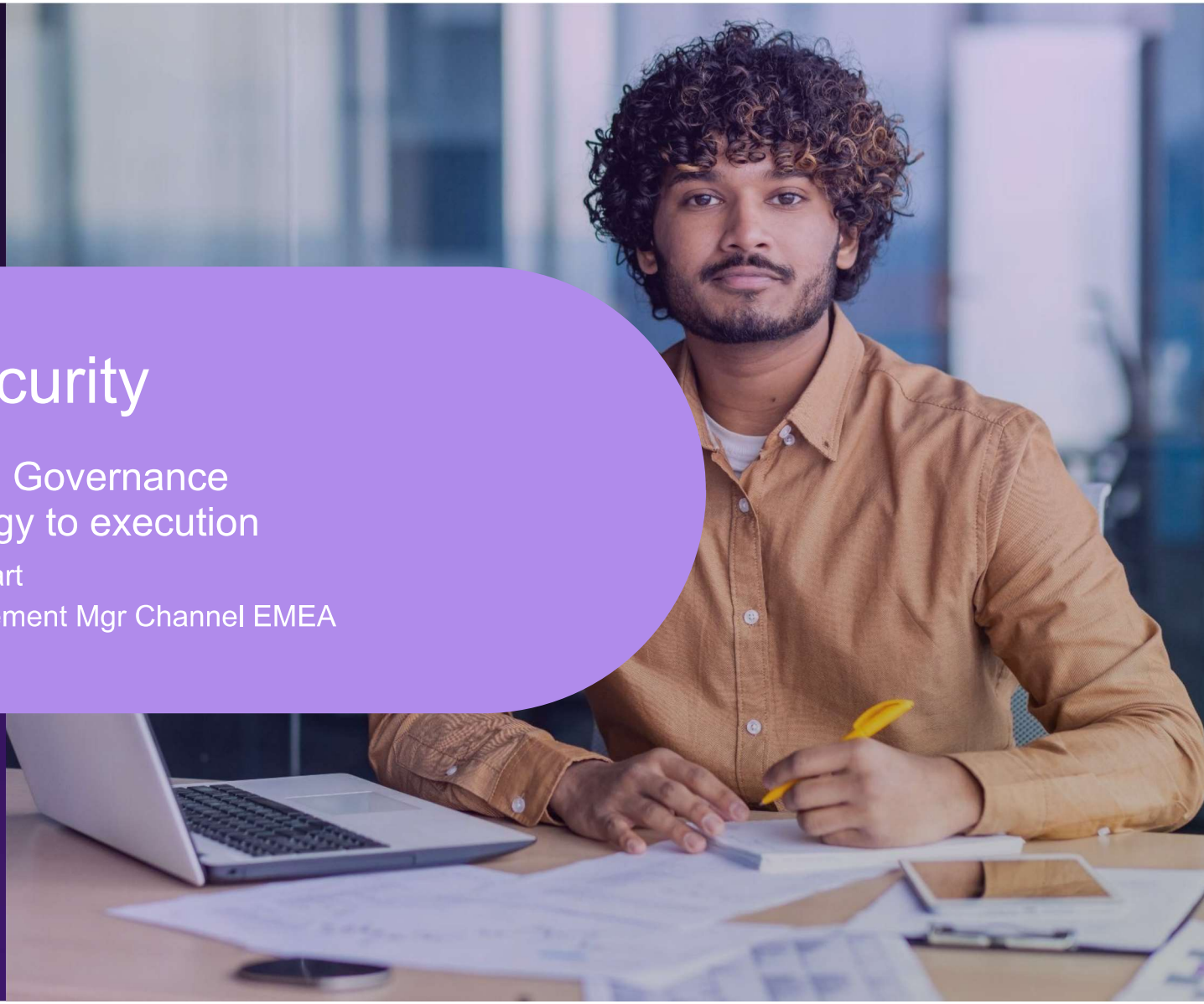
Salt Security

API Posture Governance
From strategy to execution

Martijn Bosschaart
Technical Enablement Mgr Channel EMEA



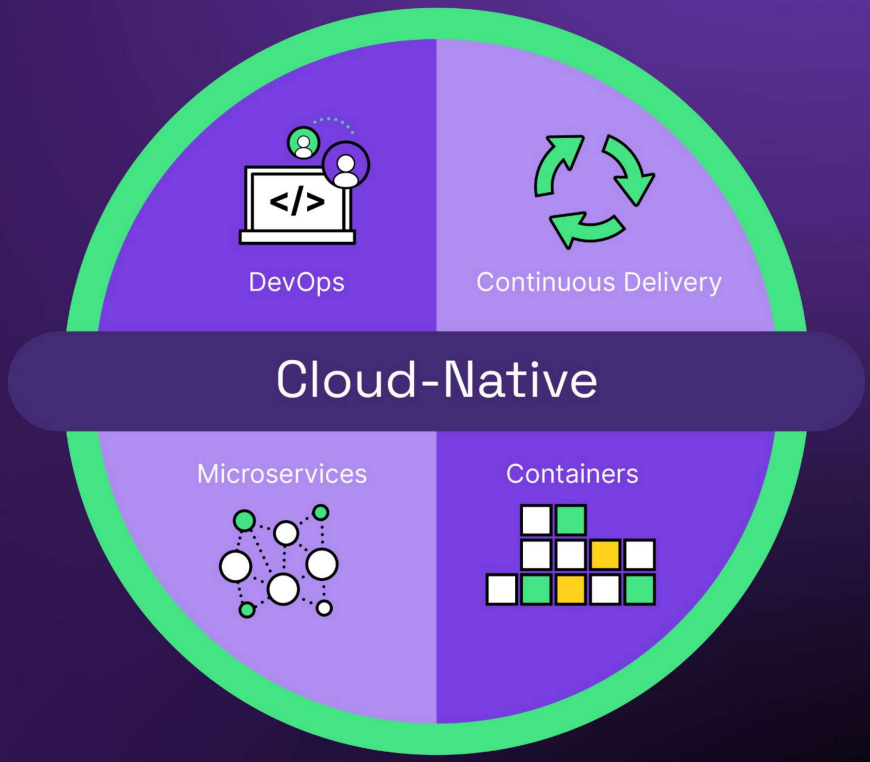
