neosec

Harness the Power of Behavioral Analytics to Detect and Stop API Attacks

Modern business is powered by application programming interfaces (APIs). From accelerating internal development to collaborating with business partners to transforming your business through innovative use of cloud and Internet of Things (IoT) technologies, APIs likely play a pivotal role in how your business operates today and where you would like to take it tomorrow.

The problem is that malicious actors view APIs just as strategically as you do.

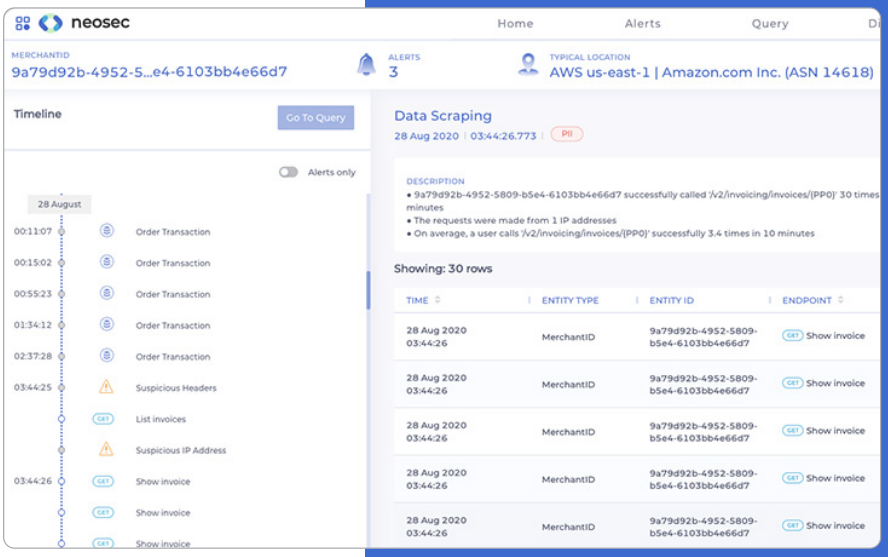
As API usage grows, often without formal planning or security governance, it creates an attractive and ever-evolving attack surface for cybercriminals and other bad actors. And just as security teams have discovered in other areas like endpoint security and firewalls, static security policies based solely on historical attack techniques and signatures are insufficient protection against today's sophisticated API threats.

Neosec Uses AI and Behavioral Analytics to Discover, Contextualize, and Protect Your APIs

Neosec is a cloud-based API security platform that uses leading-edge AI and behavioral analytics techniques to:

- Discover all of your organization's APIs through a fully automated approach
- Collect your API activity data and enrich it with contextual information and relationship mappings
- Create detailed baselines of standard API usage and behavior over time
- Perform advanced behavioral analysis to detect suspicious API activity and generate actionable, information-rich security alerts
- Give security professionals and API teams direct access to an enriched data lake, where they can perform queries and investigate issues

The Neosec platform moves beyond analysis of individual API calls or short-term session activity to give you a detailed understanding of the actor entities and business entities represented in your API activity and how they have interacted over a rolling 30-day time horizon. This increases its effectiveness over first-generation API security technologies by orders of magnitude.



How Neosec Helps

- Discover and inventory your APIs
- Uncover unsanctioned API activity through behavioral detection
- Apply insights and policy guidance to reduce your API attack surface
- Detect active API attacks quickly and accurately
- Accelerate incident response, containment, and recovery

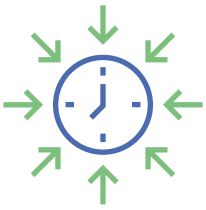
Business Impact

- Prevent exfiltration of sensitive data
- Improve security team efficiency and effectiveness
- Innovate faster by integrating security with DevOps tools and processes
- Establish and maintain customer and partner trust
- Simplify compliance activities

Key Features

Fully Automated API Discovery

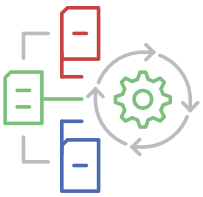
Neosec's AI-based discovery process creates a comprehensive and highly accurate API inventory automatically, including all exposed APIs, endpoints, and parameters. Analytics and AI-based classifications are provided for each endpoint, providing data classification, insights into risk posture, and alignment with best practices. While the discovery process is highly automated for speed and efficiency, it is also completely user-configurable.



