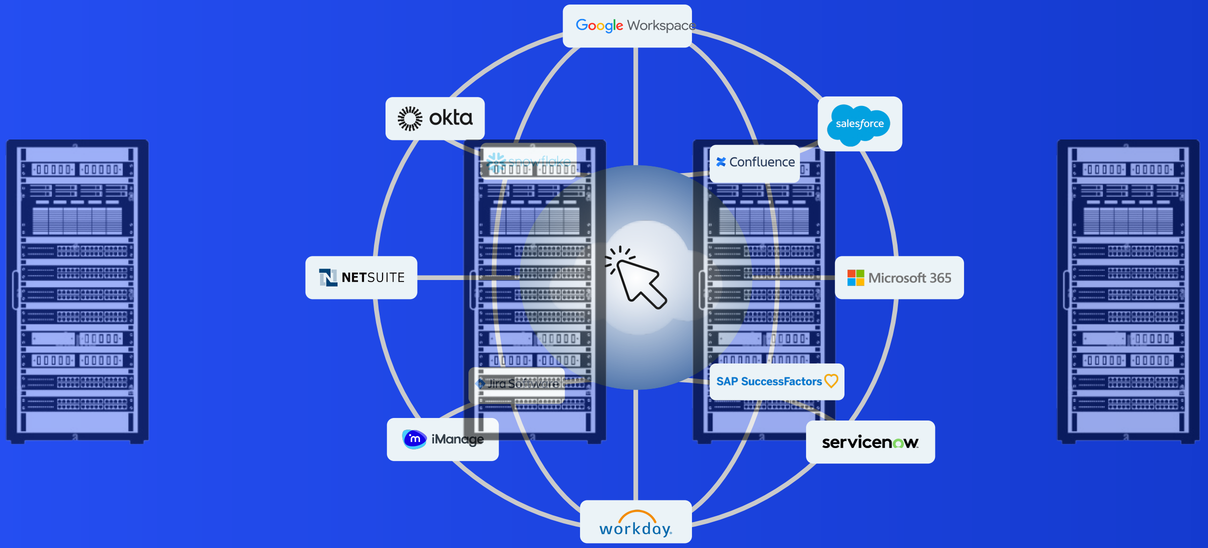
AppOmni

Building Resilient SaaS Security:

Actionable Strategies to Emerging Threats

Dan Devane
VP Sales West

Sensitive data is no longer centralized



80% of sensitive data is stored in cloud applications

1. DevSquad - SaaS Statistics and Trends for 2024

Where Does Your Most Critical Data Live?

In Your Laptop?

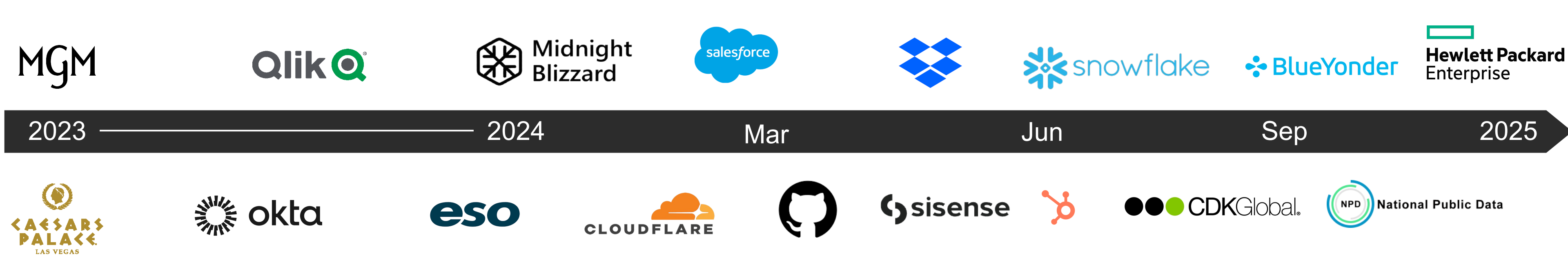
In a Cloud Database?

Or In SaaS Apps?

78% | Organizations storing sensitive data in SaaS[1]

[1] DevSquad - SaaS Statistics and Trends for 2024

More data than ever stolen from SaaS



1B+ individuals impacted by major SaaS breaches in 2024[1]

49% of organizations don't have full visibility into their SaaS applications[2]

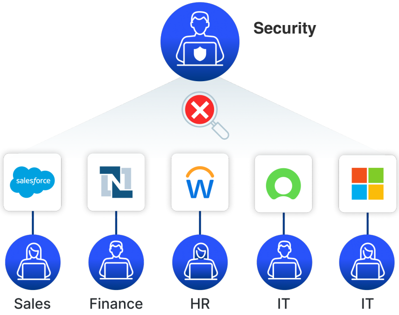
7B+ Records exposed from data breaches in the first half of 2024[3]

