API Security:
Why Context is key

Martijn Bosschaart
Security Solutions Engineer EMEA
martijnb@salt.security

SALT

Why the need for API Security?

SALT


Get us into the headlines!
Keep us out of the headlines!
CEO
Public Relations
CISO

SALT

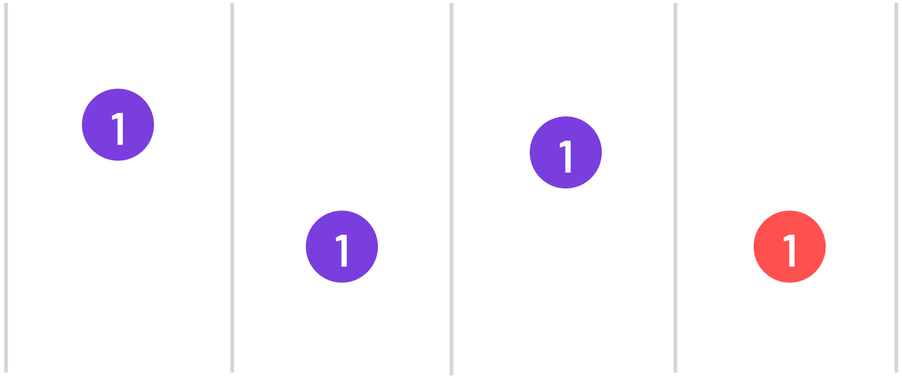
What do all these household brands have in common?

- ✓ big companies
- ✓ well-funded security programs
- ✓ sophisticated AppSec teams
- ✓ mature pipeline testing
- ✓ WAFs and gateways

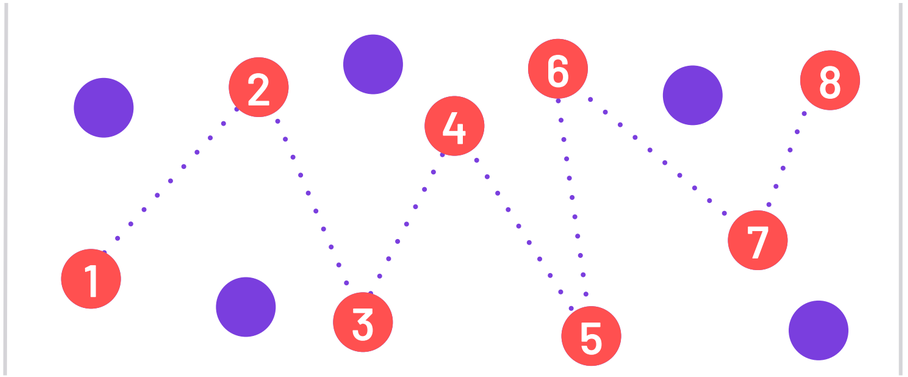
All suffered API breaches

Why all the bad headlines? The world has changed

	PAST	TODAY
Attack surface	Few APIs, static, minimal shared data	1000s of APIs, dynamic, extensive shared data
Attacks	One and done	Low and slow
	Single step, known vulns (SQLi, XSS), seconds to minutes – formulaic attacks	Multiple steps, business logic attacks, looks legit, days to weeks – custom attacks, based on recon



Easy to detect, easy to test for



Difficult to detect, difficult to test for

SALT

OWASP API Security Top 10 2023

A1: Broken Object Level Authorization

A2: Broken Authentication

A3: Broken Object Property Level Authorization

A4: Unrestricted Resource Consumption

A5: Broken Function Level Authorization

A6: Unrestricted Access to Sensitive Business Flows

A7: Server Side Request Forgery

A8: Security Misconfiguration

A9: Improper Inventory Management

A10: Unsafe Consumption of APIs

https://owasp.org/www-project-api-security/

SALT

Quiz: What is the most dangerous http response code?

