SALT

SOLUTION BRIEF

Salt Security Behavioral Threat Protection: Defending Against Evolving API Attacks

The Challenge: The Hidden Danger in Normal API Traffic

Traditional security tools are effective in identifying well-known forms of cyber attacks and vulnerabilities targeting APIs. However, their capability to detect new and sophisticated attacks, which imitate normal user behavior, is limited. In recent times, attackers have become smarter and have realized that mimicking legitimate API traffic is a successful technique. By mimicking normal user behavior, attackers can carry out subtle, low-and-slow attacks that identify weaknesses, quietly steal data, and manipulate business logic. These attacks pose a significant threat to organizations whose business depends on APIs.

The Salt Solution: Behavioral Threat Protection Powered by Our Patented Intent Engine

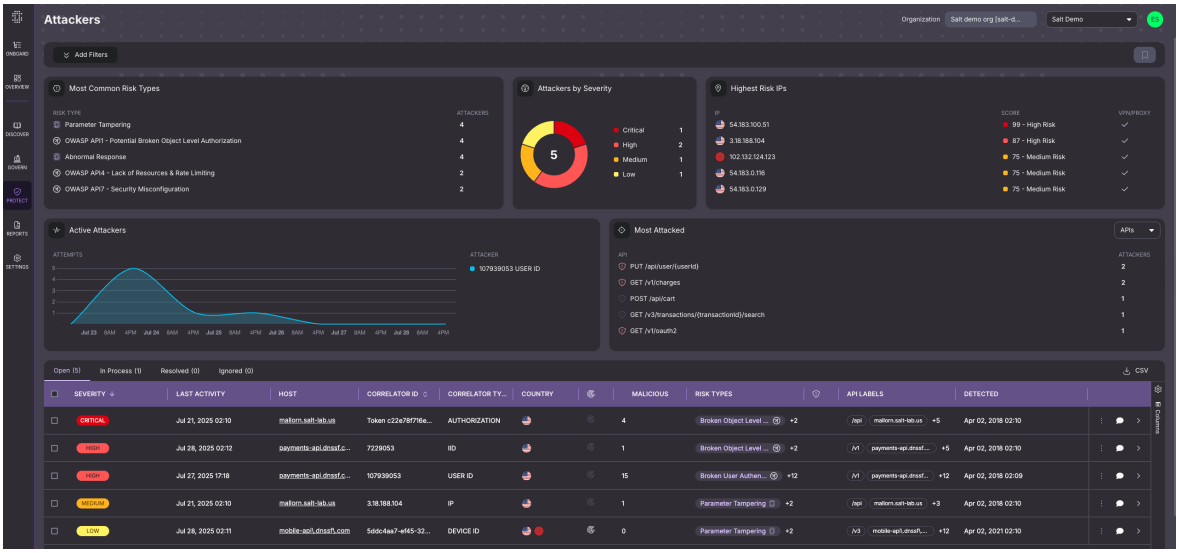
Salt Security's industry-first Behavioral Threat Protection tackles this challenge head-on by leveraging the power of our patented artificial intelligence (AI) and machine learning (ML) Intent Engine. By analyzing vast amounts of API traffic data, Salt comprehensively understands what constitutes normal API behavior for your organization. This understanding goes beyond just identifying specific API calls; it encompasses the entire interaction context, including historical behavior patterns and the expected data flows associated with different API functionalities.

Now enhanced with **Autonomous Threat Hunting,** the platform continuously monitors API traffic for deviations from this established baseline. It then acts as an automated SOC analyst, connecting subtle anomalies over time into a complete attack story. This is possible because Salt's models use adaptive baselining, continuously updating their understanding as your APIs evolve to ensure detection remains accurate and effective.

Unlike traditional tools that rely on pre-defined rules, Salt's use of unsupervised machine learning enables it to detect previously unknown threats and zero-day attacks that have no existing signature. Crucially, Salt's platform goes beyond generic attacks by incorporating an understanding of your specific business logic, allowing it to identify and prevent attackers from maliciously manipulating legitimate API functionalities.

Benefits of Salt Behavioral Threat Protection:

- **Uncover Hidden Threats with Autonomous Threat Hunting:** With its deep contextual analysis and unsupervised machine learning, Salt's platform can detect sophisticated, multi-step attack campaigns that evade traditional security measures.
- **Protect Against Zero-Day Attacks:** Salt's ability to learn and adapt from your unique data enables it to identify and stop brand-new threats before they can cause damage.
- **Reduce False Positives:** By establishing a comprehensive understanding of normal behavior and attacker intent, Salt minimizes alerts for legitimate API usage, freeing up security teams to focus on real threats.



- **Safeguard Business Logic:** Salt protects your APIs from attacks that exploit loopholes or manipulate legitimate business logic for unauthorized gains.
- **Improve Security Posture:** Salt helps you enhance your overall API security posture and safeguard sensitive data by proactively identifying and stopping API threats.

Salt Behavioral Threat Protection in Action

Let's consider a few scenarios where Salt's Behavioral Threat Protection could make a difference:

- **Account Takeover:** An attacker gains access to a legitimate user's credentials and starts making API calls that deviate from the user's normal behavior patterns. For instance, the attacker might access data that the user typically doesn't, or they might make API calls from an unusual geographical location. Salt detects these anomalies and alerts the security team.
- **Data Exfiltration:** An attacker attempts to steal sensitive data from your system by making a series of seemingly innocuous API calls. These calls might be spread out over time and involve small amounts of data at a time, making them difficult to detect with traditional methods. However, Salt's Behavioral Threat Protection can identify the pattern of these calls and flag it as a potential exfiltration attempt.
- **Business Logic Abuse:** An attacker discovers a flaw in your API's business logic that allows them to gain unauthorized access to premium features or manipulate product pricing. By analyzing the context and intent behind the API calls, Salt can recognize this behavior as malicious and prevent the attack.

Conclusion

In today's rapidly changing world of API security, where attackers are becoming more and more sophisticated, traditional security measures are no longer enough. Salt Security's Behavioral Threat Protection offers an advanced solution that uses AI and machine learning to identify and prevent even the most subtle and hidden API attacks. By understanding the unique context of your API traffic and continuously adapting to new threats, Salt Security enables organizations to take proactive steps to protect their APIs and secure their critical data. Don't wait for a breach to reveal the weaknesses in your API security. Choose Salt Security and stay ahead of the attackers.