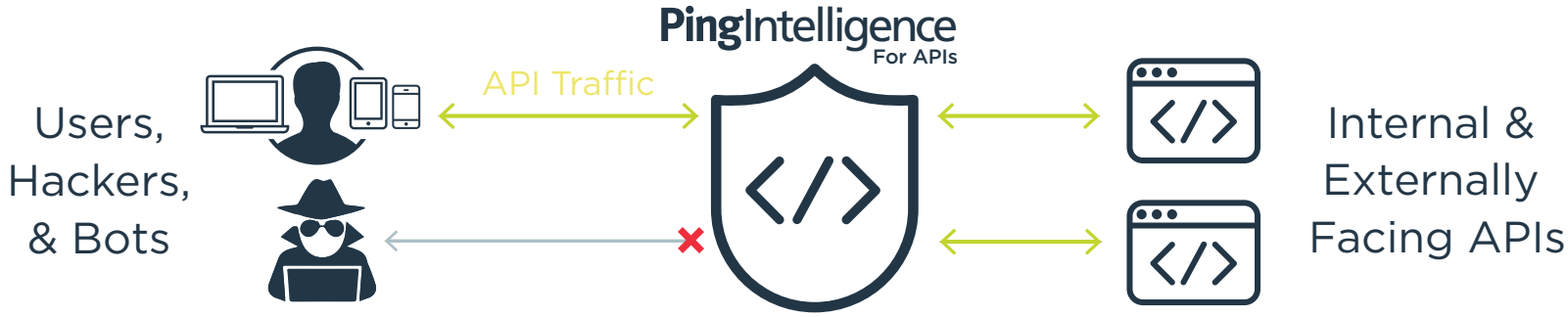
PingIntelligence For APIs

DATASHEET

Digital transformation initiatives founded on APIs are making business logic and data readily accessible to internal and external users. As API adoption continues to rise, it becomes more important than ever to monitor activity to understand who is accessing APIs and how they can be protected from vulnerabilities. PingIntelligence for APIs uses artificial intelligence (AI) to gain in-depth visibility into API traffic to centralize traffic monitoring, enabling the quick identification and blocking of anomalous traffic while providing detailed reports on all activity. Leveraging AI models specifically tailored for API security, PingIntelligence for APIs identifies attacks that go undetected by traditional security solutions, including web application firewalls, such as zero day attacks. Instead, PingIntelligence for APIs learns traffic behaviors to determine good and bad traffic, and can be deployed into your existing security infrastructure.



PingIntelligence for APIs delivers deep insight into API activity to help protect API infrastructures

FEATURES

- Rich API traffic visibility & reporting
- Automated API discovery
- Artificial intelligence for each API
- API bad traffic analytics and threat detection
- Automated attack blocking—including across clouds
- API deception & honeypot for instant hacking detection
- Multiple deployment options in public and private clouds
- Support for hybrid IT environments
- Integration with popular gateways for “drop-in” deployments
- Automatic adaptation to changing environments
- Continuous self-learning; no rules to write and maintain

