

Protecting API Infrastructure with AI

Dan Tortorici

Sr. Director, Product
Manager for AMPLIFY and
API Management Solutions

#axway



Protecting API Infrastructure with Artificial Intelligence

Agenda

API security

Challenges, or why is this so hard?

AMPLIFY API Management security

Extending security with Elastic Beam

Final thoughts

Security threats are ever present

Nissan Leaf - HTTPS protected API without any authentication



Allowed remote AC control and access to the cars logbook

National Weather Service - No client throttling of Android App that abused API



Android App takes down National Weather Service website

Instagram – Password reset API compromised



Phone numbers and email addresses of celebrities made available

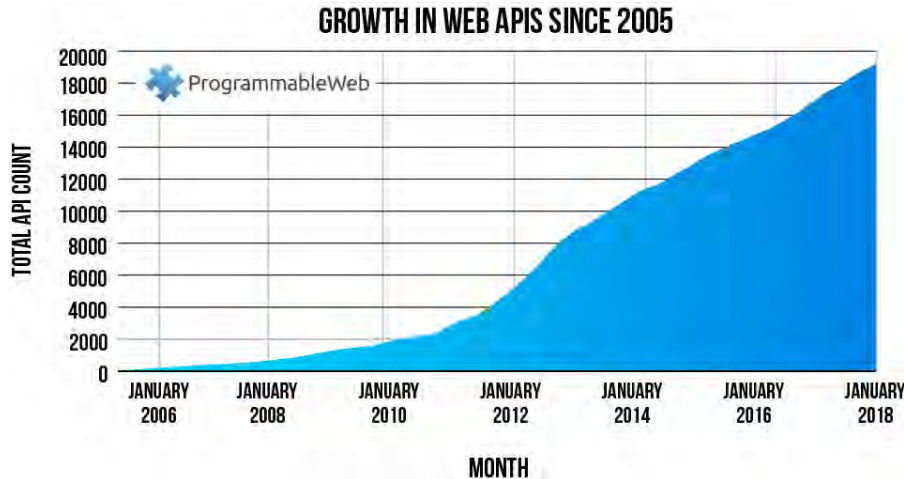
Each technology advance opens new security challenges

Technology Trend	Challenge
Networked systems	Access to industry, civil, and national systems
Software is part of everything	Increased potential for malware
Embedded sensor technology	Safety of medical and industrial systems
API proliferation	Ability to attack at many points
Higher level programming tools	Easier for less talented hackers
Bitcoin	Pay vehicle for Ransomware attacks
Cloud adoption	New vector to secure, shared responsibility model

API security critical to business

- Protect Client and Patient accounts from being taken over
- Safeguard customer records against theft, deletion, etc.
- Stop API attacks on business systems
Banking, retail, healthcare, industrial, government, etc.
- Protect services from disruption or shutdown
- Prevent Cloud / DC performance problems and costly ops snafus
- Exhaustive reporting on all API activity to satisfy Auditors/compliance

Why is it so hard?



- High traffic volume across many APIs
- Large mix of inbound client activity
 - **Legitimate clients** – expected activity used to access API services
 - **High velocity attackers** – attempt to disrupt services, gather content, etc.
 - **Hackers with valid credentials** – blend in while maliciously accessing API services
- Very hard to identify malicious activity

How vulnerable are APIs to attacks?