1. Anonyme Labs 2024 Data breaches.
2. AppOmni - State of SaaS Security Report
3. Jumpcloud - 2024 Cyber Trends

The Problem With Securing SaaS

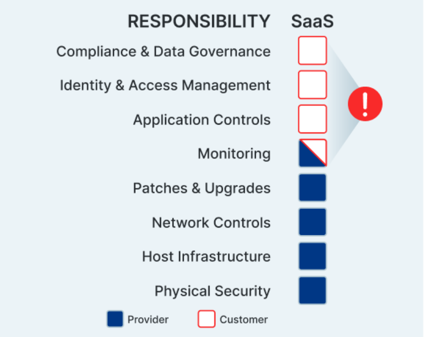
Visibility

Decentralized ownership. Security responsibility without SaaS visibility



Risk

Shared responsibility clouds the true picture of SaaS risk

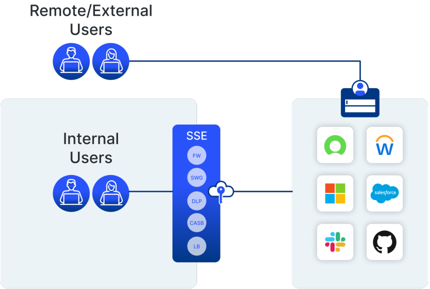


RESPONSIBILITY	SaaS
Compliance & Data Governance	□
Identity & Access Management	□
Application Controls	□
Monitoring	◩
Patches & Upgrades	■
Network Controls	■
Host Infrastructure	■
Physical Security	■

