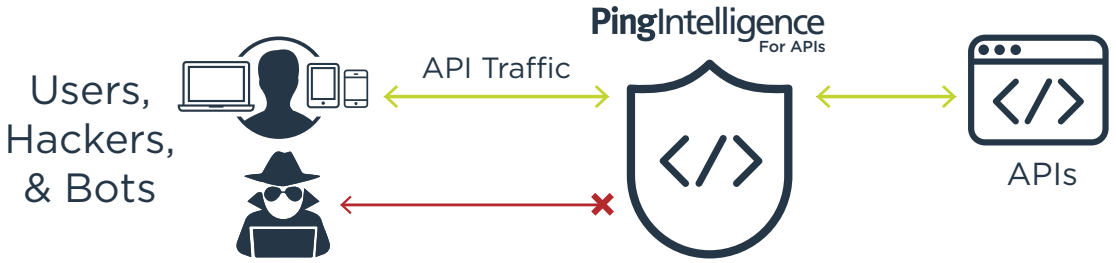
Private Preview

PingIntelligence For APIs

DATASHEET

Digital transformation initiatives founded on APIs are making business logic and data readily accessible to internal and external users. However, APIs also present a new opportunity for hackers to reach into data and systems, and predefined rules, policies and attack signatures can't keep up with this evolving threat landscape. PingIntelligence for APIs uses artificial intelligence (AI) to expose active APIs, identify and automatically block cyberattacks on APIs, and provide detailed reporting on all API activity. Leveraging AI models specifically tailored for API security, PingIntelligence for APIs brings cyberattack protection and deep API traffic insight to existing API Gateways and application server-based API environments.

PingIntelligence for APIs detects anomalous behavior on APIs, as well as the data and applications exposed via APIs, and can automatically block attacks across your API environment. For example, attempts to bypass login systems using botnet credential stuffing attacks or stolen tokens are recognized as cyberattacks. Attempts to exfiltrate, change or delete data which fall outside the range of normal behavior for an API can also be blocked and reported on in near real time.



PingIntelligence for APIs delivers deep insight into API activity and blocks cyberattacks for all API infrastructures

FEATURES

- Automated API discovery
- API threat detection & automated blocking
- API deception & honeypot
- Deep API traffic visibility & reporting
- Multiple deployment options
- Support for hybrid IT environments
- Self-learning without writing policies and rules

BENEFITS

- Discover unknown and inactive APIs
- Stop API attacks across your environment
- Safeguard data against theft and deletion
- Protect APIs from disruption or shutdown
- Instantly recognize and block hackers
- Deliver detailed forensic and compliance reports

PINGINTELLIGENCE SOLUTIONS

API CyberSecurity

PingIntelligence for APIs applies AI models and big data analytics to continuously inspect and report on all API activity, and automatically discovers anomalous traffic behavior across an enterprise's API environment. Bad actors are well versed in circumventing static security policies, so PingIntelligence was purpose-built to recognize and respond to rapidly changing, dynamic attacks unique to APIs without writing policies, rules, or code.

AUTOMATIC API DISCOVERY: Dynamically discover APIs across your environment which 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.

DOS/DDOS ATTACKS: PingIntelligence can recognize and control Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks targeting individual APIs. This manages sophisticated botnet and memory-flooding attacks which can remain below the volumetric policy threshold of other security products to avoid detection.

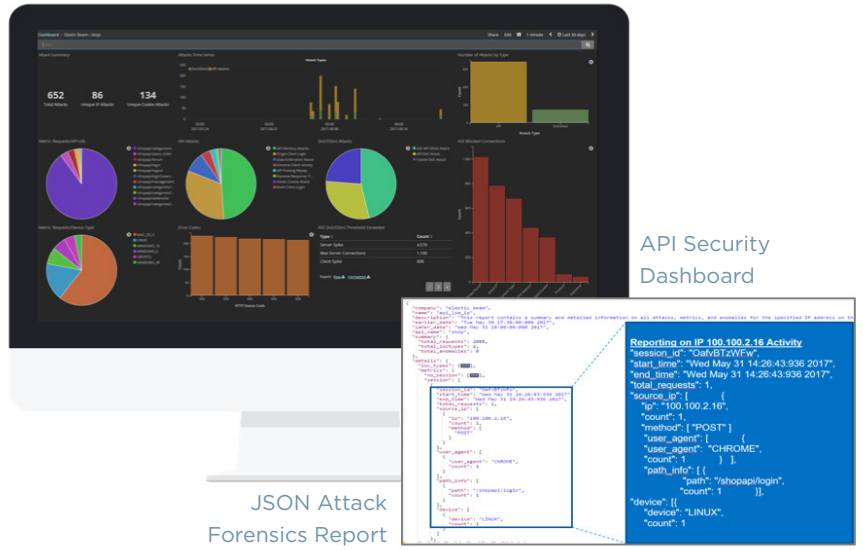
AUTHENTICATION/AUTHORIZATION ATTACKS: API clients traverse a predictable range of authentication flows, allowing PingIntelligence to detect attempts to bypass login systems using techniques such as credential stuffing, stolen cookies, or stolen tokens to access API services.

APPLICATIONS, SYSTEMS AND DATA ATTACKS: Client behavior and request/response flows can vary greatly across APIs, but PingIntelligence is able to recognize deviations from the norm to identify data extraction, deletion and alteration, as well as API attacks injecting malicious content.

MONITOR & REPORT API TRAFFIC & ATTACKS

With PingIntelligence, you can monitor all API activity including every command and method used throughout a session. Dashboards allow you to leverage a graphical view of attacks, anomalies and metrics across the API environment to help operations track discovered APIs as well as ongoing attack activity and anomalous events. 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 allow you to monitor API activity.

DEPLOYMENT FLEXIBILITY

PingIntelligence for APIs was designed for flexible deployment to work in conjunction with the Ping Identity platform and integrate with your API gateway. Additional architectural flexibility is available with both inline and sideband deployment 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 applications. 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.

INLINE DEPLOYMENT OF PINGINTELLIGENCE FOR APIs WITH AN API GATEWAY

SIDEBAND DEPLOYMENT OF PINGINTELLIGENCE FOR APIs WITH AN API GATEWAY

SIDEBAND DEPLOYMENT OF PINGINTELLIGENCE FOR APIs WITH PINGACCESS

PROTECT YOUR API INFRASTRUCTURE

The PingIntelligence solution protects you from cyberattacks and provides deep insight into API activity on existing API gateways and APIs implemented directly on app servers such as Node.JS, WebLogic, Tomcat and WebSphere—whether on-premises, in the cloud, or both. With deployment options including virtual machines, Docker containers, and bare metal environments, PingIntelligence supports automated installation and management scripts across common datacenter and cloud environments such as AWS.

ELASTIC SCALING AND HYBRID SECURITY

Dynamically expand and contract your API security infrastructure to handle peak traffic loads while managing costs. Automatically propagate security information across hybrid IT environments with real-time synchronization to protect against API attacks spanning multiple datacenters with consistent enforcement across each location.

#3341 | 06.25 | Digital v12