Pre-login and Post-Login User Attacks

API Login and API DDoS Attacks

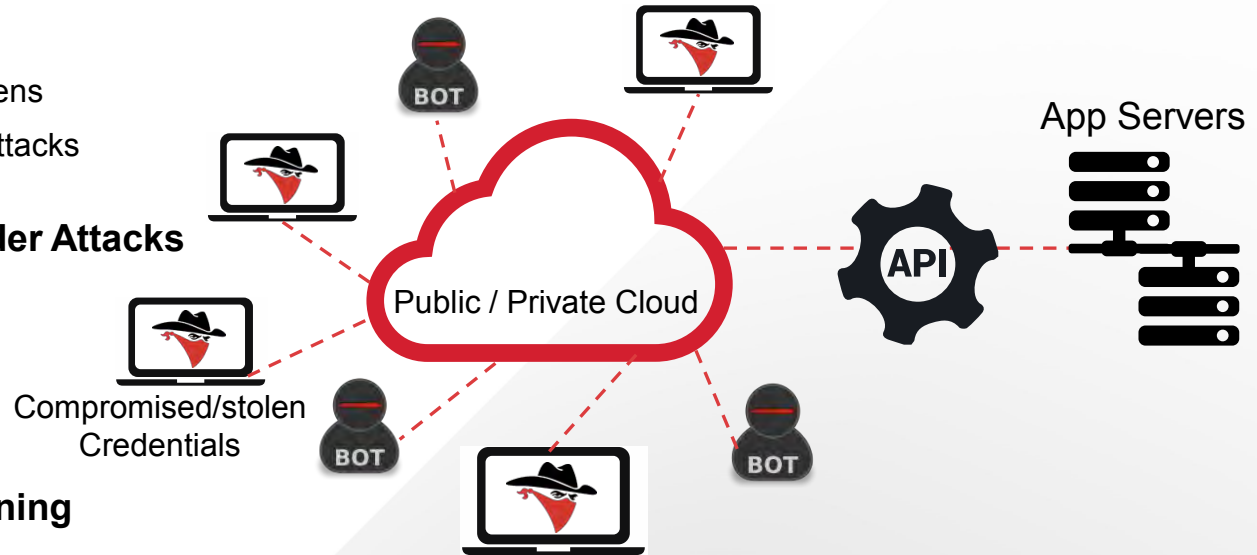
- Brute force login attacks
- Stolen identifiers: cookies and tokens
- API specific DoS and API DDoS attacks

Compromised Account / Insider Attacks

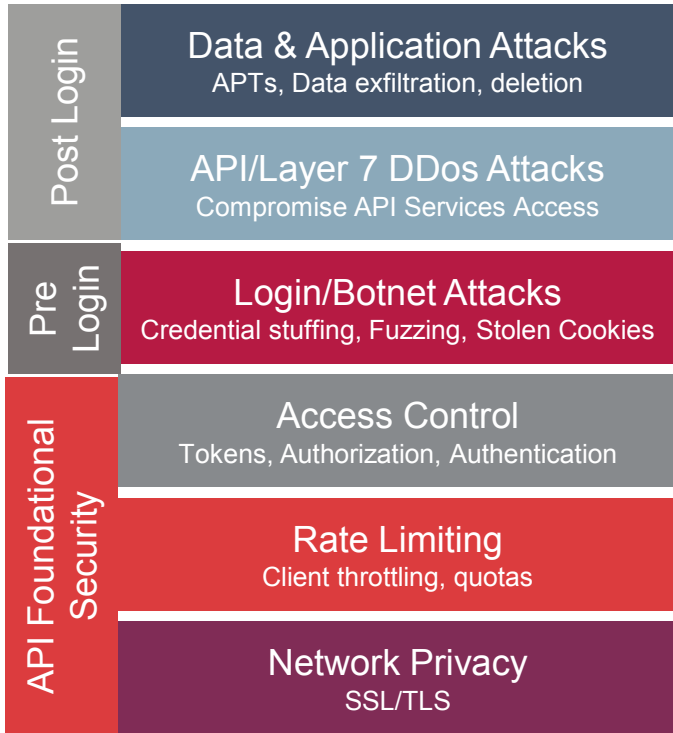
- Account take over
- Data theft
- Application control

Hackers using Machine Learning

- Every attack looks different
- Every blocked attack leads to a new attack ...