200 OK

Why WAFs and API gateways cannot protect APIs

Signatures block known attacks
APIs all have unique logic

Today's tools block transactions
Need to block the attacker

Limited context = false positives
Holistic view = high fidelity

> Protecting web APIs with general-purpose application security solutions continues to be **ineffective** since each new API endpoint represents an additional and potentially unique attack vector into your systems.
>
> — Gartner

> … a generic product [WAF] could never fully understand the intricacies of each custom web application. This approach is just **not sufficient** to properly protect critical applications …
>
> — OWASP

SALT

How are we going to solve this?

A gameplan for success in API security

Understand that it's a strategy

- Quickly minimize risk without friction
- Produce more secure APIs, enrich the ecosystem

Start right, not left

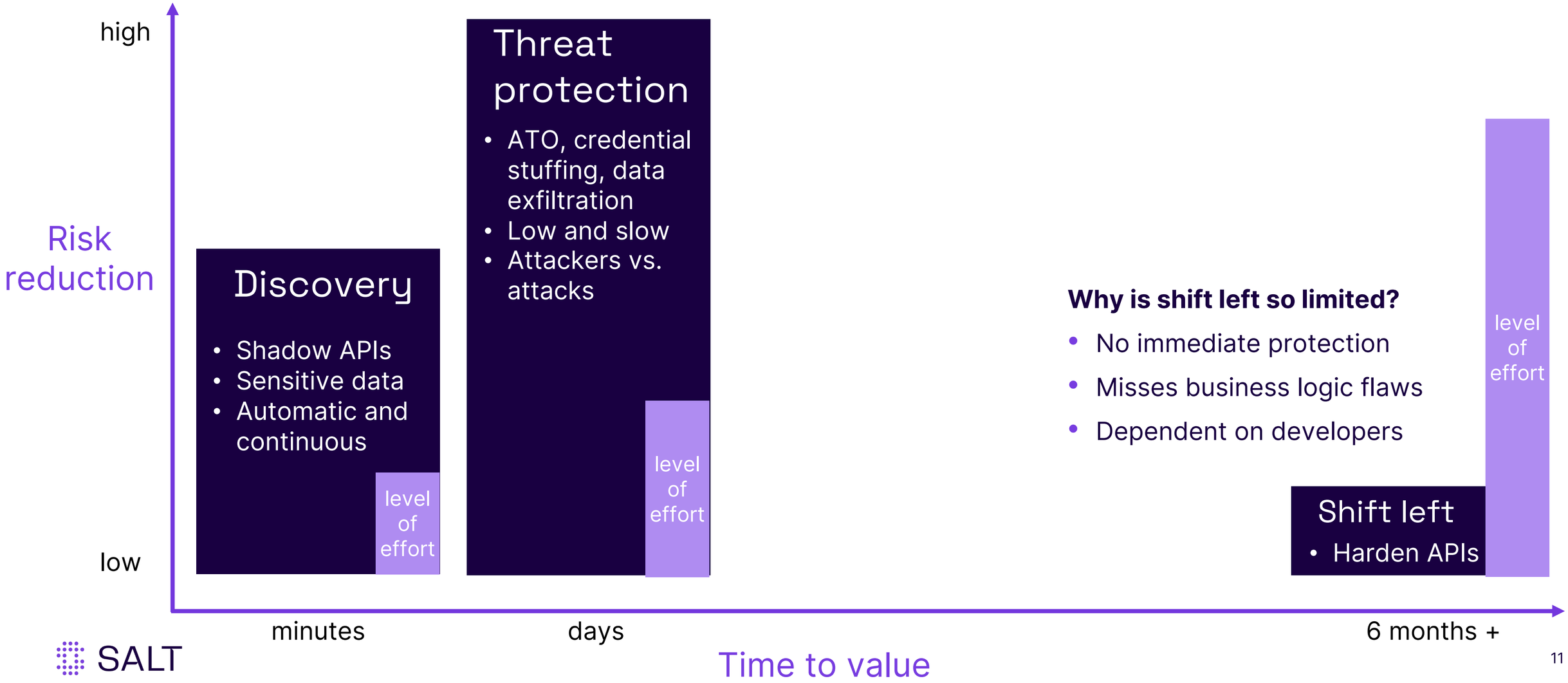
- Discovery + threat protection reduce risk now
- Pre-prod testing misses business logic gaps