Why API Security?

© 2024 Salt Security, Inc. All rights reserved.

The Big Industry Wave is Cloud-Native Apps

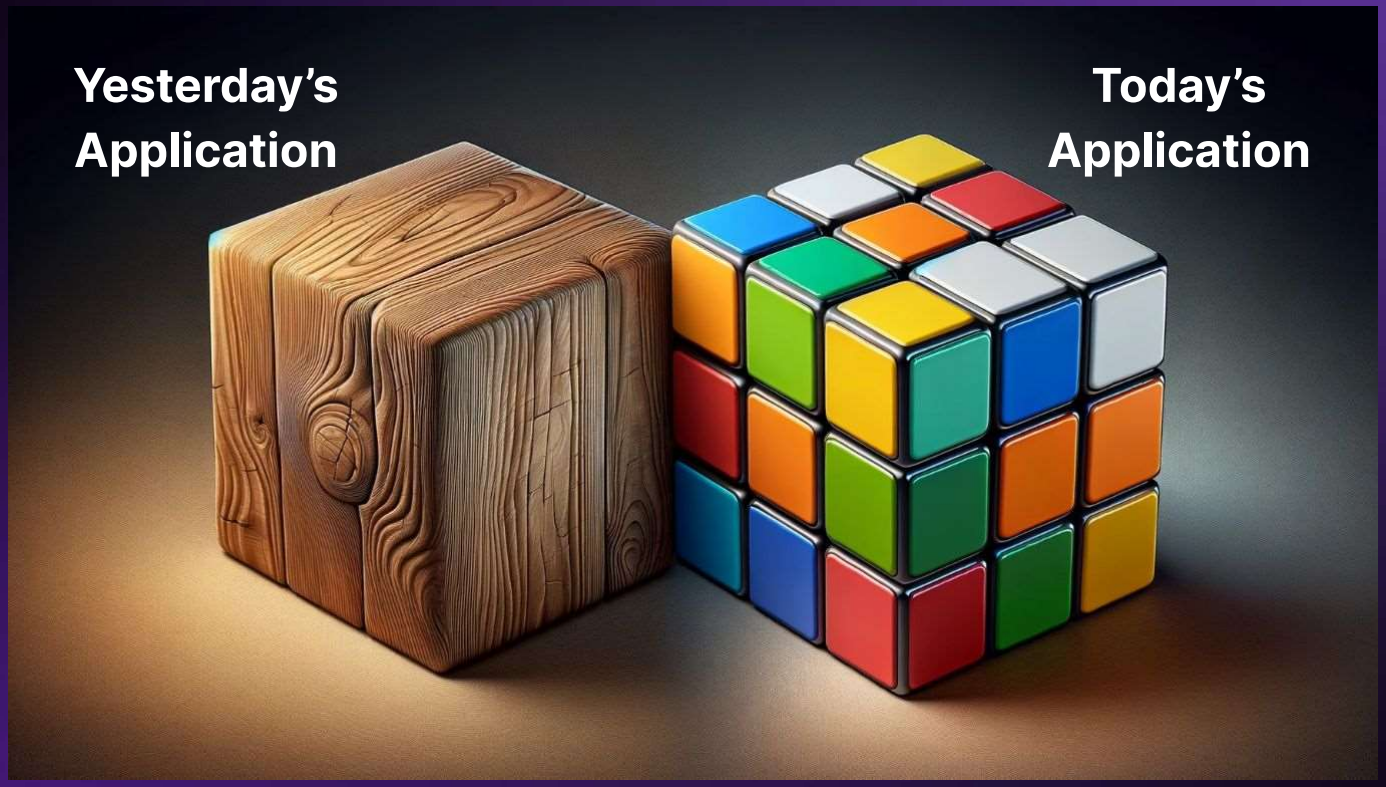
Every company is moving to modern **cloud-native applications**