Attack Layers



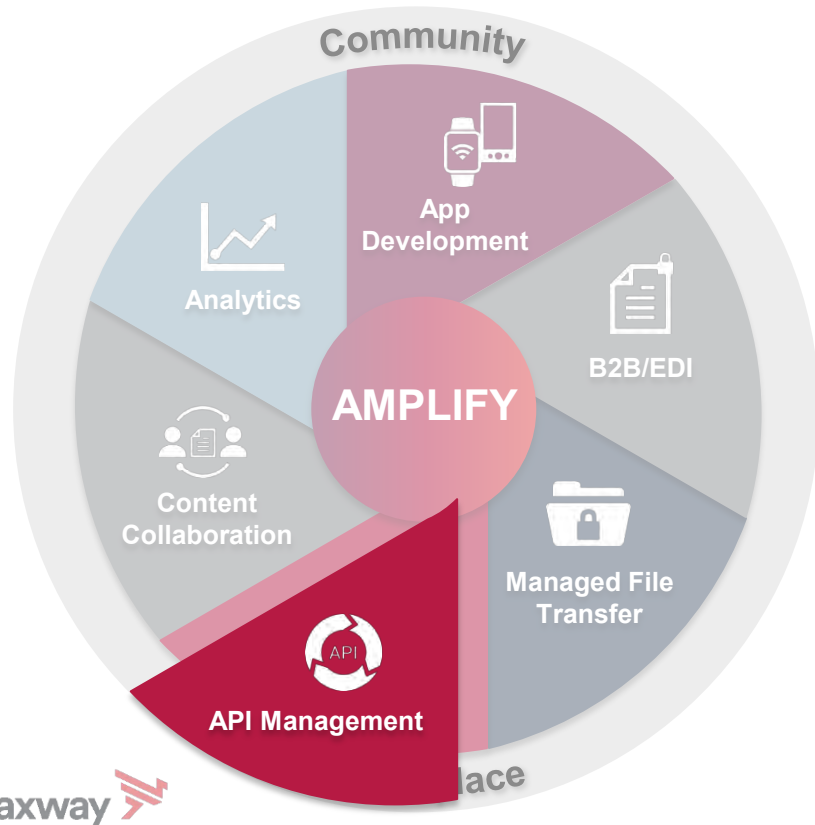
- Increasing sophistication in APTs
- Enterprises challenged to implement foundational security correctly

“We continue to observe that **authentication and authorization controls are often not hardened against abuse** from attackers. Two of the most common issues are a lack of multi-factor authentication (MFA) enforcement and securing privileged credentials.”

