



Introducing Check Point's New Paradigm for Web Application Firewall & API Security

Tomas Vobruba | Lead Se Slovakia

Jun 2024 UNINFOS Kosice

YOU DESERVE THE BEST SECURITY



ADDING **PREVENTION** TO YOUR CLOUD SECURITY



CNAPP+

Cloud Native Application Protection
& **Prevention** Platform

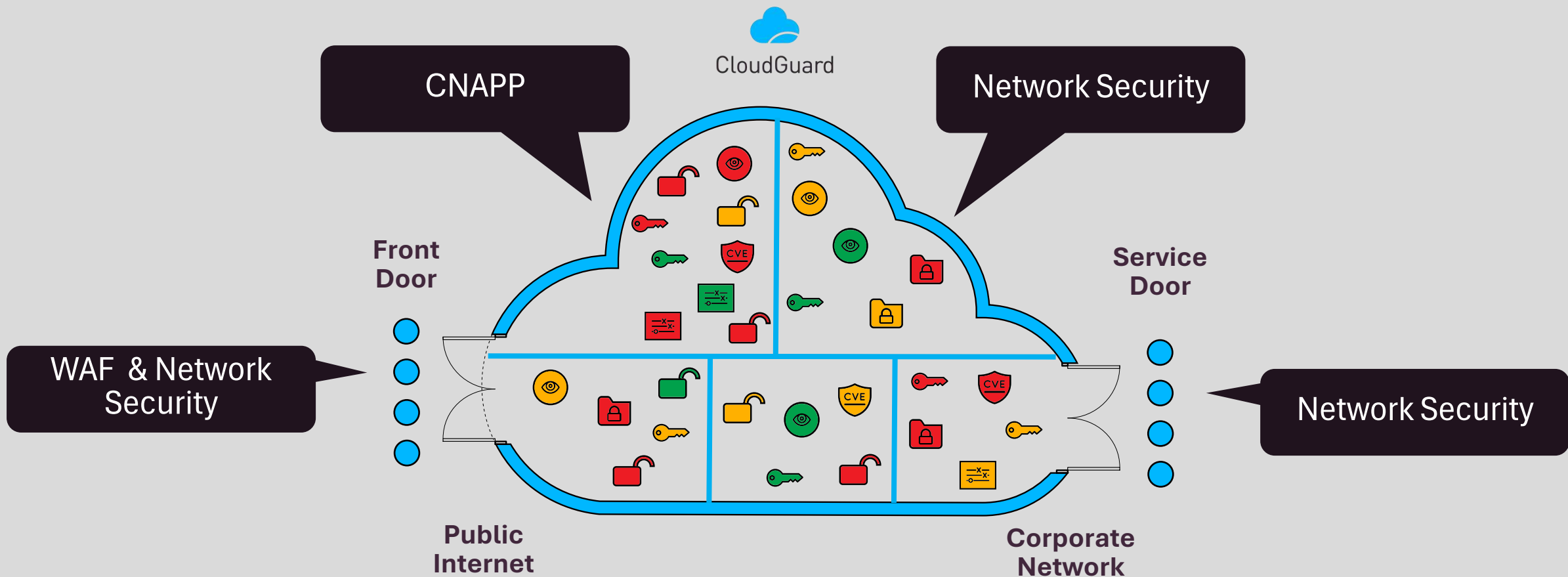


CloudGuard

The Only Cloud Solution Harnessing the Power of **Prevention**



Giving the Power Back to the Security Experts



The Only Comprehensive Cloud Security Solution to Secure Your **Front Door, Service Door, and The Entire Cloud Environment**

1

The Problem with Traditional WAFs Are They Sufficient for Modern Security?

Traditional WAF Solutions Depend on the **Ongoing Maintenance** of Rules & Signature Updates

Too Specific Rules
Leads to Overlooked
Threat Variations and
Demand Adding More
Rules to Address Them



Too Loose Rules
Leads to Overload of
False Positives and
Demand Adding Many
Exceptions

Ongoing Maintenance of Rules & Signatures Just Doesn't Work



Traditional WAF Solutions **Leave You Vulnerable to Zero Day Attacks For Days or Even Weeks**



On Average Traditional WAF Solutions Only Have an **86% Detection Rate** – Missing Malicious Traffic



On Average Traditional WAF Solutions Have an **8% False Positive Rate** - Blocking Legitimate Traffic

Based: on WAF comparison Project

When You Choose Cloud Service Providers' WAF You Multiply Your Efforts & Lose Consistency



WAF Rules



WAF Rules



WAF Rules



It's Time For a WAF & API Security Paradigm Shift

Stop Putting Your Weekend in Danger

- Relying on **Rules & Signature Updates**
- Reacting to **Zero Day Attacks**
- **Missing** Malicious Traffic
- **Blocking** Legitimate Traffic

2

Introducing Check Point's AI-Powered WAF

How to Protect Against
Zero-Day Attacks?



CloudGuard WAF



Powered By Contextual AI Engine

No More Manual Rules & Signature Updates

- Automatic AI-Based WAF Management
- Unmatched Zero-Day Prevention
- High Detection Rate & Low False Positives
- API Discovery & Schema Enforcement