This means a disintegration of monolithic applications into **API-first** companies that rely on **microservices** to drive revenue and customer experience



© 2024 Salt Security, Inc. All rights reserved.

Today, applications are mostly a bundle of interconnected APIs



© 2024 Salt Security, Inc. All rights reserved.

The Evolution of Applications

Monolithic Apps

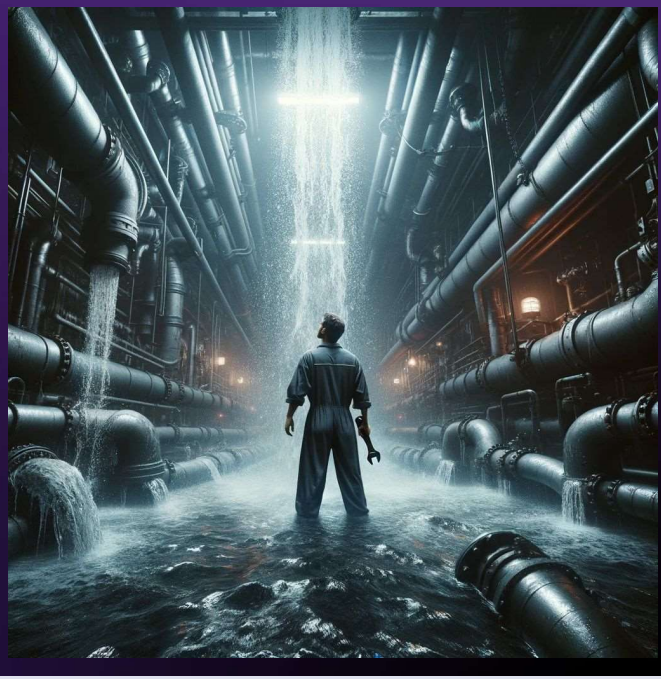
Early 2000s until 2015

Microservices and Distributed Apps

2015 to 2023

The Era of Generative AI

2024 and beyond



© 2024 Salt Security, Inc. All rights reserved.

GenAI accelerates business growth…and is a huge cybersecurity risk

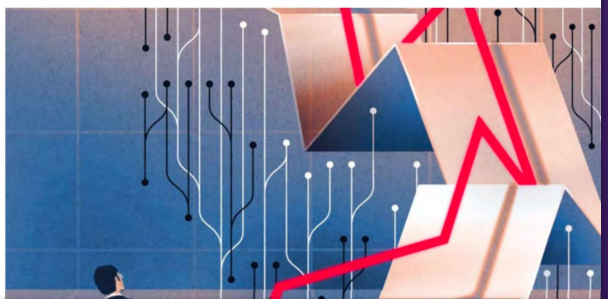
Promising exponential growth and transformation

"Generative AI has the power to be as impactful as some of the most transformative technologies of our time."