Start now, not later

- API sprawl, blind spots, data leaks are common
- API-based ATO is too easy

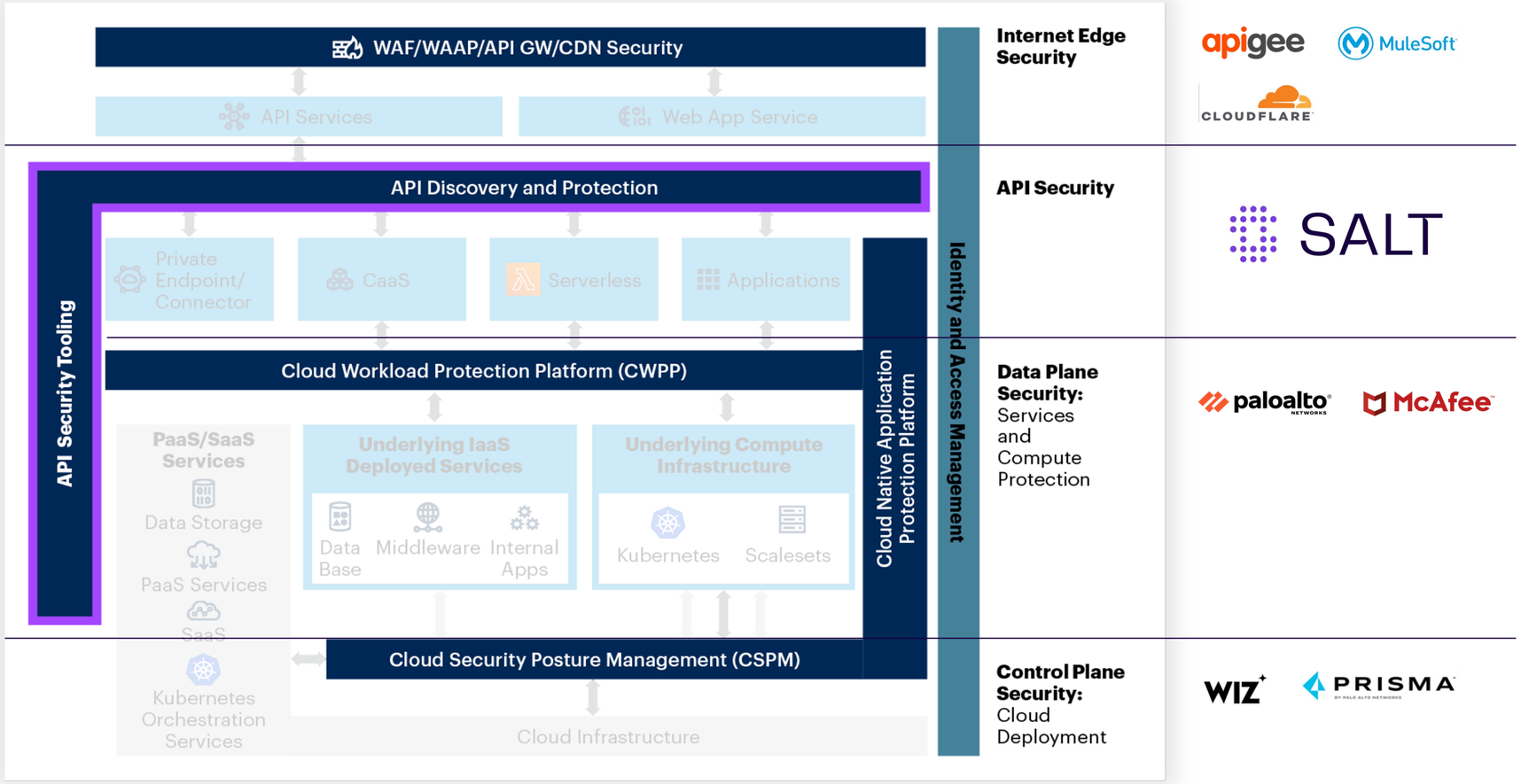
Today's dynamic threats require adaptive intelligence

Where to focus in API security



SALT

Gartner on how companies need implement API security



"Advance Your Platform-as-a-Service Security,"

Richard Bartley, 25 August 2021

Gartner

Why is cloud-scale big data needed to gain context?