Get Up & Running in Under 15 Min. with Flexible Deployments Options

No More Manual Rules & Signature Updates



Relying on **Rules & Signature Updates**



Automatic **AI-Based WAF** Management

Reacting to **Zero Day Attacks**



Preemptive Zero-Day Prevention

Missing Malicious Traffic



Nearly Perfect Detection Rate

Blocking Legitimate Traffic



Nearly Zero False Positives

Wide API attack surface



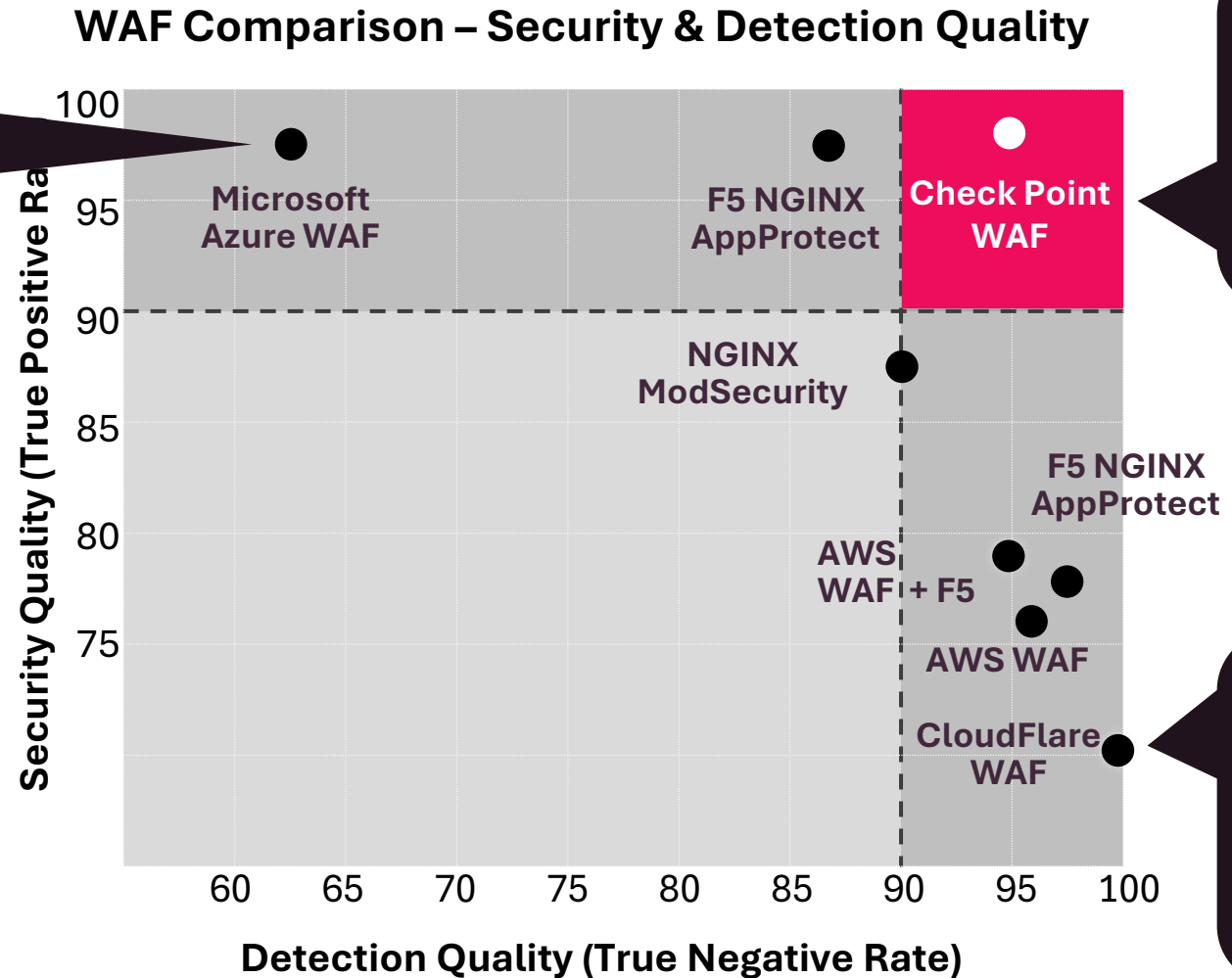
Automatic API Discovery & Security

Check Point WAF #1 in Security Performance

High Detection Rate
BUT
Many False Positives

973,964 legitimate HTTP requests

73,924 malicious payloads



ALMOST PERFECT
Detection Rate & False Positives

Few False Positives
BUT
Low Detection Rate



CloudGuard WAF

Unmatched Prevention Results

Check Point WAF

98.8% vs 86.6%

**Highest Threat Detection
vs Top WAFs**

0.81% vs 8.69%

**Lowest False Positives
vs Top WAFs**

Preemptive Prevention of Top Zero Day Attacks in Recent Years



Sprint4Shell



Log4Shell



Text4Shell



MOVEit

Comprehensive Web Application & API Security



AI #1 Attack Indicator Analysis

Prevent application & API attacks including OWASP Top 10 using contextual AI



IPS

Update your defenses with the latest compromise indicators with 50+ engines packed with AI-based Features and Capabilities



AI #2 Context Analysis Engines

Eliminate False Positives & Keep High Detection Rate By Learning Applications & APIs Behavior



File Security

Analyze any files uploaded and consult Check Point's ThreatCloud regarding the file's reputation.



DDoS

DDoS attack prevention is now available for CloudGuard WAF SaaS deployment



Bot Prevention

Stop automated attacks, Inclusive of user credential abuse



Rate Limit

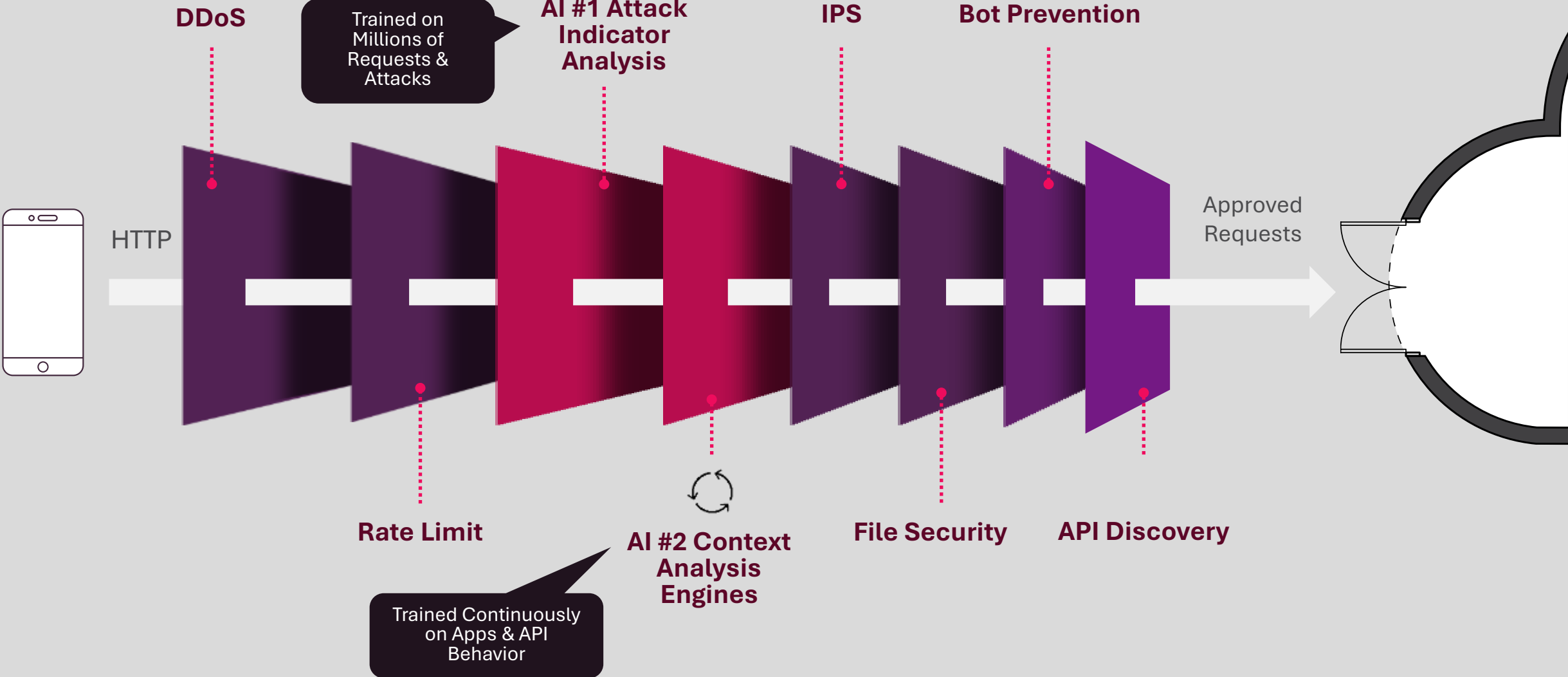
Limit the number of requests to an API/App resource within a configured time, scope to block DDoS attacks