Mandiant m-Trends2018

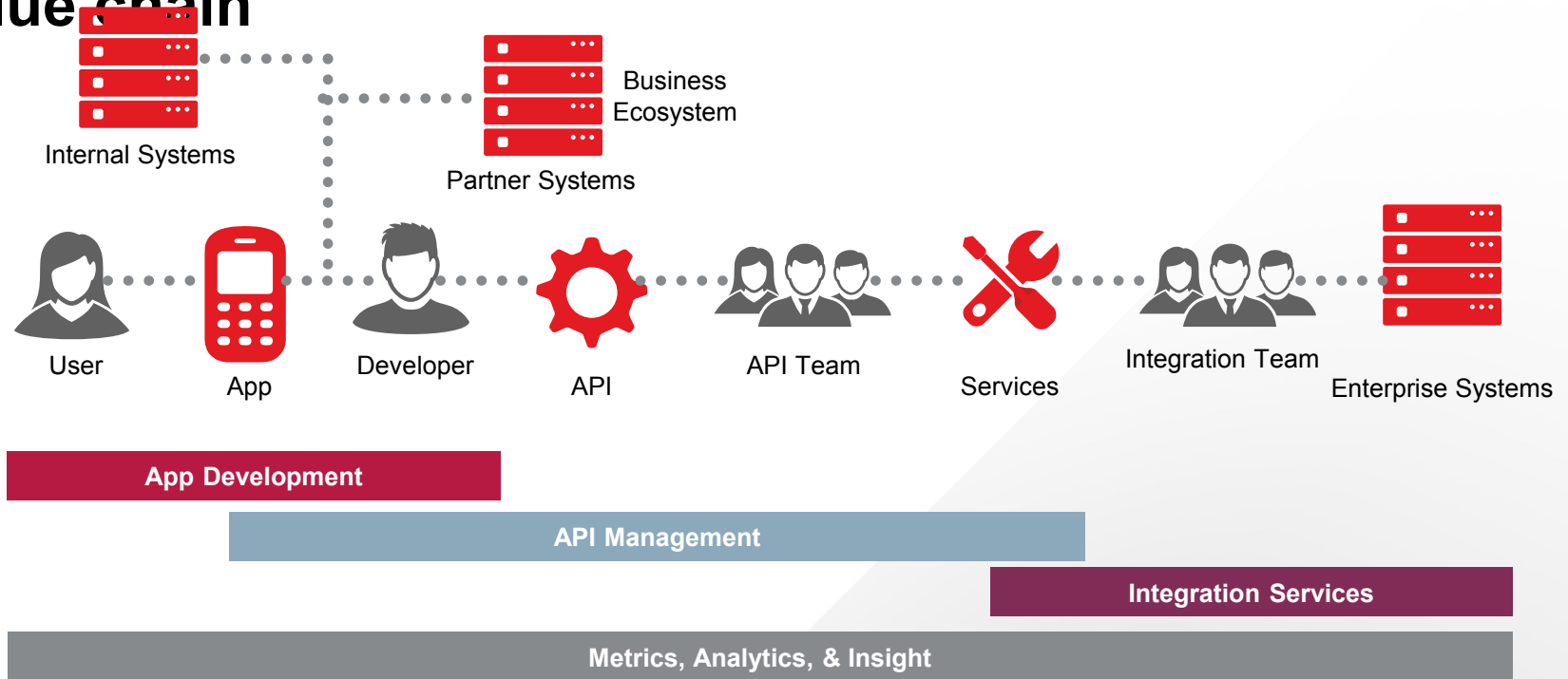
Axway AMPLIFY

The hybrid **integration** and **engagement** platform that unlocks digital experiences by connecting individuals, systems, businesses and ecosystems



- Data integration & engagement
- API driven synergy
- Common user interface
- Global API catalog
- Marketplace
- Community
- Hybrid deployment

AMPLIFY enables the complete digital business value chain



AMPLIFY API Management: Full API lifecycle coverage

Create 

API Builder

- Rapid REST API creation
- Connectors
- API Mockups and Data APIs
- Node JS / Microservice runtimes

API Gateway

- REST SOAP API creation
- REST to SOAP
- Light ESB: SOAP/message-based integration
- Visual Mapper
- Policy Studio and Filters


Mobile Back End Services

- Push Notifications
- 20+ prebuilt mobile services

 Govern 

API Gateway/Manager

- API Catalog & Lifecycle
- Generic policies
- Partner Management
- OAuth (AS/RS) and OpenID Connect
- Check identities in any Directory Server
- Leverage any Access Management
- Quota & Throttling
- Threat detection
- API Firewalling

Consume 

API Portal

- Branding and customization
- Self-service onboarding
- API Discovery and TryIt
- Client App creation and authorization
- Client SDK Generator
- Blogs
- Forums

Measure 

Embedded Analytics

- Predictive insights
- For technical and business users
- API usage/health baselines
- Proactive identification of abnormal situations
 - API Health
 - API consumption
 - API engagement
 - API infrastructure

Mobile Analytics

- Proactive mobile stability and performance,
- Event metrics

Cloud, On Premise, and Hybrid Deployments
Unified user experience
Docker support

Axway API Gateway – Integration, Security, Control & Acceleration.



Over 200+ Pre-built Policies and Filters

Integration

- Protocol Translation
HTTP, JMS, ...
- Message Transformation
REST, SOAP, JSON
- Message Enrichment
- Token Translation
- API Management
- Service Virtualization

Security

- Policy Enforcement Point
- Auth'N, Auth'Z, Audit
- OAuth, Open ID
- WS-*, SAML, XACML...
- XML Firewall
- Encryption & Signing
- Security Token Service
- Key Management
- Data Privacy Filtering