Raw Traffic

Billions of calls per month

RESPONSE

200 OK

Server:nginx/1.6.2
Date:Mon, 02 Apr 2018 09:10:13 GMT
Connection:keep-alive
X-Frame-Options:SAMEORIGIN
Content-Type:text/html; charset=UTF-8
Content-Length: 41

{"account_balance": 2006, "userId": 107939053, "description": null, "subscriptions": {"has_more": false, "total_count": 0, "object": "list", "data": [ ], "url": "/v1/customers/f86e2276-98d0-4ad6-81ef-68fa1bcf5281/subscriptions"}, "livemode": false, "currency": "usd", "shipping": null, "id": "f86e2276-98d0-4ad6-81ef-68fa1bcf5281", "delinquent": false, "created": 1504792830, "default_source": null, "object": "customer", "sources": {"has_more": false, "total_count": 0, "object": "list", "data": [ ], "url": "/v1/customers/f86e2276-98d0-4ad6-81ef-68fa1bcf5281/sources"}, "discount": null, "email": "john.doe@mail.com", "metadata": {}}

REQUEST

GET /v1/customers/f86e2276-98d0-4ad6-81ef-68fa1bcf5281?accountId=f86e2276-98d0-4ad6-81ef-58fc1bcf5382 HTTP/1.1

Accept: "*/*"
Accept-Encoding: "gzip, deflate"
Authorization:
"Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbGciOiJSUzI1NiIsImF1ZCI6IjN2MUo4WHczemVHdUdPT2ImQWh0WFdFUkliLCJlbWFpbCI6ImNhcm90NDEyMkBnbWFpbC5jb20iLCJleHAiOiIxNjAzNzg2Njc3liwiaWF0IjoiMTYwMzcwMDI3NyIsImlzcyI6Imh0dHBzOi8vY2hhcmdlc25ldHdyb2suYXV0aDAuY29tIiwic3ViIjoiYXV0aDB8NWY5NT0xZmU1ZDkxMWUwMDEiLCJ0eXAiOiJKV1QifQ.0hNZPMk14zkX7mcFk1zfwO0gzoLhLbaygv13PNHFT2w"
Authorization.alg: "RS256"
Authorization.aud: "3v1J8Xw3zeGuGOOifAhPXWERB"
Authorization.email: "carot4122@gmail.com"
Authorization.exp: "1603786677"
Authorization.iss: "https://chargesnetwrok.auth0.com"
Authorization.sub: "auth0|5f954fe5d911e001"
Authorization.typ: "JWT"
Authorization.userId: "1603700277"
Connection: "keep-alive"
Content-Length: "0"
Content-Type: "application/json; charset=UTF-8"
Host: "payments-api.dnssf.com"
User-Agent: "secful-script"
X-Forwarded-For: "54.183.50.90"
Cookie:_ga="GA1.3.630674023.1502871544" _gid="GA1.2.1579405782.1502871544" userId=" 107939053 "

Structural Metadata

100s to 1000s per call

domain
protocol
method
URI
URI parameter names
URI parameter count
URI parameter length
URI parameter datatype
request.headers
request.headers count
request.headers.names
request headers.names.datatype
request headers.names.length
request headers.names.classification
request headers names.value.datatype
request.headers.names.value.length
request.headers.names.value.classification
request.size
request.body.content-type
request.body.content-type.parameters
request.body.content-type.parameters.names
request.body.content-type.parameters.names.datatype
request.body.content-type.parameters.names.length
request.body.content-type.parameters.names.classification
request.body.content-type.parameters.names.value.datatype
request.body.content-type.parameters.names.value.length
request.body.content-type.parameters.names.value.classification
response.size
response.headers
response.headers count
response.headers.names
response.headers.names.datatype
response.headers.names.length
response.headers.names.classification
response.headers names.value.datatype
response.headers.names.value.length
response.headers.names.value.classification
response.body.content-type
response.body.content-type.parameters
response.body.content-type.parameters.names
response.body.content-type.parameters.names.datatype
response.body.content-type.parameters.names.length
response.body.content-type.parameters.names.classification
response.body.content-type.parameters.names.value.datatype
response.body.content-type.parameters.names.value.length
response.body.content-type.parameters.names.value.classification
...

