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. Traditional security tools do not easily detect such attacks and can pose a significant threat to organizations. APIs are the lifeblood of how many organizations run their business, so deploying purpose-built security solutions is critical to help find and mitigate advanced API attacks.

The Salt Solution: Behavioral Threat Protection Powered by AI

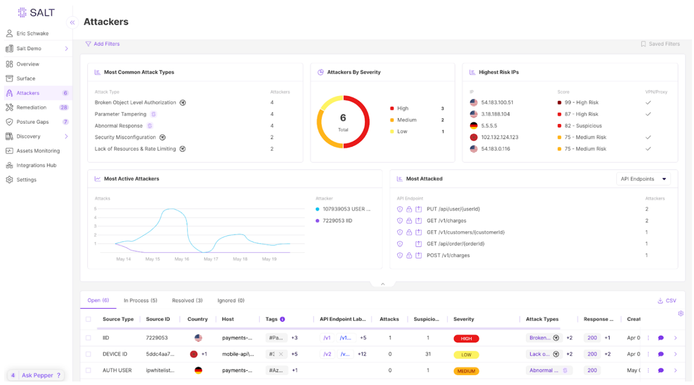
Salt Security's industry-first Behavioral Threat Protection tackles this challenge head-on by leveraging the power of artificial intelligence (AI) and machine learning (ML). By analyzing vast amounts of API traffic data, Salt comprehensively understands what constitutes normal API behavior for your organization.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

Salt's Behavioral Threat Protection then continuously monitors API traffic for anomalies and deviations from this established baseline. These anomalies can be subtle – for example, a slight increase in the frequency of API calls from a particular user, a sudden change in the types of data being accessed, or an unexpected shift in the geographical location of API requests. By considering the full context of the interaction, Salt can differentiate between legitimate activity and potential malicious intent.

Salt Security Platform Behavioral Threat Protection – Key Differentiators

- AI-Powered Detection: Leverages cutting-edge AI and ML to uncover hidden threats.
- LLM-Atacker Insights: Natural language explanation for attacks
- Contextual Analysis: Considers the full context of API interactions for accurate detection.
- Adaptive Learning: Continuously updates its understanding of normal behavior.
- Business Logic Protection: Defends against attacks that exploit API functionality.
- Seamless Integration: Integrates with your existing security ecosystem.

Furthermore, Salt's Behavioral Threat Protection employs adaptive baselining techniques. This means that the system's understanding of normal behavior is not static. As your APIs evolve and user patterns change over time, Salt's machine-learning models continuously update the baseline to ensure that anomaly detection remains accurate and effective. This is particularly important in today's dynamic API environment, where new APIs are constantly being deployed, existing APIs are frequently updated, and user behavior patterns can naturally fluctuate.



Most Common Attack Types

Attack Type	Attackers
Broken Object Level Authorization	4
Parameter Tampering	4
Abnormal Response	4
Security Misconfiguration	2
Lack of Resources & Rate Limiting	2

High	3
Medium	2
Low	1

Highest Risk IPs

IP	Score	VPN/Proxy
54.183.100.51	99 - High Risk	✓
3.18.188.104	87 - High Risk	✓
5.5.5.5	82 - Suspicious	
102.132.124.123	75 - Medium Risk	✓
54.183.0.116	75 - Medium Risk	✓

Most Attacked

API Endpoint	Attackers
PUT /api/user/{userId}	2
GET /v1/charges	2
GET /v1/customers/{customerId}	1
GET /api/order/{orderId}	1
POST /v1/charges	1

Source Type	Source ID	Country	Host	Tags	API Endpoint Lab...	Attacks	Suspicio...	Severity	Attack Types	Response ...	Creat
IID	7229053		payments-...	#Pa... +3	/v1 /v1... +5	1	1	HIGH	Broken... +2	200 +1	Apr 0
DEVICE ID	5ddc4aa7...	+1	mobile-api\...	#: +5	/v2 /v... +12	0	31	LOW	Lack o... +2	200 +2	Apr 0
AUTH USER	ipwhitelist...		payments-...	#Az... +1		0	1	MEDIUM	Abnormal ...	200	May (

Another key differentiator of Salt's Behavioral Threat Protection is its use of unsupervised machine learning. Unlike traditional security tools that rely on pre-defined rules and signatures to identify threats, Salt's ML models are able to learn and adapt from the data itself. This enables them to detect previously unknown threats and zero-day attacks that haven't been documented or codified into traditional security signatures.

Finally, Salt's Behavioral Threat Protection goes beyond protecting against generic attacks by incorporating an understanding of your specific business logic. Many API attacks involve attackers attempting to exploit loopholes or maliciously manipulate legitimate API functionalities. By analyzing the business logic embedded within your APIs, Salt can identify these types of attacks and prevent them from succeeding.

Benefits of Salt Behavioral Threat Protection:

- Uncover Hidden Threats: With its deep contextual analysis and unsupervised machine learning, Salt Behavioral Threat Protection can detect sophisticated attacks that evade traditional security measures.
- LLM-Attacker Insight: Provide natural language explanation of attacks providing quick explanations to easily understand the nature of the attack.
- Protect Against Zero-Day Attacks: Salt's ability to learn and adapt from data enables it to identify and stop new threats before they cause damage.
- Reduce False Positives: By establishing a comprehensive understanding of normal behavior, 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 business logic for unauthorized gains.
- Improve Security Posture: Salt helps you enhance your overall API security posture and safeguard the sensitive data that flows through your APIs 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 this maclicous activity 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 an 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 help 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.