- Siridya Sridharan, VP and group research director at Forrester

"79% of director- to C-suite-level respondents expect generative AI to transform their organizations within three years"

- Deloitte Deloitte's State of Generative AI in the Enterprise Quarter one report January 2024



CIO JOURNAL

AI Is Generating Security Risks Faster Than Companies Can Keep Up

Rapid growth of generative AI-based software is challenging business technology leaders to keep potential cybersecurity issues in check

By Belle Lin

Aug. 10, 2023 2:28 pm ET WSJ PRO

© 2024 Salt Security, Inc. All rights reserved.

Number of APIs is Exploding with No End in Sight

57%

of dynamic HTTP traffic on Cloudflare network is API related

And growing as a result of GenAI usage...APIs created in seconds

© 2024 Salt Security, Inc. All rights reserved.

How to create APIs with AI demo

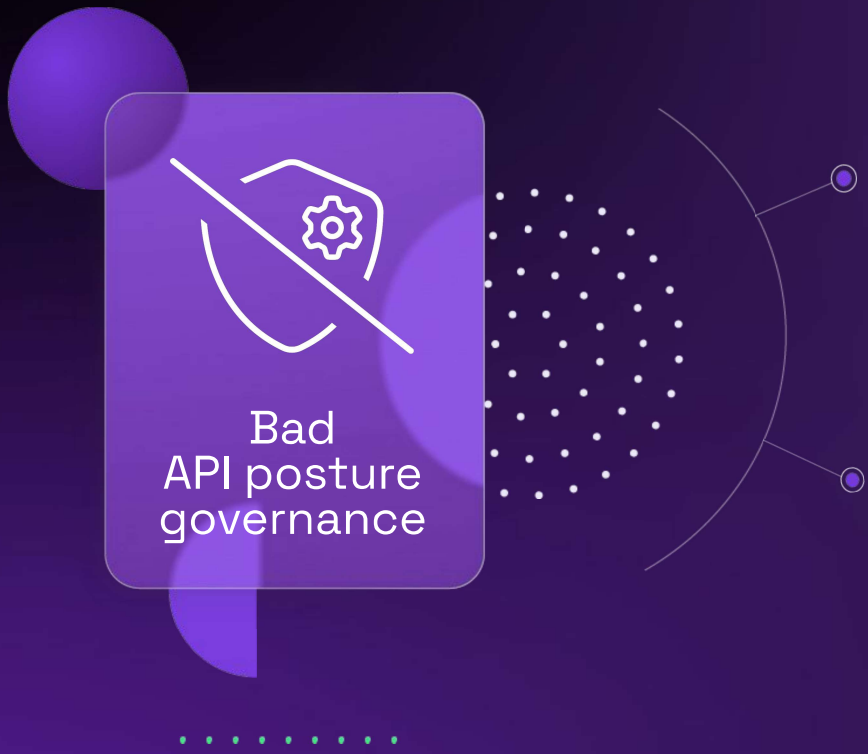
© 2024 Salt Security, Inc. All rights reserved.

All of these Companies Had a WAF and API Gateway

They were all Still Breached

© 2024 Salt Security, Inc. All rights reserved.

Security challenges with becoming API-first



API Sprawl and high frequency of updates

- What APIs do I have?
- What is their purpose?
- What data is associated with them?

Inadequate posture governance program

- What risk is associated with our APIs in use?
- Do our APIs meet corporate standards, industry best practices, and regulatory requirements?
- Have we defined our standards for stakeholders?

© 2024 Salt Security, Inc. All rights reserved.

Security challenges with becoming API-first

- Incumbent defenses serve different purposes and can only detect and block known bad transactions
- As a result, malicious behaviors, such as low and slow API reconnaissance and active attack campaigns targeting business logic and misconfigurations go undetected

© 2024 Salt Security, Inc. All rights reserved.

Security challenges with becoming API-first

Lifecycle stakeholders

(devops, architects, secops, etc.) are not in sync with security posture governance standards

Existing production shields

don't have API threat intelligence required to provide in-depth defense

Appsec tools

such as DAST, don't have API context to appropriately test APIs

© 2024 Salt Security, Inc. All rights reserved.

Legacy Technology Can Not Keep up with the Problem

API Security Requirement	WAF/API Gateways
Deep Observability	✗
Complete API Inventory	✗
API Posture Governance	✗
Automatic Business Logic Attack Detection	✗
DAST Integrations	✗
API Inventory Threat Hunting	✗
API SIEM Event Stream	╲

© 2024 Salt Security, Inc. All rights reserved.