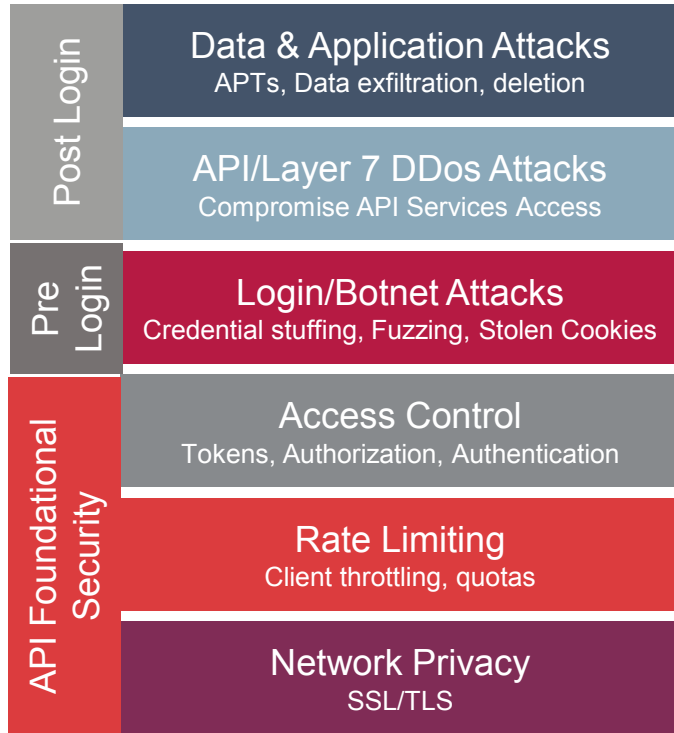
Control

- SLA Monitoring & Audit
- SLA Policy Enforcement
- Service/License Metering
- API Usage Tracking
- Traffic Throttling
- Traffic Smoothing
- Content Routing
- Content Blocking
- Service Usage Analysis

Acceleration

- Parsing
- Schema Validation
JSON, XML
- Transformation
- Signing
- Encryption & Decryption
- SSL Termination / Ops.
- Caching
- Content Based Routing

AMPLIFY Gateway Security



Rate Limiting

- Traffic Throttling & Smoothing
- Content Blocking
- API Usage Tracking

Network Privacy

- Confidentiality – transport and message level encryption
- Integrity – detect unauthorized modifications, message digest
- Secure Connections between all product components.

AMPLIFY Gateway Security

Data & Application Attacks

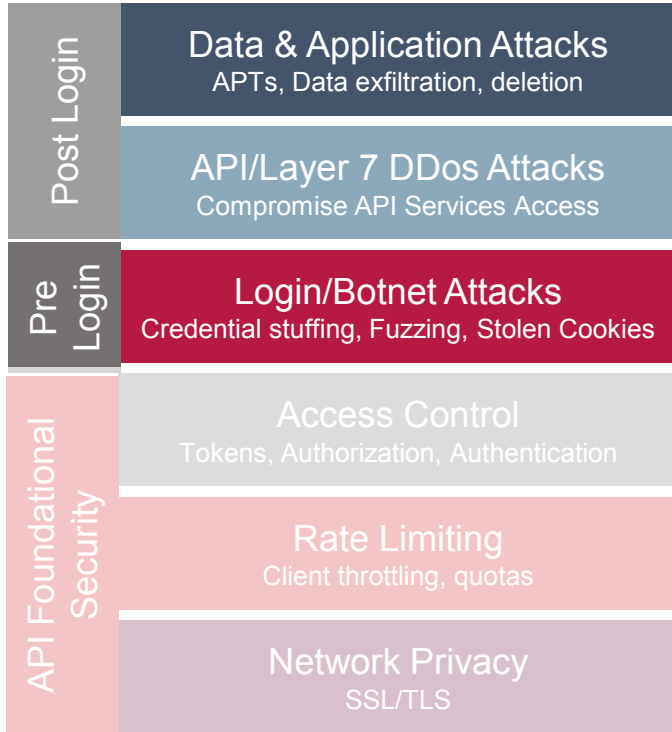
- Prevent DoS attacks at application level