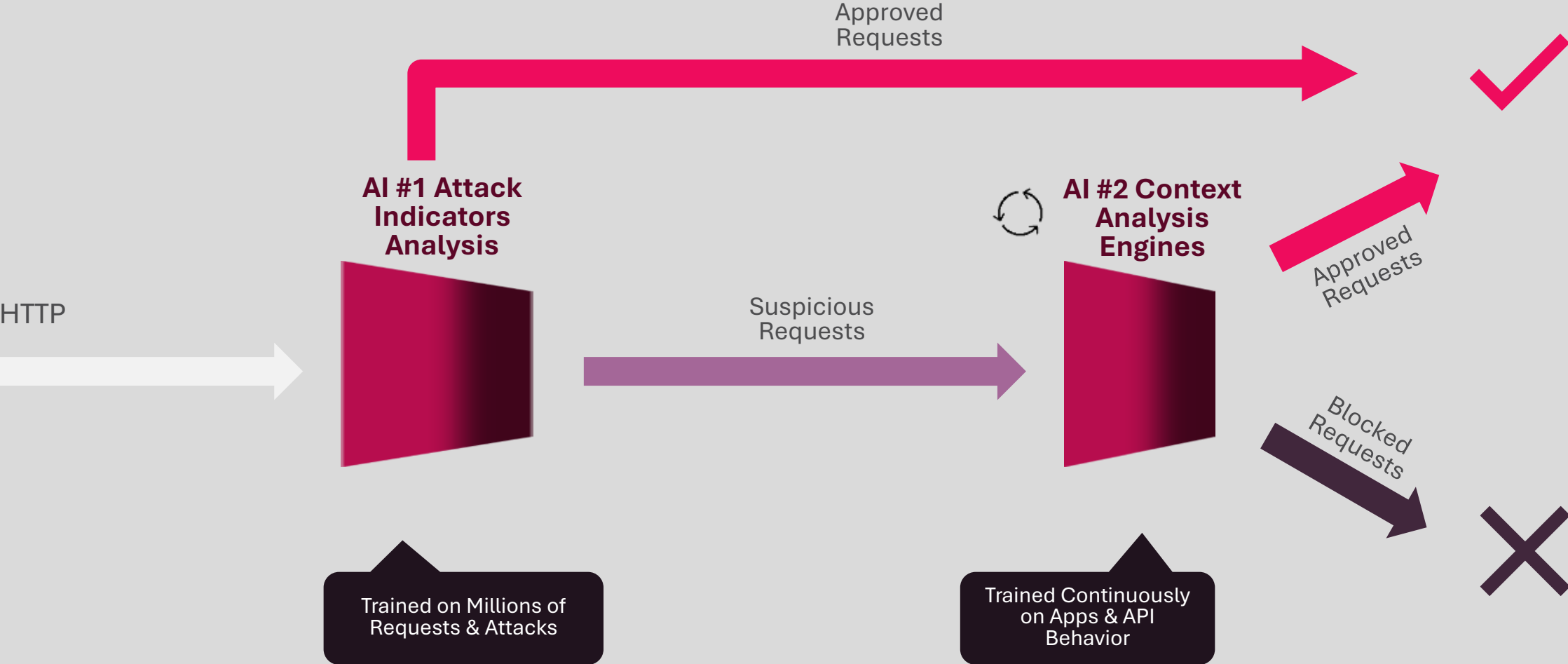
API Discovery

API runtime inspection, discovery with auto generated SWAGGER schema, sensitive data detection, and schema enforcement

Comprehensive Web Application & API Security

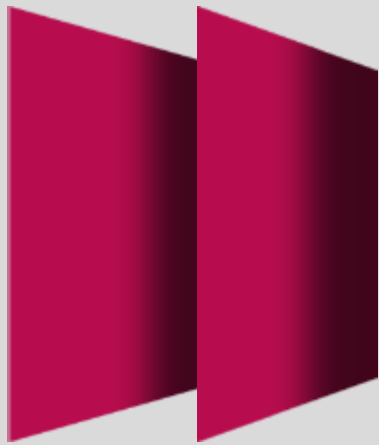


CloudGuard WAF is Based on Cascade Machine Learning Technology



2nd AI Consists of 4 Context Analysis Engines

AI #1 Attack
Indicator
Analysis



AI #2 Context
Analysis
Engines



User Behavior

Compare the user behavior baseline to assess malicious intent from prior user requests



Crowd Behavior

Continuous learning of users' activity with a good reputation, which allow us to auto adapt to the application



Trusted users

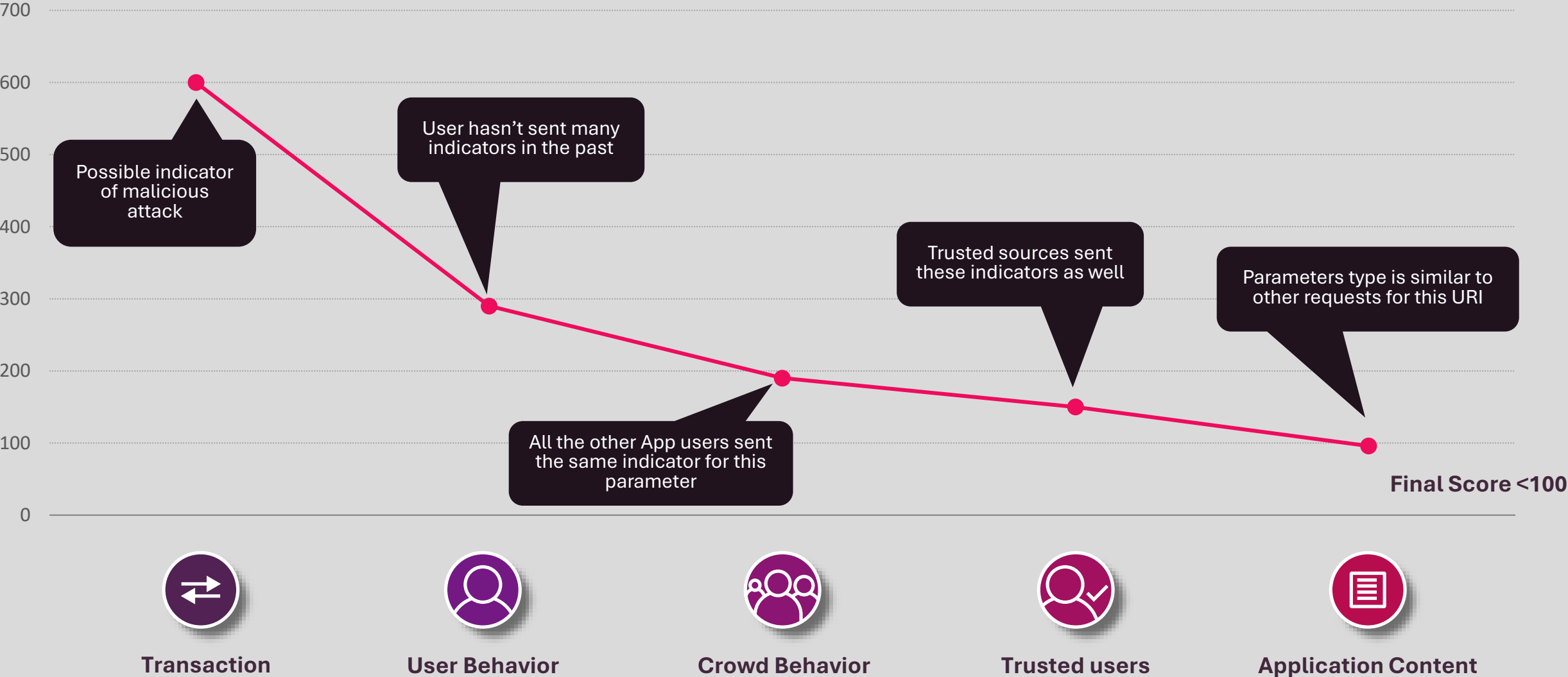
Acceleration of application learning with creation of allow list of permitted inputs from trusted users