How do we solve this problem?

© 2024 Salt Security, Inc. All rights reserved.

The **AI-Infused** API Security Journey

Posture Governance

Continuous Discovery

- Accurately inventory API assets with expert trained & Neural Network powered panoramic discovery
- Identify sensitive data in motion
- Map APIs to owners & functions

Crawl

Posture Management

- Define & enforce corporate API standards with the industry's only API security posture policy engine
- Adopt industry best practices from expansive API policy library
- AI-based insights help assess and prioritize riskiest API assets

Walk

Threat Protection

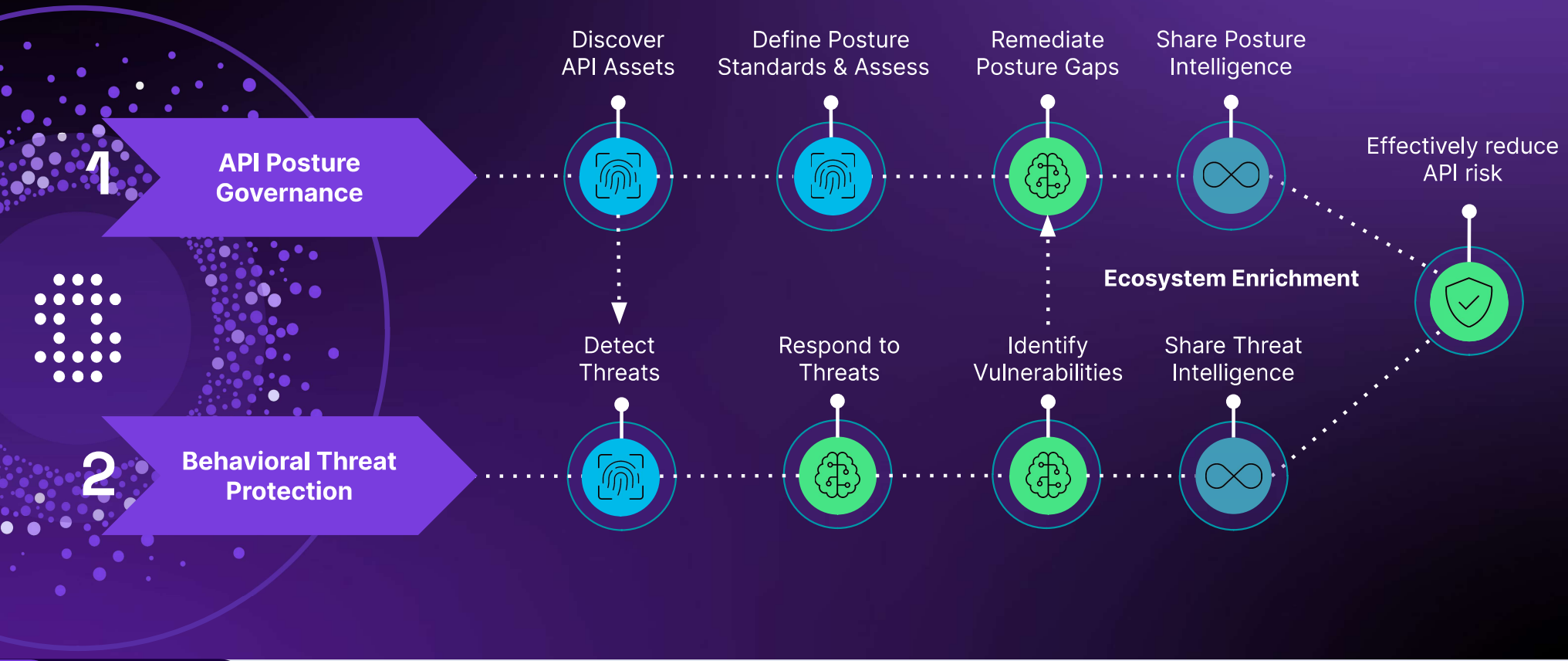
Behavioral Threat Protection

- Identify malicious intent from benign anomalies with extensively trained, cloud-scale AI & ML models
- Deliver API threat intel to SIEM or other tools in the SecOps ecosystem
- AI-based attacker insights help assess and prioritize riskiest API assets