Integrated Response Actions

Neosec gives security teams the power to define granular automation rules to initiate automated responses. Automation rules can reference a wide range of API activity attributes, including the endpoint, service, alert name, alert category, alert severity, actor entity, business entity, alert labels, and alert description. When malicious activity is detected and a rule condition is matched, the configured response is automatically carried out.

Two-way integration with external tools can be used to trigger response workflows automatically, provide supporting information, and enable on-demand access to enriched data through the NeoGraph API. Automated responses can also extend to the API infrastructure itself. For example, if the incident responder believes a certain API attack or misuse warrants automated token revocation, she can write a rule prompting the API gateway to revoke the alerted user's token with just a few clicks.



AI-Based Detection of Attacks and Abuse

Like many areas of information security, early attempts at API security relied heavily on signature-based detection. While signature-based approaches are capable of detecting known malicious activity, effective API security requires a more nuanced approach. For example, real-world API risks like business logic attacks and misuse often originate from seemingly legitimate user accounts, making them impossible to detect with pre-defined signatures. For this reason, Neosec augments signature- and rule-based detection with sophisticated behavioral analytics.

The Neosec AI engine develops a detailed picture of the actors and business entities represented in your API activity and monitors interactions over extended periods to establish baselines of expected usage and behavior. This provides the ability to detect both fast-moving and "low and slow" API attacks that would be undetectable in traditional API security approaches.