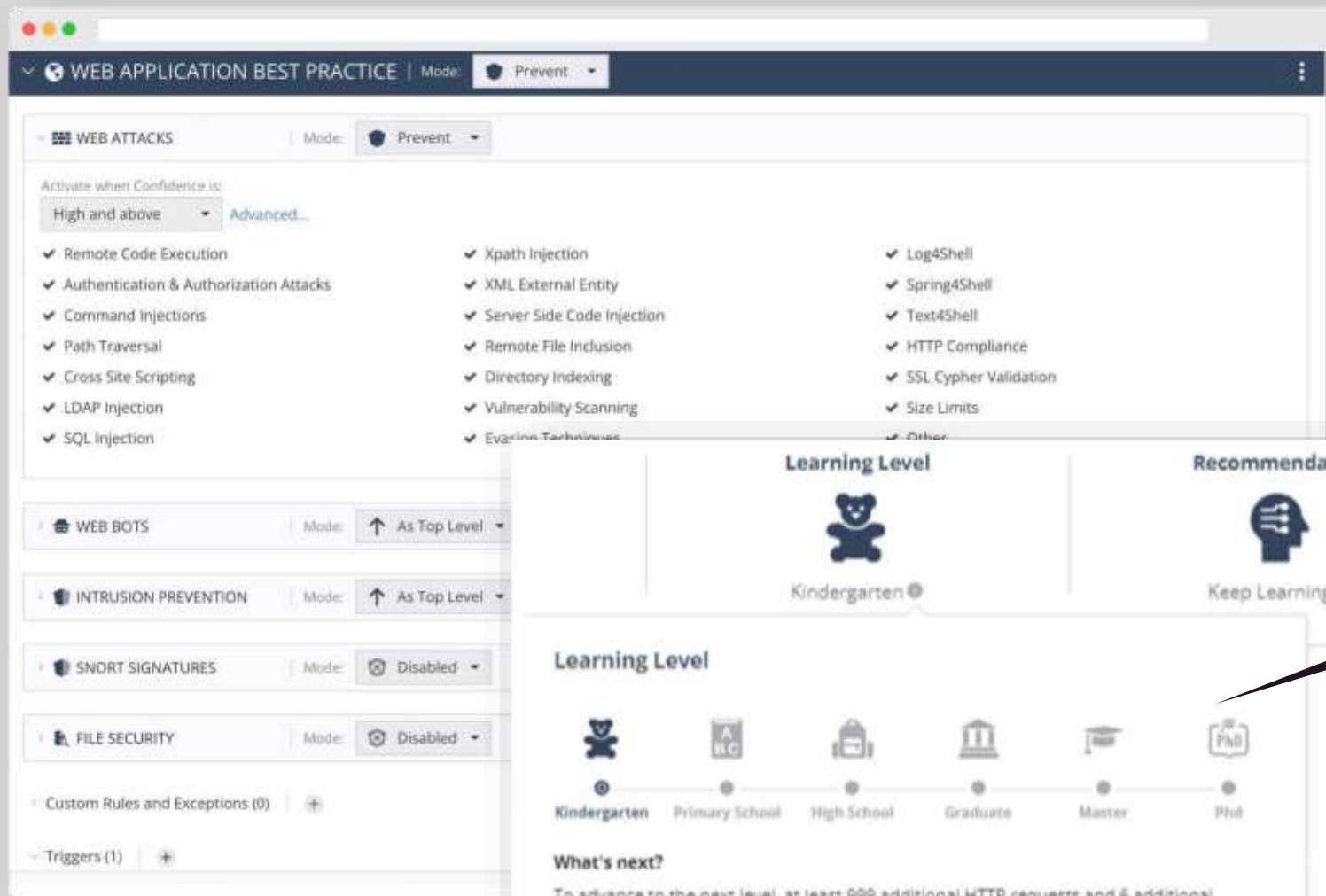
Application Content

Unsupervised learning of fields types and values

Context Analysis Engines **Reduce False Positives**



CloudGuard Continuously Learns Specific Apps & API Behavior



Ready to Prevent Attacks Within Three Days of Deployment

Learning Level is Displayed in The WAF Management Platform

Est. Learning Period
≤ 3 Days

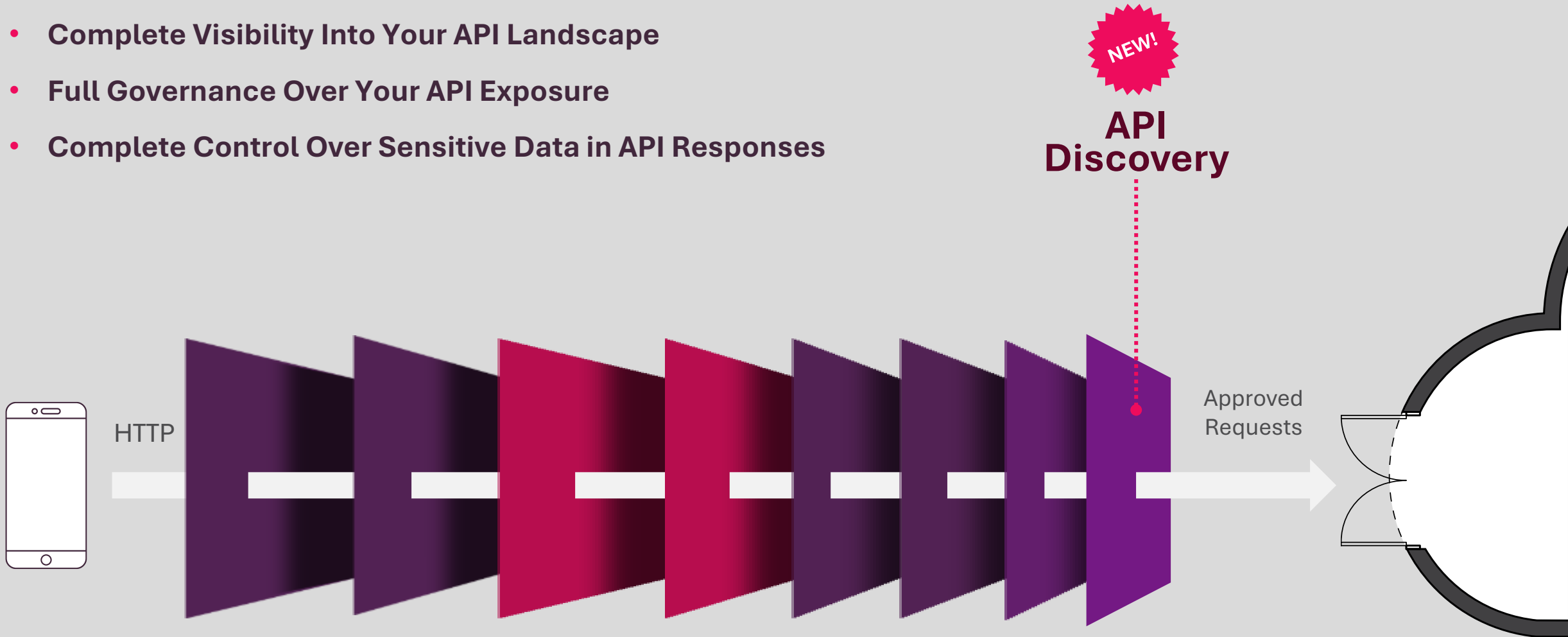
3

Introducing Check Point's API Security

How to Have Visibility and
Protection of APIs?