Run

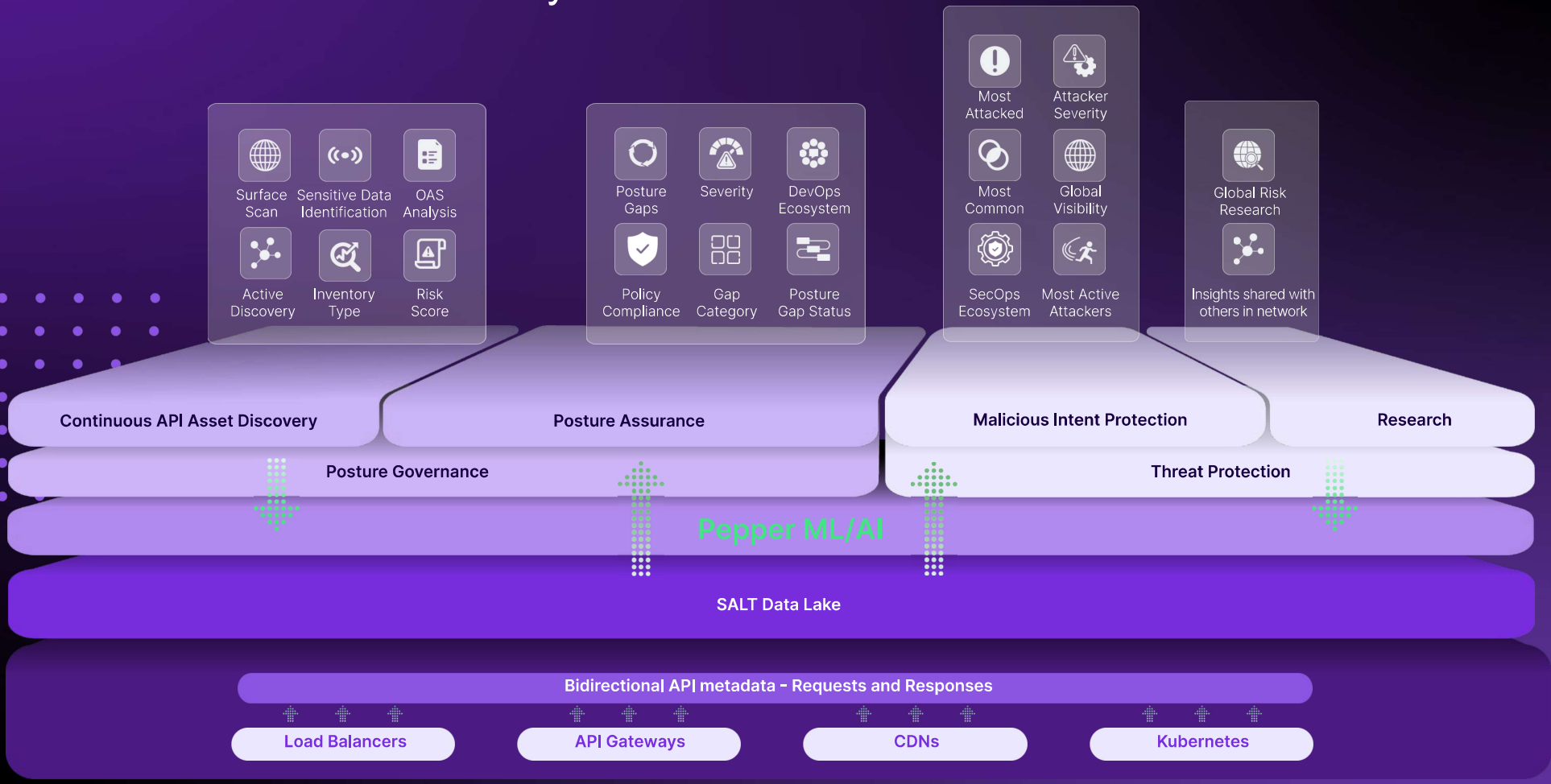
© 2024 Salt Security, Inc. All rights reserved.