Login/Botnet Attacks

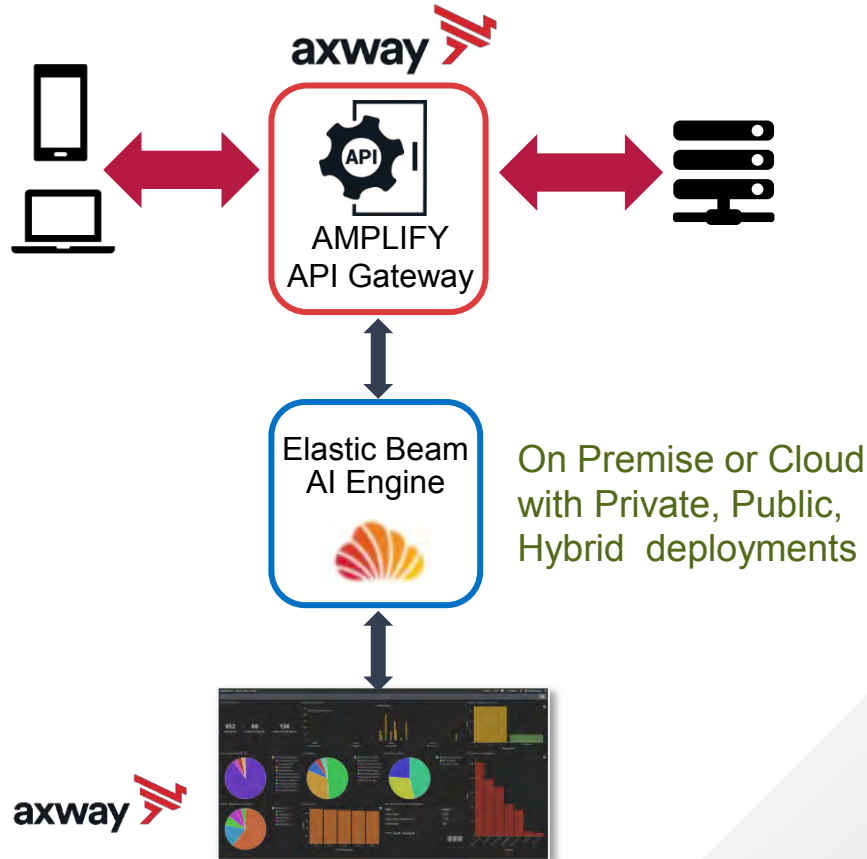
- Anti Virus

Access Control

- Threat Protection – WAF, whitelist /blacklist
- CORS - Cross-Origin Resource Sharing
- Request Validation - parameters, headers, body
- Authentication & Authorization, Auditing
- HSM support
- Redaction of sensitive data
- Identity Mediation
- Common Criteria/CSPN/FIPS
- Integrated Security Audit
- Nonrepudiation – digital signatures
- OAuth 2.0, API Keys