New API Discovery is Now Available

- Complete Visibility Into Your API Landscape
- Full Governance Over Your API Exposure
- Complete Control Over Sensitive Data in API Responses



CloudGuard WAF Automatically Discovers API Schemas and **Allows You To Enforce Them**

Visibility Into Shadow & Zombie APIs

2. Dashboard & Full API Usage

Governance Over Publicly Exposed APIs

3. Schema Validation and Enforcement

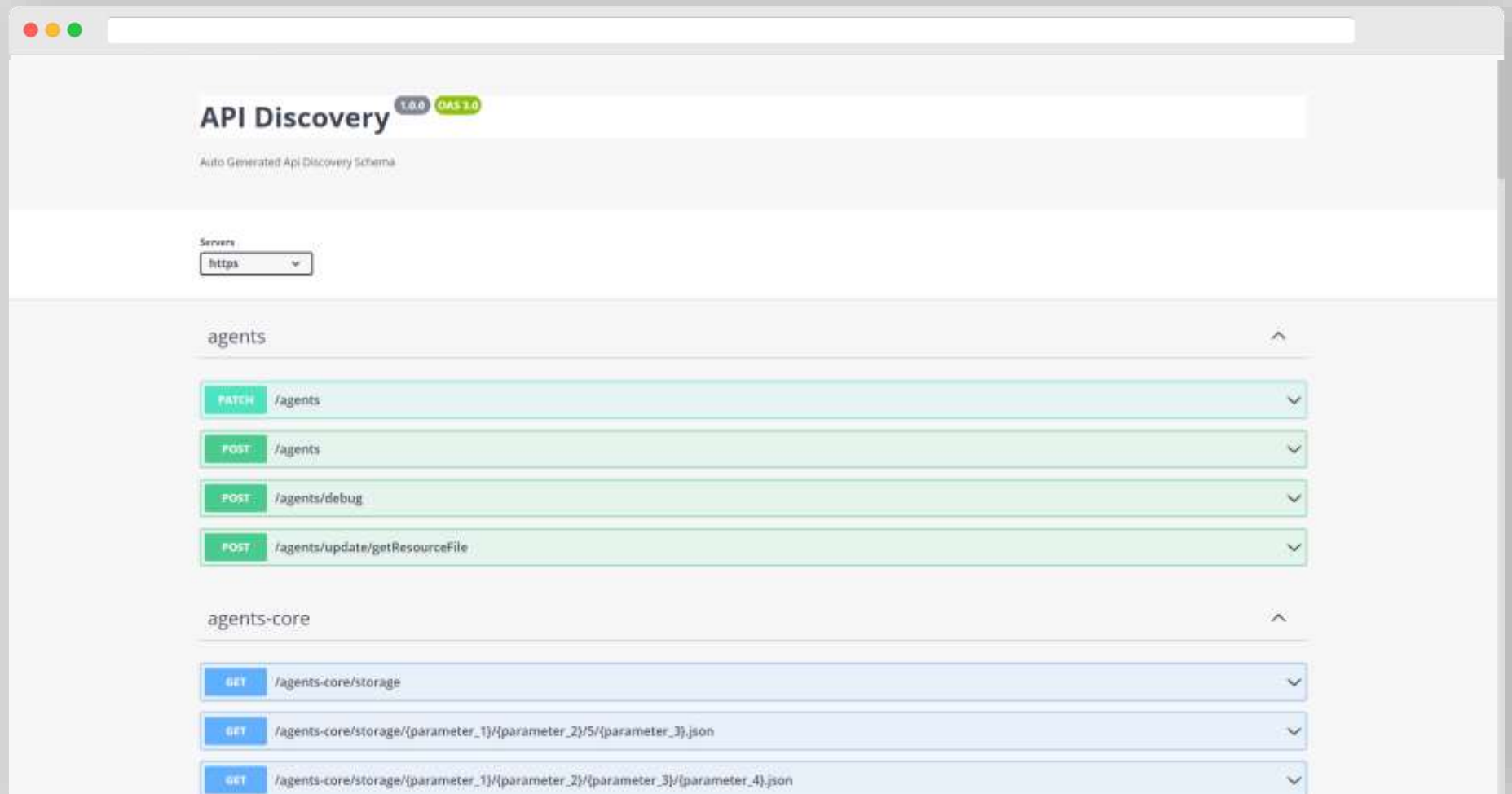
Preventing Unnoticed Sensitive Data

4. Sensitive Data Discovery

1. API Discovery (Auto Generated Schema)

```
    "id": 123, "name": "John", "email": "john.doe@example.com", "password": "123456", "created_at": "2023-01-01T00:00:00Z", "updated_at": "2023-01-01T00:00:00Z", "status": "active", "role": "user", "last_login": "2023-01-01T00:00:00Z", "profile_picture": "https://example.com/profile_pictures/123.jpg", "phone_number": "1234567890", "address": "123 Main St, New York, NY 10001", "bio": "A passionate developer with a love for technology and innovation.", "social_links": {"github": "https://github.com/johndoe", "linkedin": "https://www.linkedin.com/in/johndoe"}, "preferences": {"notifications": true, "language": "en", "timezone": "America/New_York"}, "metadata": {"source": "api", "tags": ["user", "profile"]}}
```

CloudGuard WAF Automatically Inspects & Generates **Your API Schemas**



CloudGuard WAF Allows You To Manage Your API Usage

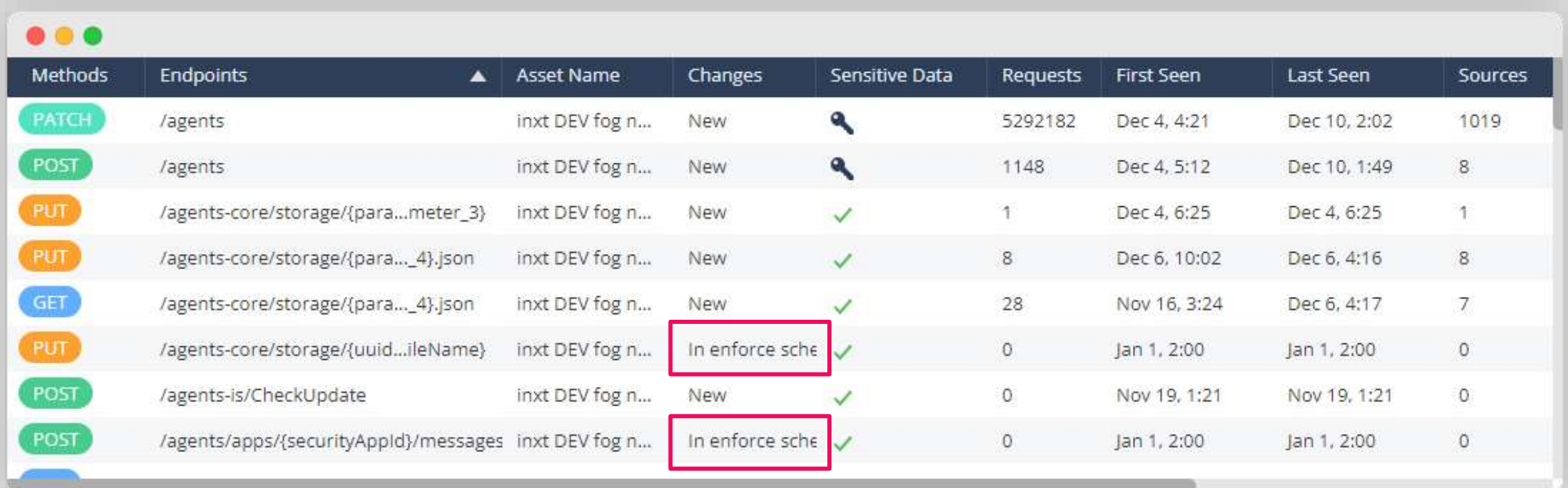
The screenshot displays the CloudGuard WAF API Dashboard. At the top, three key metrics are shown: 166.6K API Requests (with a green trend arrow), 12 Sources (with a green trend arrow), and 146.1K Blocked API Requests (with a red trend arrow). Below these are four main sections:

- Most Used APIs:** A horizontal bar chart showing the top 5 most used APIs. The top API is '/api' with 165,864 requests.
- Least Used APIs/Not in Use:** A list of APIs with zero requests, including '/api/accounts/avatar', '/api/webauthn', '/api/emergencyaccess/trusted', and '/api/settings/domains'.
- Top APIs with Sensitive Data:** A horizontal bar chart showing the top 3 APIs with sensitive data, with 'Email' being the most prominent.
- Discovery of API Changes:** A stacked bar chart showing the discovery of API changes over time, with a legend for 'Exists' (blue) and 'New' (yellow).

At the bottom, an 'API Endpoints' table provides a detailed view of the API endpoints, including their methods, endpoints, asset names, change status, sensitive data flags, request counts, and dates first and last seen.