Strategy to Reality: API Risk Reduction Journey



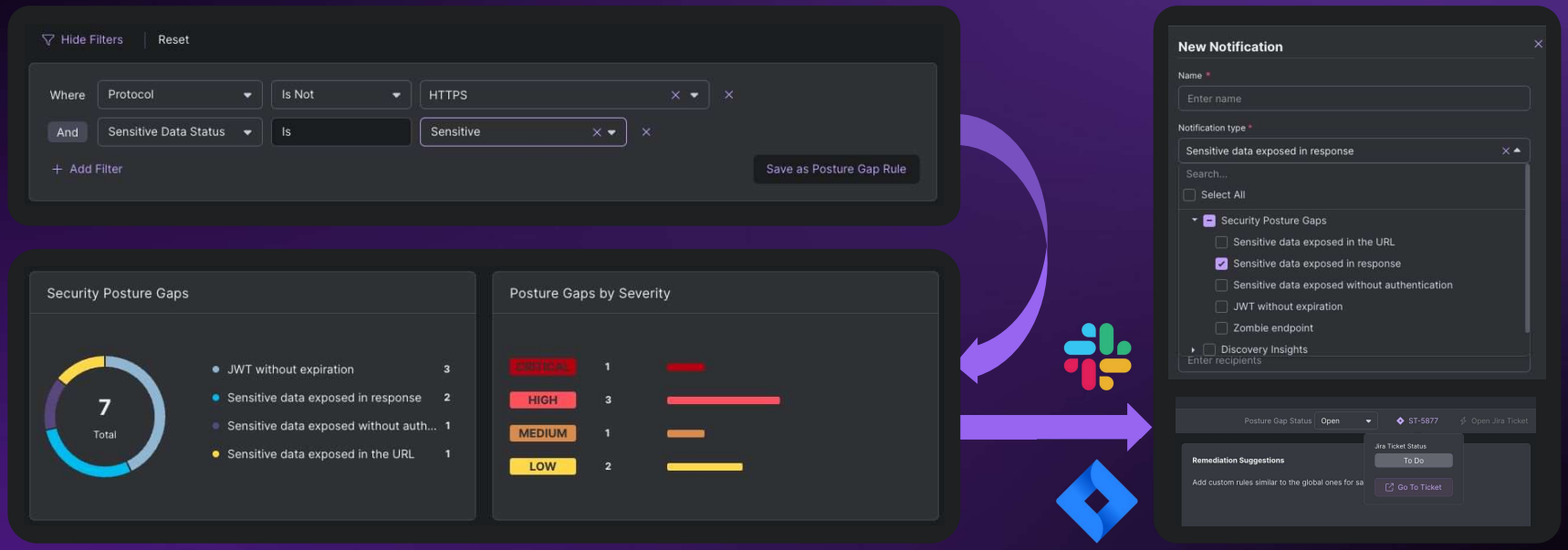
© 2024 Salt Security, Inc. All rights reserved.

Salt's AI-Infused API Security



Salt's API Posture Governance Engine

Salt's API Posture Governance provides organizations with the ability to inventory their API assets, author corporate API posture standards, assess compliance with those standards, and remediate posture gaps through notifications and workflow integrations with corporate systems such as Jira.



© 2024 Salt Security, Inc. All rights reserved.

Posture Standards Examples

- External API response codes should only be 200, 404, 301
- No API requests should contain API keys in querystrings
- Sensitive data is only to be returned from an HTTP Post
- All APIs that ingest payment data must pass through Cloudflare
- All userids must be in UUID format
- All APIs responses must have internal CMDP appid and workload location in response
- All APIs must have a rate limit configured
- All external CAD design document requests must be authenticated and encrypted
- External / outbound API calls should not contain any sensitive data unless it's going to Salesforce

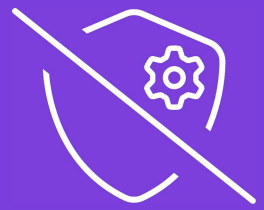
© 2024 Salt Security, Inc. All rights reserved.

Demo Posture Gap management

© 2024 Salt Security, Inc. All rights reserved.

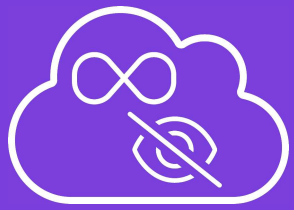
Bottom Line

API risk is an inescapable production reality



Bad API posture governance

Attacks evade web defenses



Ecosystem lacks API awareness

© 2024 Salt Security, Inc. All rights reserved.

Thank you!

Questions?

Please see us at our booth for a more extensive demonstration.

© 2024 Salt Security, Inc. All rights reserved.