CYBER

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.

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

VT Cyber 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

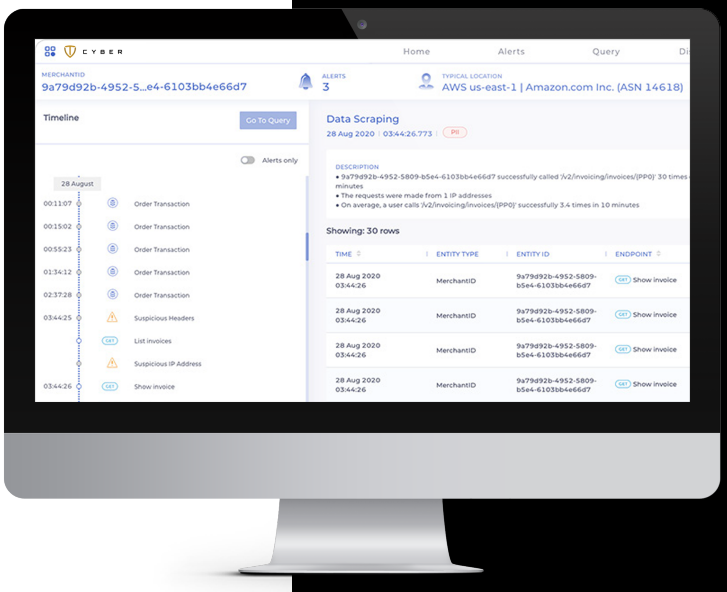
The VT Cyber platform moves beyond analysis of individual API calls or short-term session activity to give you a detailed understanding of the actor entities and business entities represented in your API activity and how they have interacted over a rolling 30-day time horizon. This increases its effectiveness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

How VT Cyber 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



Detect and Respond to Business Logic Abuse Quickly

While securing your APIs against external attackers is essential, business logic abuse by authenticated users poses an even greater business risk. Authenticated users have access to much larger attack surface than external attackers, and application developers are often lulled into a false sense of security when developing features that are only intended for use by authorized users.

Further complicating matters is the fact that business logic abuse is notoriously difficult for traditional security tools to detect due to its similarity to expected usage patterns and efforts by bad actors to blend abuse in with legitimate transactions over extended time periods.

VT Cyber's AI-powered behavioral monitoring and anomaly detection capabilities – continuously applied over a sliding 30-day time window – are uniquely capable of distinguishing attempts to exploit vulnerable business logic from legitimate activity. This innovative approach, combined with other proven techniques such as attack signature matching and proactive detection of the OWASP API Top 10 Security Vulnerabilities, can detect a much wider array of API attacks with much greater accuracy than other security tools.

Technology Integrations

API Gateways

apigee, Kong, MuleSoft, Akamai

Cloud

aws, Azure, Google Cloud

Microservices

kubernetes, docker

Networking

NGINX, APACHE HTTP SERVER PROJECT, imperva, f5, Gigamon

Response

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

Key Features

Fully Automated API Discovery – A comprehensive and highly accurate API inventory, including data classifications and insights into risk posture, is automatically and continuously populated and enriched with context.

AI-Based Detection of Attacks and Abuse – A sophisticated AI engine develops a detailed picture of the actors and business entities represented in your API activity and monitors interactions for anomalies using a sliding 30-day contextual window.

Integrated Response Actions – Security teams can define granular rules that initiate automated responses when malicious activity matches a condition, and two-way integration with external tools initiates and accelerates incident response workflows.

Enriched Data Lake and Query Interface – VT Cyber's enriched API activity data and machine learning model outputs are stored in a cloud-based data lake, where API stakeholders can perform queries and pivot through all of the entities included.

Architecture and Integrations

Cloud-Native Platform for True Machine Learning – VT Cyber is delivered as a cloud-native software-as-a-service (SaaS) platform for fast and simple deployment, seamless scaling, and the power to perform true machine learning for vast amounts of data.

Rapid Integration With All Common API Architectures – Out-of-band log event collection integrations with popular API gateways, WAFs, cloud platforms, and data center technologies simplify onboarding and anonymize all data before it is transmitted to the cloud.

Automation-Ready Approach – A flexible set of APIs push timely alerts, supporting analytic details, and machine learning outputs to your preferred security and IT operations tools and provide programmatic access to the complete set of VT Cyber features, models, and data sets.

Get started today

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

Visit vtcyber.pl to start your free trial.

CYBER