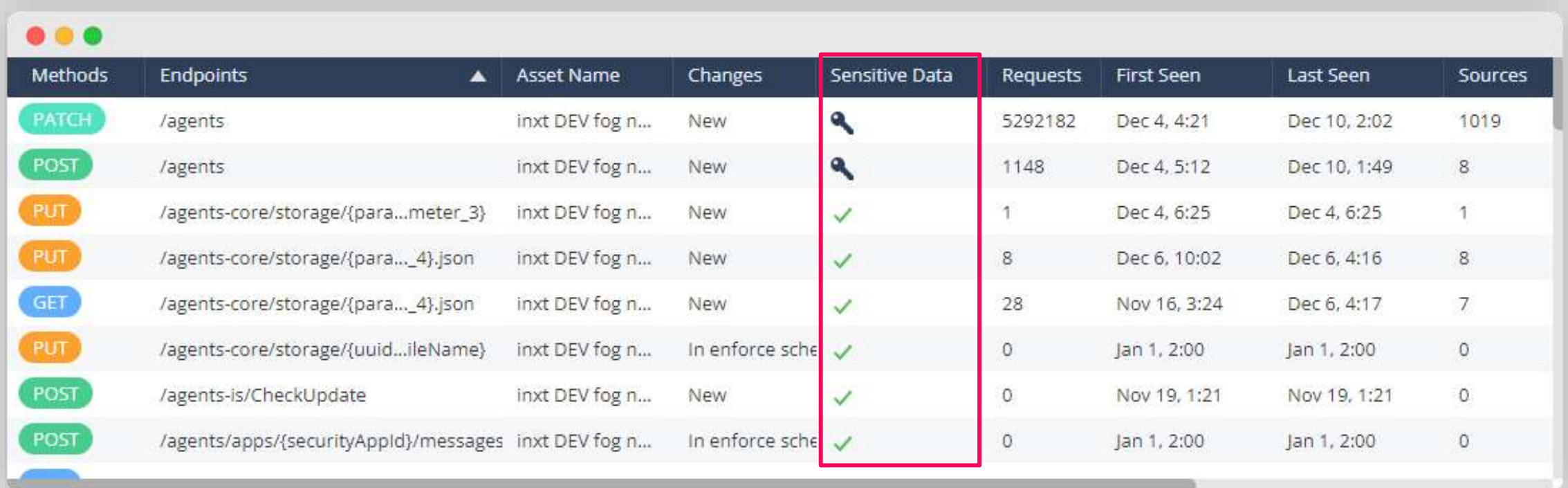
Methods	Endpoints	Asset Name	Changes	Sensitive Data	Requests	First Seen	Last Seen	Sources	Pub
GET	/api	Bitwarden API	Exists	-	14,467	Mar 24, 18:28	Apr 16, 14:02	4	Yes
GET	/api/env	Bitwarden API	New	-	0	-	-	0	No
PUT	/api/accounts/avatar	Bitwarden API	Exists	-	0	-	-	0	No
GET	/api/accounts/profile	Bitwarden API	Exists	-	0	-	-	0	No
PUT	/api/accounts/profile	Bitwarden API	Exists	-	0	-	-	0	No
GET	/api/accounts/revision-date	Bitwarden API	Exists	-	0	-	-	0	No
POST	/api/accounts/verify-email/token	Bitwarden API	Exists	-	0	-	-	0	No
POST	/api/ophers	Bitwarden API	Exists	-	0	-	Mar 22, 23:01	0	No
PUT	/api/ophers/{parameter_1}	Bitwarden API	Exists	-	0	-	Mar 27, 18:51	0	No
PUT	/api/ophers/{parameter_1}/delete	Bitwarden API	Exists	-	0	-	Mar 16, 0:35	0	No

CloudGuard WAF Allows You to Enforce API Schema Blocking Parameters and Identify Changes Outside of The Schema



Methods	Endpoints	Asset Name	Changes	Sensitive Data	Requests	First Seen	Last Seen	Sources
PATCH	/agents	inxt DEV fog n...	New	🔑	5292182	Dec 4, 4:21	Dec 10, 2:02	1019
POST	/agents	inxt DEV fog n...	New	🔑	1148	Dec 4, 5:12	Dec 10, 1:49	8
PUT	/agents-core/storage/{parameter_3}	inxt DEV fog n...	New	✓	1	Dec 4, 6:25	Dec 4, 6:25	1
PUT	/agents-core/storage/{parameter_4}.json	inxt DEV fog n...	New	✓	8	Dec 6, 10:02	Dec 6, 4:16	8
GET	/agents-core/storage/{parameter_4}.json	inxt DEV fog n...	New	✓	28	Nov 16, 3:24	Dec 6, 4:17	7
PUT	/agents-core/storage/{uuid...ileName}	inxt DEV fog n...	In enforce sche	✓	0	Jan 1, 2:00	Jan 1, 2:00	0
POST	/agents-is/CheckUpdate	inxt DEV fog n...	New	✓	0	Nov 19, 1:21	Nov 19, 1:21	0
POST	/agents/apps/{securityAppId}/messages	inxt DEV fog n...	In enforce sche	✓	0	Jan 1, 2:00	Jan 1, 2:00	0

CloudGuard WAF Automatically Detects whether **Sensitive Data** such as PII, PCI, Keys, and Secrets Exist in the Response



Methods	Endpoints	Asset Name	Changes	Sensitive Data	Requests	First Seen	Last Seen	Sources
PATCH	/agents	inxt DEV fog n...	New	🔑	5292182	Dec 4, 4:21	Dec 10, 2:02	1019
POST	/agents	inxt DEV fog n...	New	🔑	1148	Dec 4, 5:12	Dec 10, 1:49	8
PUT	/agents-core/storage/{para...meter_3}	inxt DEV fog n...	New	✓	1	Dec 4, 6:25	Dec 4, 6:25	1
PUT	/agents-core/storage/{para..._4}.json	inxt DEV fog n...	New	✓	8	Dec 6, 10:02	Dec 6, 4:16	8
GET	/agents-core/storage/{para..._4}.json	inxt DEV fog n...	New	✓	28	Nov 16, 3:24	Dec 6, 4:17	7
PUT	/agents-core/storage/{uuid...ileName}	inxt DEV fog n...	In enforce sche	✓	0	Jan 1, 2:00	Jan 1, 2:00	0
POST	/agents-is/CheckUpdate	inxt DEV fog n...	New	✓	0	Nov 19, 1:21	Nov 19, 1:21	0
POST	/agents/apps/{securityAppId}/messages	inxt DEV fog n...	In enforce sche	✓	0	Jan 1, 2:00	Jan 1, 2:00	0

4

Deployment

How to Deploy a Cloud-Designed WAF within 15-60 Minutes?

If You Loved CloudGuard WAF, Replacing Your Current WAF is Easier Than Ever



<15 min.