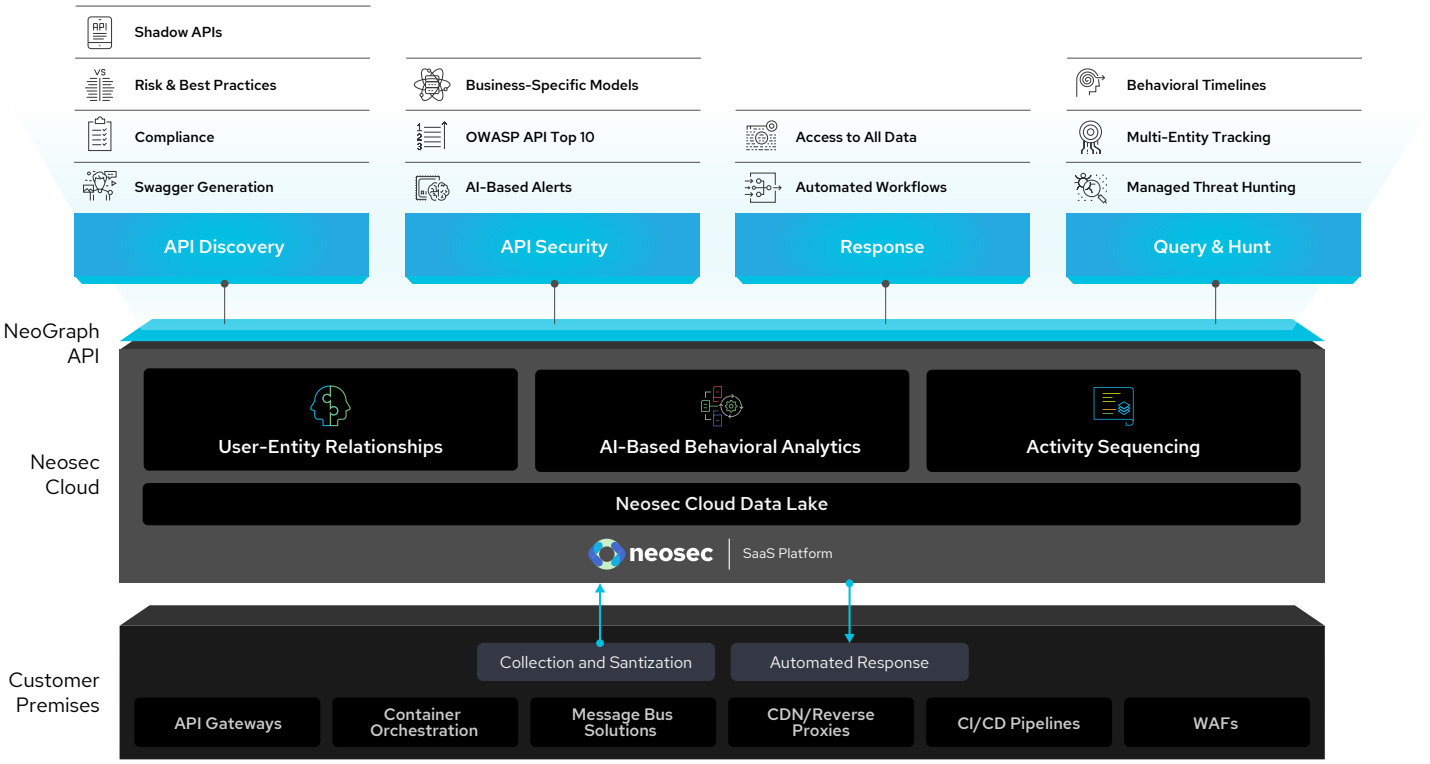
Enriched Data Lake and Query Interface

The Neosec platform enriches the API activity data it collects with contextual information that enables more advanced behavioral analysis techniques and makes it more relevant to security researchers, incident responders, API teams, and API business leaders. The data is stored in a cloud-based data lake, where API stakeholders can perform queries and pivot through all of the entities included. Incident responders can use this powerful capability to investigate specific alerts or hunt for threats based on the characteristics of a particular attacker. In addition, API teams and business users can use the Neosec data lake and query interface to debug APIs and understand usage and behavior patterns.configurable.

Architecture and Integrations

Cloud-Native Platform for True Machine Learning at Scale

Neosec is delivered as a cloud-native software-as-a-service (SaaS) platform, so it can be deployed in minutes, and scaling is seamless as your API usage grows. Along with delivering speed, simplicity, and scalability, Neosec's SaaS-based architecture also makes it possible to perform true machine learning at scale for the vast amounts of data produced within a sliding 30-day time window by all of the entities represented in your API activity.



Rapid Integration With All Common API Architectures

Neosec integrates with your existing API architecture using out-of-band log event collection integrations with popular API gateways, WAFs, cloud platforms, and data center technologies.

This includes:

- Plug-ins for leading API management platforms and gateways
- Cloud provider log ingestion
- On-premises log collectors
- Integration with web applications firewalls (WAFs)
- Integration with Kubernetes container orchestration

As data is collected, it is anonymized on-premises, transmitted to the Neosec cloud infrastructure, and stored in a data lake for a rolling 30-day period.

Automation-Ready Approach

Speed is everything for DevSecOps teams, so Neosec offers a flexible set of NeoGraph APIs that can be used to push timely alerts and supporting analytic details and machine learning outputs to your preferred security and IT operations tools. The NeoGraph APIs also allow external tools to access the complete set of Neosec features and models for further research and analysis through a single interface. This includes the ability to access hundreds of features, along with a 30-day history of API activity data and machine learning models.

"Because APIs expose core business functionality, the approach of applying AI-based behavior analysis to track and analyze all relationships between users and business entities is so critical for detecting abuse."

Rinki Sethi, VP & CISO Twitter

API Gateways

apigee · Kong · MuleSoft · Akamai

Cloud

aws · Azure · Google Cloud

Microservices

kubernetes · docker

Networking

NGINX Part of F5 · APACHE HTTP SERVER PROJECT · imperva · f5 · Gigamon

Response

webhooks · Jira Software · servicenow · PagerDuty · splunk> · slack

Get started today

See for yourself how Neosec can bring unprecedented visibility and security to your API activity.

Visit Neosec.com to start your free trial.

neosec