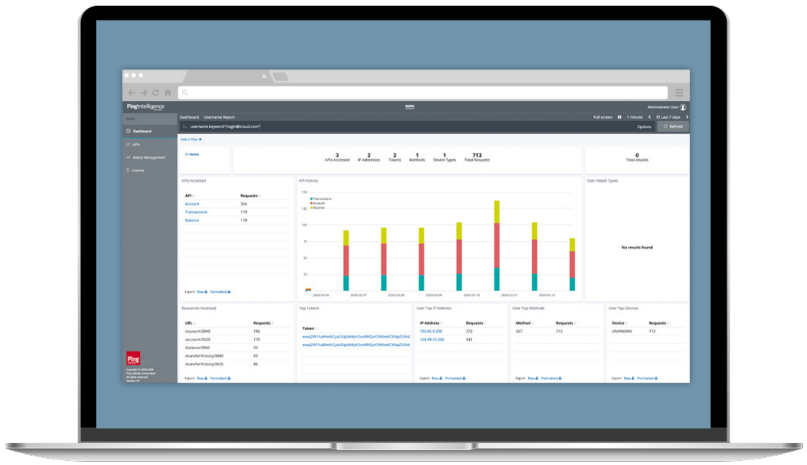
BENEFITS

- Helps sort out good and bad API traffic
- Automatically discovers new APIs on your infrastructure
- Delivers unique insight into API activity with dashboards and in-depth reports
- Provides unified view of API activity across API gateways and clouds
- Protects API infrastructures from disruption, data theft and shutdown
- Increases protection against threats in the OWASP API Security Top 10 and beyond
- Enables self-learning to save security analysts from having to write or maintain rules
- Simplifies investigations and compliance tracking with the right information

IN-DEPTH VISIBILITY INTO API TRAFFIC

With PingIntelligence for APIs, you can gain visibility into all API activity across all gateways, data centers and clouds to understand the behavior of each API to distinguish between good and bad traffic to your APIs. Traffic data is fed into dashboards, allowing you to gain a unified view of newly discovered APIs, detailed API activity, most active client activity, bad traffic, attacks across your infrastructure and attack management. Dashboards can be deployed standalone or integrated into an in-house operations console via PingIntelligence REST APIs.

Security analysts can also generate forensic reports to investigate historical activity, such as all APIs and paths accessed by a hacker leading up to an attack. For regulated industries, detailed reporting of all API activity associated with database and file system access, line of business applications or control systems is available for compliance purposes.



Built-in dashboards and reporting centralize the monitoring of API activity

PINGINTELLIGENCE FOR APIS

Protect Internal and External APIs

PingIntelligence for APIs applies AI models and big data analytics to continuously inspect and report on all API activity, for both internal and external APIs. By applying a combination of AI and user behavioral analytics, PingIntelligence for APIs can automatically discover anomalous traffic behavior across an enterprise's API environment. PingIntelligence for APIs was purpose-built to recognize and respond to rapidly changing, dynamic attacks unique to APIs without writing policies, rules or code.

Automated API Discovery: Dynamically discover APIs across your environment that are inadvertently exposed, unknown or forgotten. Generate detailed reports on activity across these APIs and look for attacks on their data and applications.

API Deception: Use decoy APIs (honeypots) to instantly reveal hacker's activity. Since decoy APIs should never be accessed by legitimate clients, API deception will immediately recognize the attack and prevent access to production APIs.

Sort Out Good and Bad Traffic: API infrastructures can be subjected to all sorts of bad traffic, from an API used by a partner in a non-intended way, to a system "misfiring" and sending vast amounts of traffic to a gateway cluster, to a hacker using a valid user account to reverse engineer an API and gain access to other accounts while looking like a normal user.

Sample of Attacks Detected: Existing solutions, such as API gateways and web application firewalls, weren't built to protect against attacks designed to take advantage of vulnerabilities unique to APIs and the data and systems to which they provide access. PingIntelligence for APIs works with these solutions by detecting, blocking and reporting on attacks that represent anomalous behavior on each API, including:

- Anomalous API access patterns
- Credential stuffing and password spraying
- Account takeover with stolen token, cookie or API key
- API takeover attacks
- Data extraction or theft
- Data scraping
- Data deletion or manipulation
- Data injected into an application service
- Malicious code injection
- Extreme application activity
- Probing and fuzzing attacks
- Targeted API DDoS attacks
- Extreme client activity
- Header manipulation attacks
- Fraudulent user access behavior

DEPLOYMENT FLEXIBILITY

PingIntelligence for APIs provides flexible deployment options to work with your existing API infrastructure with both inline and sideband options, allowing IT to choose the model appropriate for their environment. The inline model offers a high-performance reverse proxy that can protect any number of API gateways and cloud APIs implemented directly on application servers. Alternatively, sideband deployment with an API gateway or PingAccess provides the same AI-powered attack detection and comprehensive insight as the inline option, without requiring network or infrastructure modifications. In this deployment mode, PingIntelligence for APIs is simply "dropped-in" on the side of the gateway or PingAccess—outside of the data path—to monitor the traffic, identify abnormal behaviors and threats, and communicate when blocking is required.