Update Your DNS
Record & Immediately
Route Traffic through
**WAF as a
Service**

<1 Hour

Deployment within
**Kubernetes
Ingress**

<1 Hour

Deployment within
**On-Prem.
Environment**

ETA <15 Min

Prove domain ownership

Route domain DNS record to Check Point WAF SaaS

Domain Configuration

demo.inextshop2.com

Certificates & Domain Management

Certificates managed by Check Point Upload certificates

To prove ownership of demo.inextshop2.com add the following records to your DNS:

CNAME name:

CNAME value:

Domain ownership validation succeeded

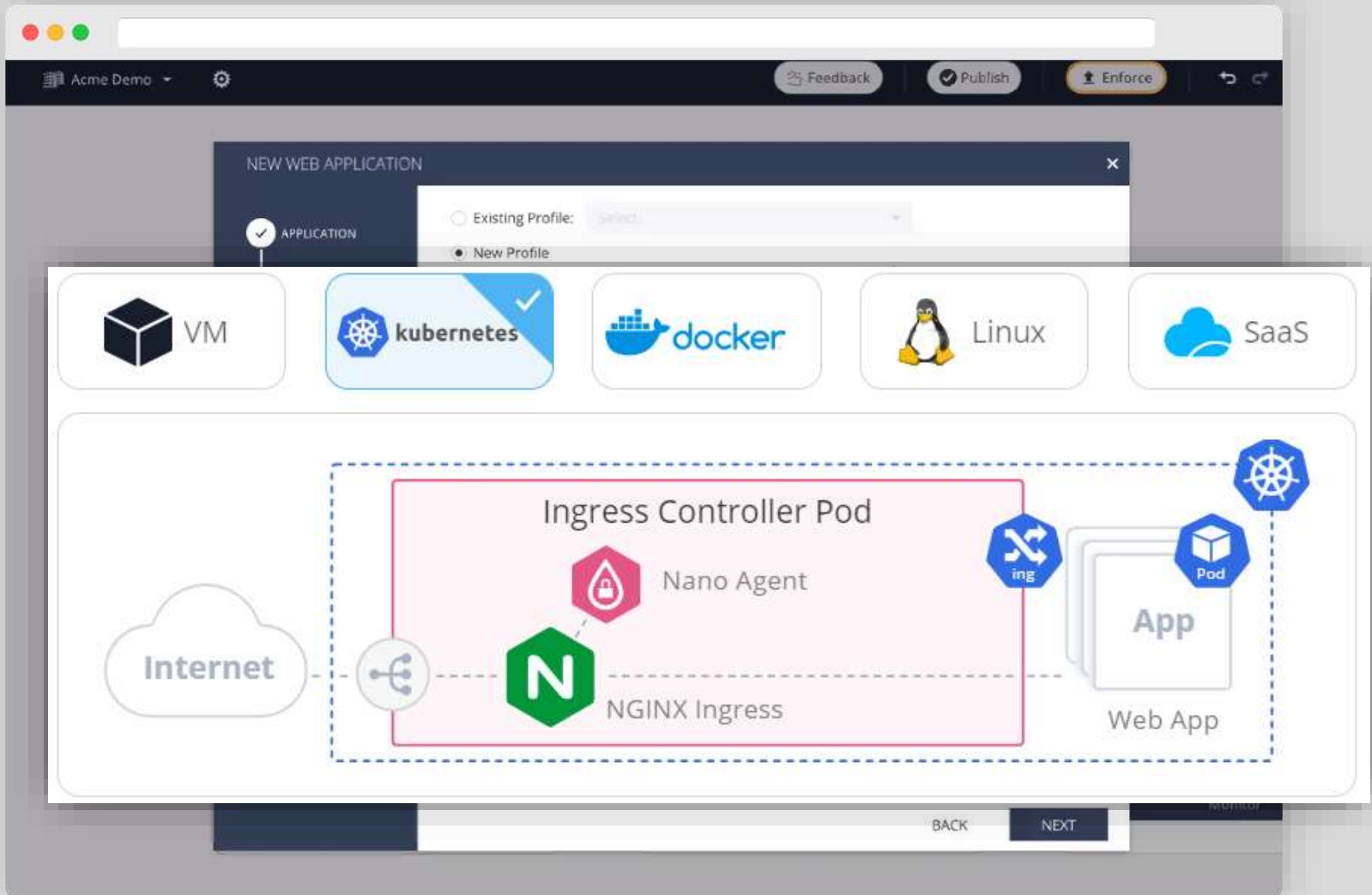
Update the DNS record for demo.inextshop2.com to point to the following CNAME value:

Status: Ready

Test Access

Cancel

Unlike Cloud Native WAFs, CloudGuard WAF Offers Deployment Into Your Kubernetes Ingress



ETA
<1 Hour

CloudGuard WAF Offers Additional Deployment Options

VM Gateway



Docker Deployment



ETA
<1 Hour



Linux (NGNIX)



Kong Gateway Pod



Summarizing **Check Point Unmatched Advantage** Over Cloud Native WAF Solutions

		
Use Case	CloudGuard WAF	Cloud Native WAF
Zero-Day Prevention	✓ Immediate	✗ Avg. 40 days*
WAF Management	✓ AI - Automated	✗ Manual
Detection Accuracy	✓ Leader 97%	✗ Avg. 87%*
API Discovery	✓ Yes	✗ Not Provided
Flexible Deployments	✓ Multi-Cloud & On-Prem	✗ Single Cloud

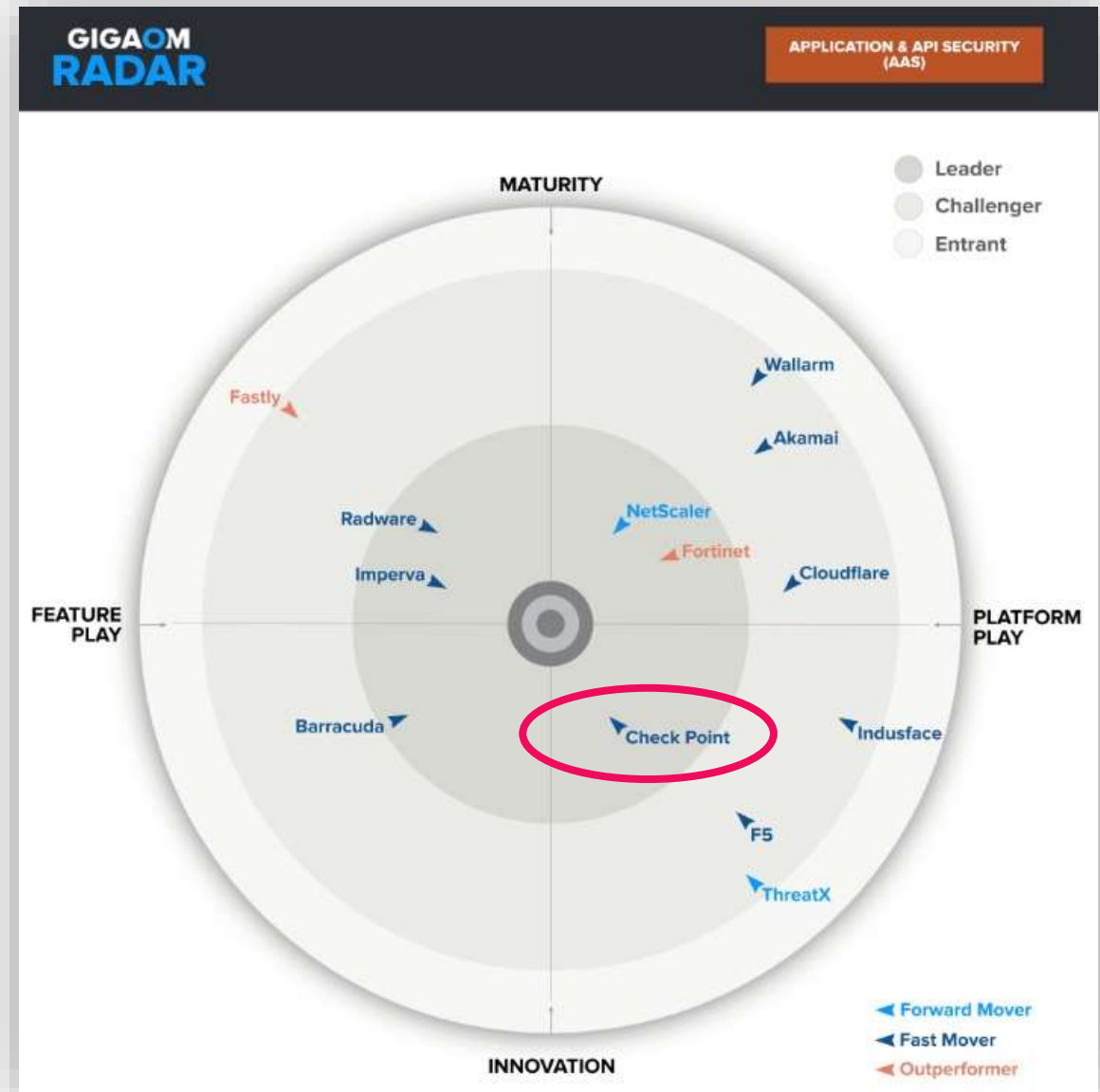
Check Point is the Leader in Web Application & API Security



Don MacVittie

Analyst of DevOps,
Security & Risks Analyst,
GigaOm

“ While All Vendors can either import or detect APIs and most vendors can do both, CloudGuard is able to do both and **generate sample protection rules based upon the definition and information gleaned from traffic.** This earned them our highest score on the API import and discovery key feature.”



