of the API threat intel provided by Salt Security. Salt's extensible API also allows for custom integrations and data enrichment, empowering you to tailor security to your specific needs and leverage custom threat intelligence sources.

Conclusion:

In today's rapidly expanding cloud-forward world, APIs are the lifeblood organizations rely on for the business. The Salt Security Platform offers a comprehensive and effective solution for API risk reduction, empowering you to secure your applications and the APIs they run on, protect your data, and confidently navigate the ever-evolving threat landscape.

With Salt, you can unlock the full potential of APIs while safeguarding your business from the ever-growing risks.