Behavioral Attributes

100s to 1000s per call

session correlation

user identification

API characteristics (internal/external)

authentication identification

static data determination

dynamic data determination

request header data relationships

request body data relationships

response header data relationships

response body data relationships

sensitive data relationships

call sequences

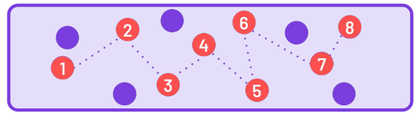
call frequency

user attributes

user past behavior

...

Analysis Windows



seconds

minutes

hours

days

weeks

and beyond ...

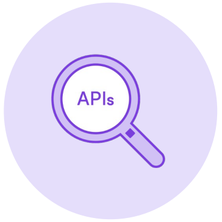
AI Algorithms

The only way to effectively discern user intent in near real-time with no alert fatigue (false positives) and no missed security events (false negatives)

SALT

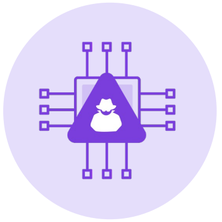
What do we need to do?

Top use cases for API security



Discover shadow APIs

Prevent sensitive data exposure



Stop API attacks

Prevent ATO, data exfiltration

Shift Left with proactive security

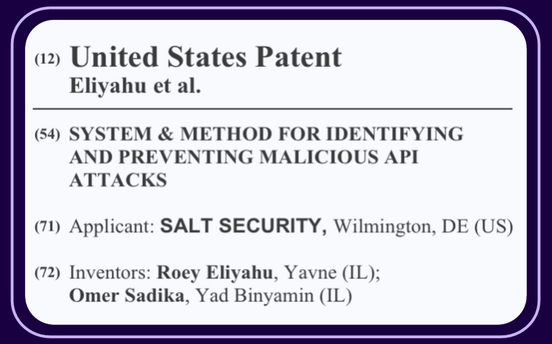
Accelerate incident response

Provide remediation insights

Simplify compliance

SALT

Salt – a unique architecture delivering adaptive intelligence



(12) **United States Patent**
Eliyahu et al.

(54) **SYSTEM & METHOD FOR IDENTIFYING AND PREVENTING MALICIOUS API ATTACKS**

(71) Applicant: **SALT SECURITY,** Wilmington, DE (US)

(72) Inventors: **Roey Eliyahu**, Yavne (IL); **Omer Sadika**, Yad Binyamin (IL)

API Context Engine (ACE) Architecture

- ✓ trillions of calls analyzed
- ✓ 100s of baselines, months of data
- ✓ diverse models, 4+ years of training
- ✓ real-time analysis
- ✓ network effect across customers

Salt Security API Protection Platform

Fix write more secure APIs using production insights

Discover
identify APIs and manage their posture

Protect
block attackers by discerning user intent

ML/AI - diverse, trained models

cloud-scale API data lake

100s of behavioral attributes

bidirectional API metadata – requests and responses

load balancers | API gateways | CDNs | Kubernetes

Salt in action

1. Not inline
2. Automated, continuous
3. Environment agnostic

Clients

SaaS, web, mobile, IoT

API traffic

API collection options

Agentless

API gateways

apigee, MuleSoft, Kong, AWS API Gateway, Azure API Management, IBM DataPower, axway, webMethods, TIBCO, WSO2, software AG, gravitee.io

microservices

kubernetes, docker

load balancers, edge, servers

f5, NGINX, citrix, AWS ALB, envoy, Akamai, CLOUDFLARE Workers, Gigamon, servers, Traffic Mirroring

cloud

aws, Azure, Google Cloud

Block
manual
or automatic

Mirror all
API traffic

Customer environment | Salt Cloud

Salt API Protection Platform

HYBRID SERVER

Salt Security
Hybrid/Edge
(optional)

API metadata

SALT CLOUD

Salt Security
Cloud Console

Alerts, remediation tickets

Operations and management

Jira Software, PagerDuty, slack, splunk>, sumo logic, snowflake, SOAR, Webhooks

- API discovery
- Data classification
- Baselining 100s of attributes
- Attack detection/prevention

SALT

How is Salt different from a typical WAF?