CloudGuard WAF is Also Available as Open-Source



- Fully Open-Source Project
- The Only Open Source WAF Project Certified with **LEXFO** Code Audit
- Aligned With **OpenSSF** Best Practices
- Fast Growing Community with More Than **600 Active Installation**

CloudGuard WAF is Offered in 3 Packages

Community



**Open Source
for FREE**

Advanced



**Agent-Based
or SaaS**

Premium



**Agent-Based
or SaaS**

Check Point Provides Full **Application Security** With Open-Source Projects



open-appsec

+



Spectral

CloudGuard WAF

Securing Web Application & APIs with AI-Based WAF

CloudGuard Code Security

Securing Code, Repositories, and CI/CD Pipeline



CloudGuard WAF as Part of CNAPPP Platform

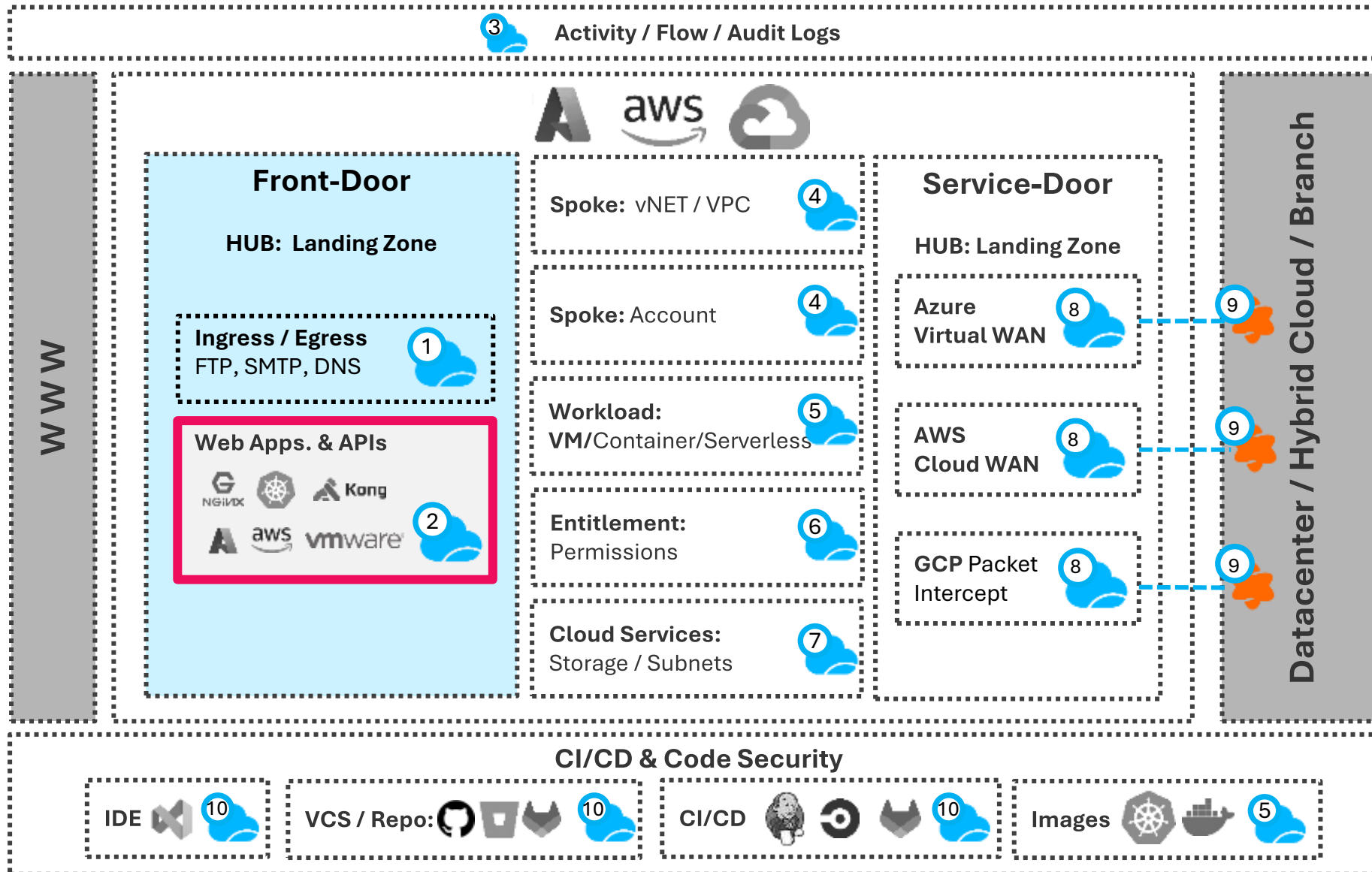
8 Modules & 52 Engines

Network Security	WAF	CSPM	CWPP	CIEM	CDR	DSPM	Code Security
IPS Protection	ML-based Threat Prevention		Container Vulnerability	Graph Visualization	Network Log Analysis		Code & IaC Scanning
Threat Emulation & Extraction	API discovery and security		Malware Scanning	Effective Permissions Calculation	Kubernetes Network Log Analysis	Coverage of Azure & AWS	IaC, Secret, & CI/CD Detectors
Hybrid Cloud VPN	Bot Prevention	Service Inventory	Runtime Threat Detection	Overprivileged Identities Detection	Account Activity Log Analysis	Cloud Native Classification Engine:	Custom Detectors
Cloud Native WAN Integration	API Schema Validation	Out-of-the-box Rulesets	Behavior Anomalies	Inactive Identities Detection	Threat Identification	Amazon Macie & Microsoft Purview	Offline & Online Scanning
Hub & Spoke Segmentation	File Security	Best Practice Rulesets	Function Self Protect (Serverless)	Behavior Anomalies	Behavioral Analysis	Identify PII, PCI, PHI	Software Composition Analysis (SCA)
Bot Protection, DLP, TP	Intrusion Prevention (IPS)	Compliance Standards Rulesets	Agent & Agentless	Best Practice Violations	Anomaly Detection	Indicated as a risk factor	Repos, Local, & Pipeline Scan
IaC deployment	IaC deployment	Custom Rules					

CloudGuard Unified Platform



CloudGuard WAF & API Security as Part of Check Point Cloud Security Blueprint



- CloudGuard**
- 1 Firewall, IPS & DLP
 - 2 WAF & API: Agent / SaaS
 - 3 Cloud Detection & Response
 - 4 Hub & Spoke Segmentation
 - 5 Workload Security
 - 6 Entitlement Security (CIEM)
 - 7 Cloud Posture Management
 - 8 Cloud WAN with NGFW
 - 9 Hybrid Cloud VPN
 - 10 Code Security

Thank You