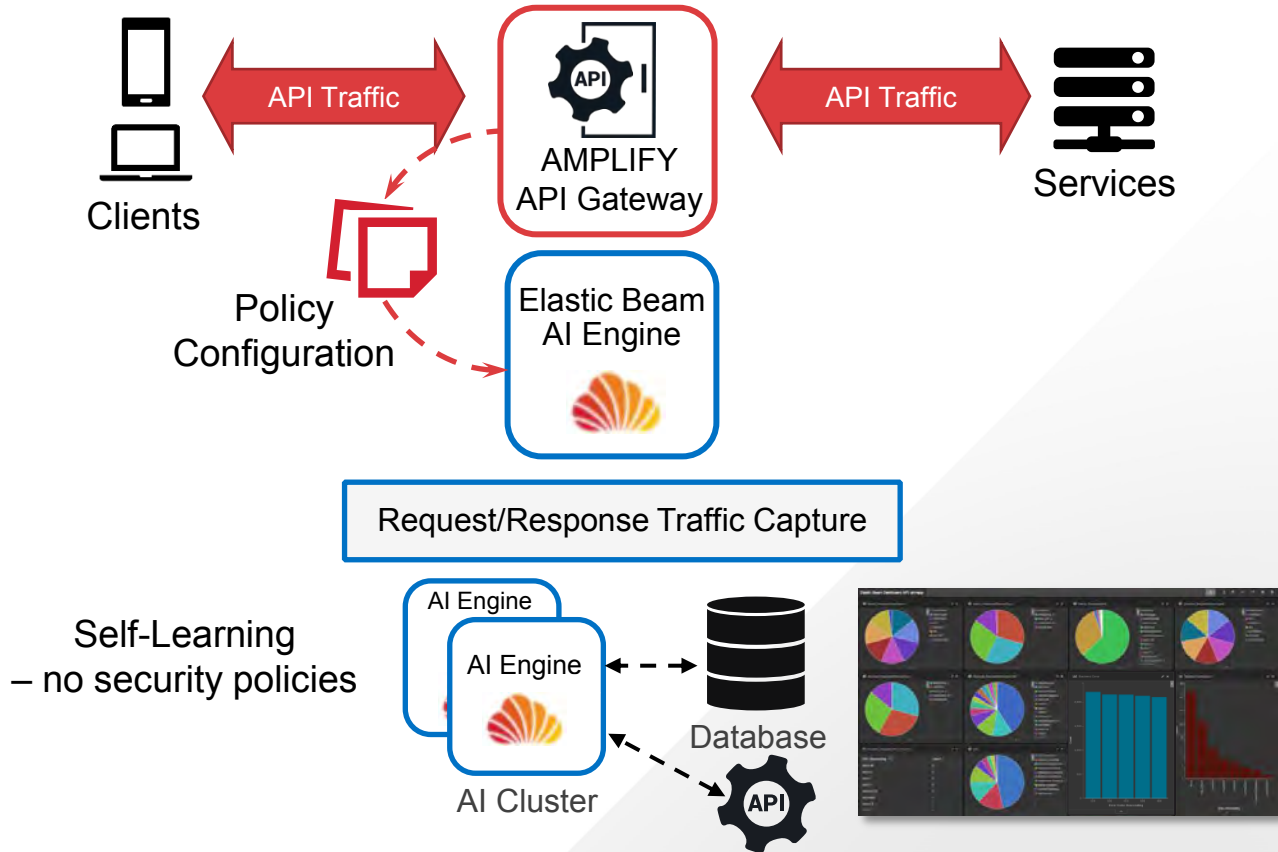


Extending protection from cyberattacks with Elastic Beam API Behavioral Security

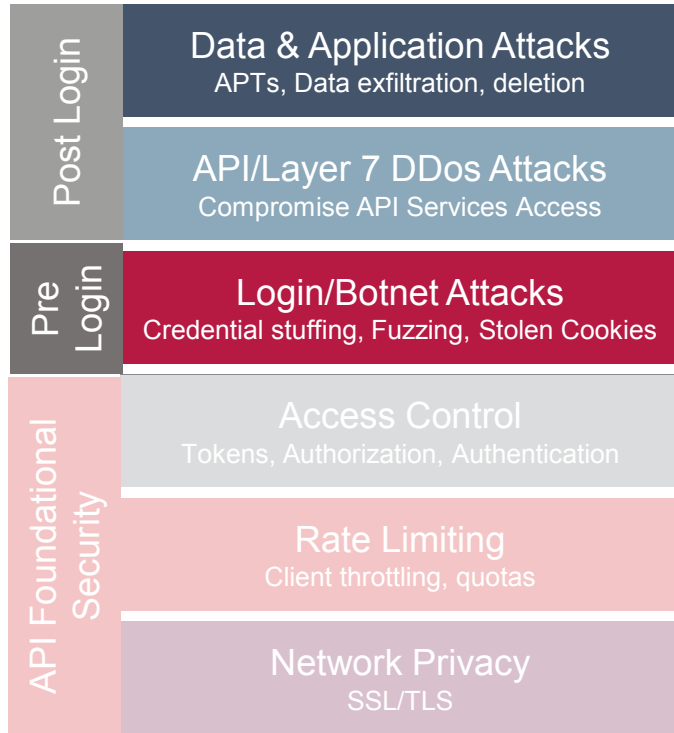


- **AI identifies and blocks cyberattacks on APIs, data, systems, and connected apps**
- **API Honeypot with fake APIs for instant hacking detection**
- **Deep API traffic visibility** for Ops, Compliance, and Forensic reports
- **Automated attack blocking** via Axway Gateway
- Automated attack blocking across clouds
- **Drops in existing deployment via config policy** Operational simplicity, high-scale/performance

Elastic Beam AI-based Security



Extending security with Elastic Beam



Data & Application Attacks

- Data Exfiltration
- Advanced Persistent Threats (APT)
- Data Integrity - Deletion, Change, etc.
- Memory Injection Attacks