WAF

- Inline
- Programed with known-bad patterns
- Blocks known-bad transactions
- Provides basic blocking

SALT

- Out of band
- Learns normal API behavior
- Blocks attackers abusing API business logic
- Provides visibility, runtime protection, and proactive security

Salt API Security

Visibility

- Continuous API inventory
- Identify zombie and shadow APIs
- Sensitive data leak detection
- Continuous sensitive data catalog

Runtime Protection

- Baseline all API traffic and users
- Block attackers during recon
- Block OWASP API Top 10 ++
- Block injections (XSS, SQLi, L/RCE)
- Block OWASP Top 10 attacks
- L3 blocking, Protocol, DDoS attacks

Proactive Security

- API security posture insights
- OAS analysis
- Automated API vuln hunting
- Leverage attackers as pen testers

Addressing the OWASP API Top 10 Threats

OWASP API Security Top 10 Threats	WAFs	API Gateways	OAS Schema Validation	On prem API Security	SALT
API1:2019 – Broken Object Level Authorization	✗	✗	✗	✗	✓
API2:2019 – Broken Authentication	✗	manual	✗	partial	✓
API3:2019 – Excessive Data Exposure	✗	✗	✗	partial	✓
API4:2019 – Lack of Resources and Rate Limiting	✗	manual, partial	manual, partial	partial	✓
API5:2019 – Broken Function Level Authorization	✗	partial	✓	✓	✓
API6:2019 – Mass Assignment	✗	✗	✗	partial	✓
API7:2019 – Security Misconfiguration	partial	✗	✗	✓	✓
API8:2019 – Injection	(signature based)	(signature based)	✗	✓	✓
API9:2019 – Improper Assets Management	✗	manual, partial	manual, partial	✓	✓
API10:2019 – Insufficient Logging and Monitoring	partial	partial	partial	✓	✓

Only Salt delivers the depth of protection you need

Weeks of data, 4 years+ of training models, real-time analysis, network effect

Better at discovery

- Intelligent parsing of APIs, endpoints
- More accurate data classification

Better at runtime

- Stop more “in the wild” attacks
- Block attackers, not attacks

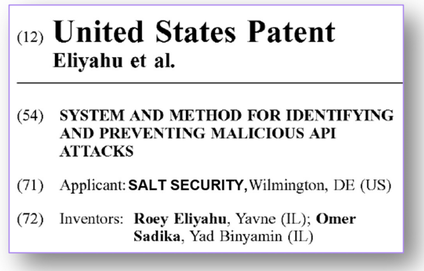
Better at shift left

- Pre-prod tests tuned to your APIs
- Runtime insights for dev teams

Salt Security defined and leads the API security category

> Salt Security has automatically blocked tens of 1000s of credential stuffing attacks. Without Salt, we'd be out of business.
>
> Nir Valtman
> VP product and data security
>
> FINASTRA

SALT LABS


(12) **United States Patent**
Eliyahu et al.

(54) **SYSTEM AND METHOD FOR IDENTIFYING AND PREVENTING MALICIOUS API ATTACKS**

(71) Applicant: **SALT SECURITY**, Wilmington, DE (US)

(72) Inventors: **Roey Eliyahu**, Yavne (IL); **Omer Sadika**, Yad Binyamin (IL)

ABInBev · AstraZeneca · Nationwide® · KPMG

MassMutual · ESTĒE LAUDER · GAP · Takeda

AON · MARKEL® · Amway · zoom

CapitalG · SEQUOIA · CROWDSTRIKE

Forbes 2021 NEXT BILLION-DOLLAR STARTUPS · Gartner COOL VENDOR 2020 · 2020 SINET 16 INNOVATOR · WINNER 2021 CISO CHOICE AWARDS Application Security · SC awards 2021 FINALIST Best Emerging Technology

Thank you!

Questions?