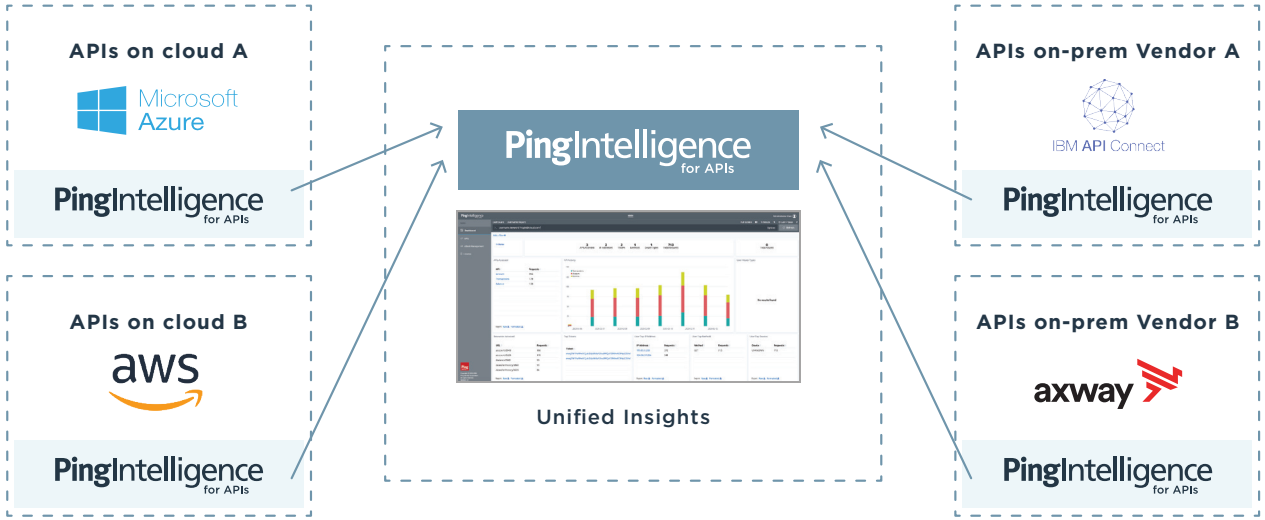
Inline Deployment of PingIntelligence for APIs with an API Gateway

Inline Deployment of PingIntelligence for APIs with an Application Server

Sideband Deployment of PingIntelligence for APIs with an API Gateway or PingAccess

INTEGRATIONS FOR YOUR ENVIRONMENT

PingIntelligence for APIs provides deep insight into API activity to protect both internal and external APIs, whether on-premises, in clouds or in hybrid cloud implementations. It supports a wide variety of API gateways with sideband integrations with PingAccess, as well as leading API gateway platforms, including those from Amazon (AWS API Gateway), Google/Apigee, MuleSoft, IBM (DataPower/API Connect), Axway, NGINX, CA/Broadcom (Layer 7), WSO2 and Azure API Gateway. When deployed inline, PingIntelligence for APIs supports existing API gateway platforms, including RedHat, TIBCO, Software AG and others. Additionally, PingIntelligence for APIs supports APIs implemented directly on app servers such as Node.JS, WebLogic, Tomcat and WebSphere. With deployment options including virtual machines, Docker containers and bare metal environments, PingIntelligence for APIs supports automated installation and management scripts across common datacenter and cloud environments such as AWS and Azure.



TRY IT TODAY!

The PingIntelligence for APIs trial is a cloud-delivered service. Apply for the PingIntelligence for APIs Trial.

#3341 | 05.20 | v20