API/Layer 7 DDoS Attacks

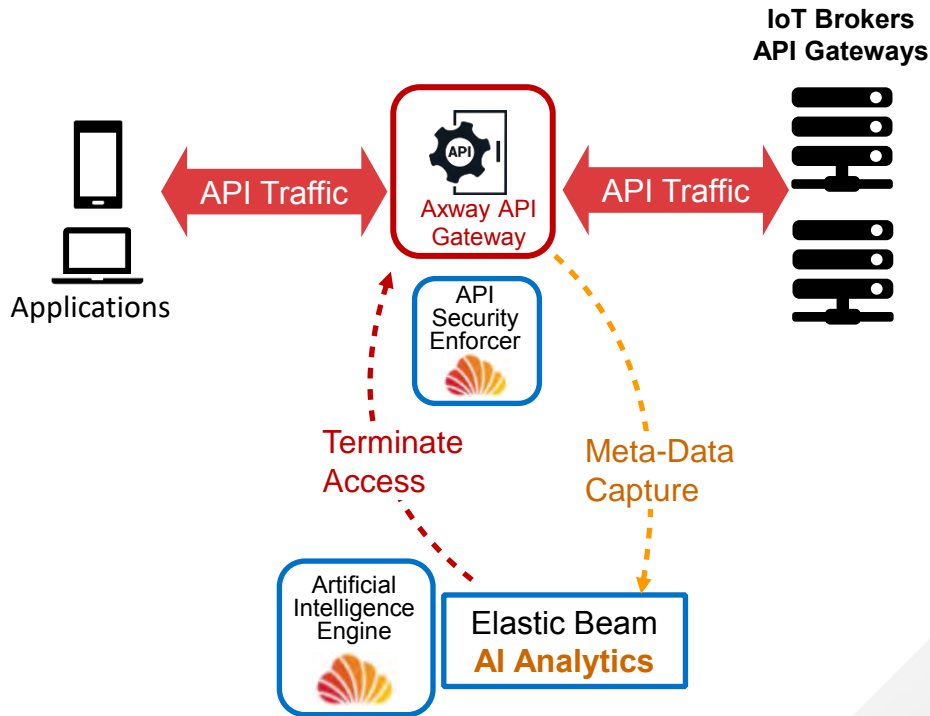
- DDoS API attack
- Login service DDoS attack
- Cookie management service
- Botnet attacking API

Login/Botnet Attacks

- Stolen cookie / cookie poisoning
- Probing replay and fuzzing
- System command / application attack
- Login credential stuffing

Automated Attack Detection and Blocking

Continuous protection of APIs with Artificial Intelligence



- **Automated** threat detection & blocking
- **Protects** against hackers, insiders, bots ...
- **Self-learned**: no security rules or policies to write
- **AI-powered API attacks detection**
 - **Data theft, deletion, poisoning, system takeover, API memory attacks, API code injection, etc.**
 - **Cookie, token, or WebSocket session mgt attacks**
 - **API-specific layer 7 DDoS attacks** – multiple types
 - **Login services** breaches, stolen cookies or tokens
- **Protects against new and changing attacks**
Not reliant on specific patterns
- **Automated attack blocking across DCs and**

Extensive Reporting – at Scale

API Auto-Discovery and Full API Activity Visibility for Deep API Insight



API Usage Information

```
{
  "total_requests": 50420,
  "source_ip": [
    {
      "ip": "192.168.11.179",
      "count": 50413,
      "method": [
        "websocket",
        "GET"
      ]
    },
    {
      "ip": "192.168.11.104",
      "count": 7,
      "method": [
        "websocket"
      ]
    }
  ],
  "user_agent": [ {
    "user_agent": "Mozilla",
    "count": 50420
  } ],
  "path": "/eb_demo/ws",
  "device": [ {
    "device": "UBUNTU",
    "count": 50420
  } ]
}
```

- Full API and traffic visibility including every command or method used on any API, for any system, etc.
- Automatically discover APIs and all connected IPs and sessions, etc.
- Full traffic visibility
- API forensic data
- Compliance reports
- Dev Ops reports
- Could be used to map API usage trends
- REST API to access JSON analytics data, attack information, etc. for dashboards and internal reports

Elastic Beam Rich
Data Set for
API Reporting
and Security
Tracking



Industry Support

.... **Elastic Beam's technology would have blocked those attacks,**” said Gartner analyst Mark O’Neill. “Until recently people had to adapt either website security products or general purpose API management products for API security. None of those really were providing built-for-purpose solutions for API security.”

Elastic Beam is on to something good,” “And all the possible use cases where APIs can be exposed to risk — they address each type of risk with this platform. **Those security capabilities are a very much needed detail in security strategy for API use.**” 451 Research analyst Carl Lehmann

Final Thoughts

- Hackers are exploiting APIs today – many attacks undetected
- Providing an easy new attack surface
- IDs and passwords – that protect APIs – never stop hackers
- Need to analyze traffic details and automate attack blocking
- Axway AMPLIFY API Management and Elastic Beam provide the full range of coverage



Thank You!