■ Provider □ Customer

Access

SaaS data risks, access, and threats bypass traditional controls

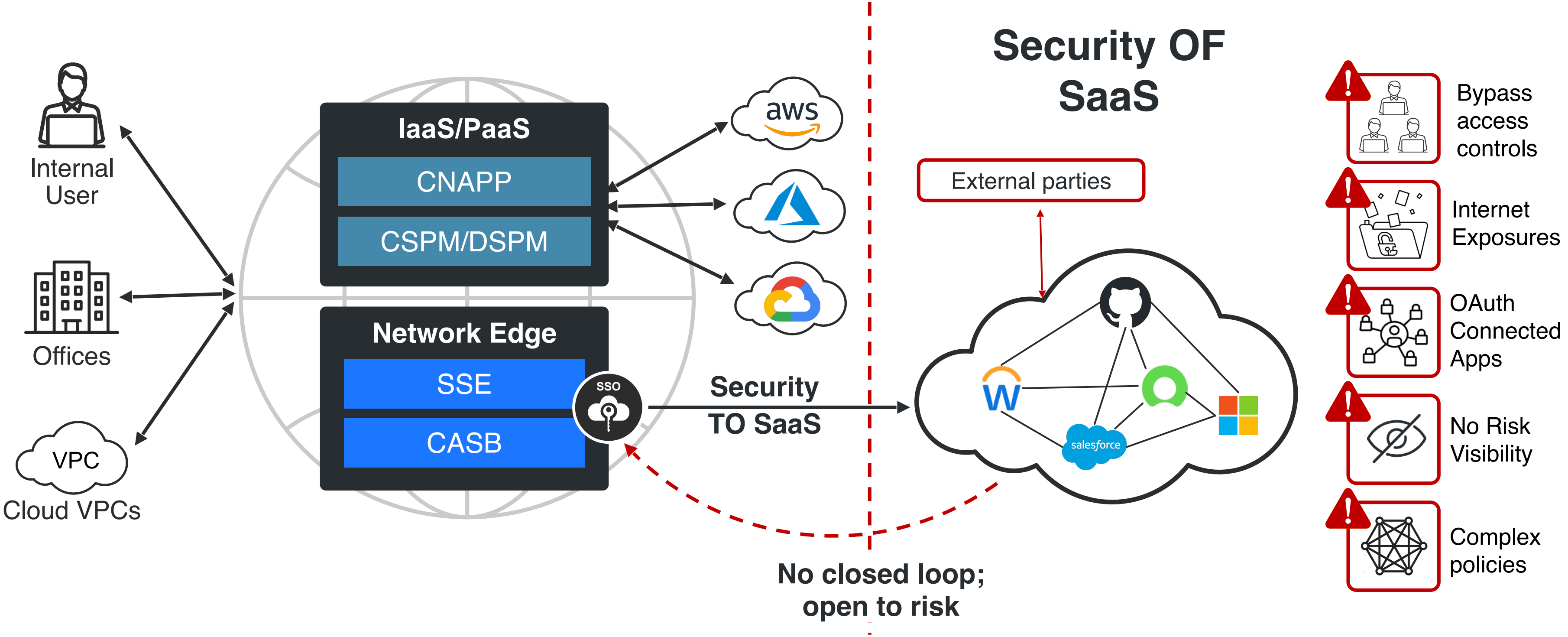


Complexity

Complex environment - different apps, configs, logs & app-to-app connections

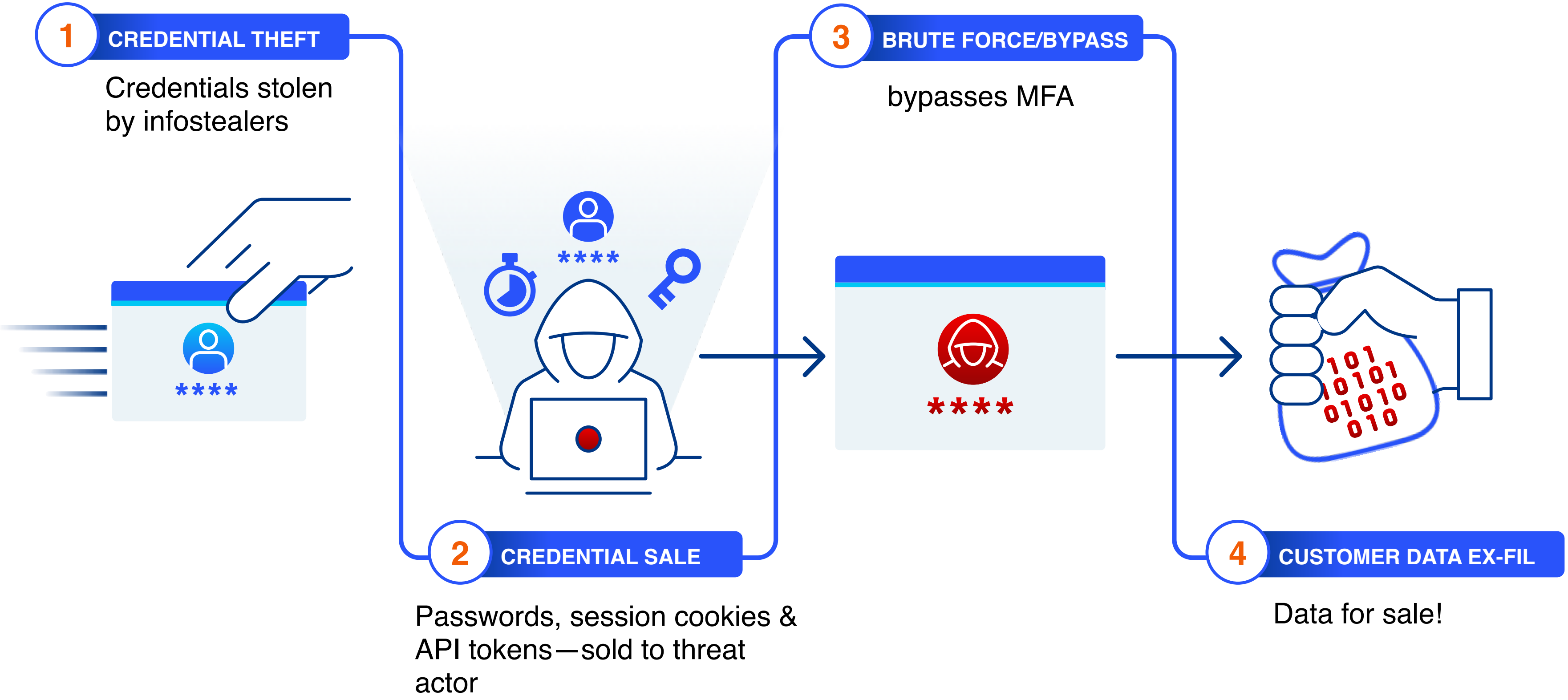
State of Cloud Security

SaaS Risks Outpacing Solutions



AppOmni

What Does a SaaS Breach Look Like?



1 CREDENTIAL THEFT

Credentials stolen
by infostealers

2 CREDENTIAL SALE

Passwords, session cookies &
API tokens—sold to threat
actor

3 BRUTE FORCE/BYPASS

bypasses MFA

4 CUSTOMER DATA EX-FIL

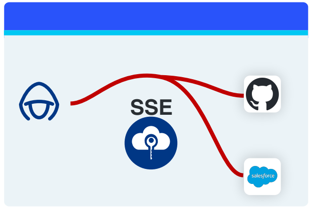
Data for sale!

How AppOmni Prevents SaaS Breaches

1 Brute Force / PW Spray

Multiple Login Attempts

2 BYPASS SSE

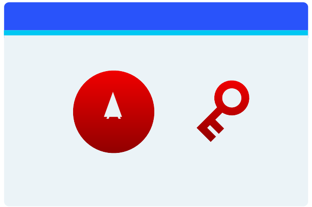


Account is not MFA enabled

User has least privilege

IP restrictions for login

3 NEW ACCESS OR OAUTH

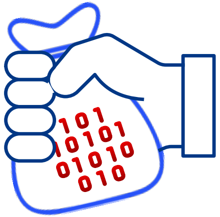


Permitted modifications to OAuth

Login from unknown proxy or tor

New access key

4 EXFIL



Atypical ASN

Mass download

Prevent

Detect

AppOmni

Where SaaS alerting orginiates

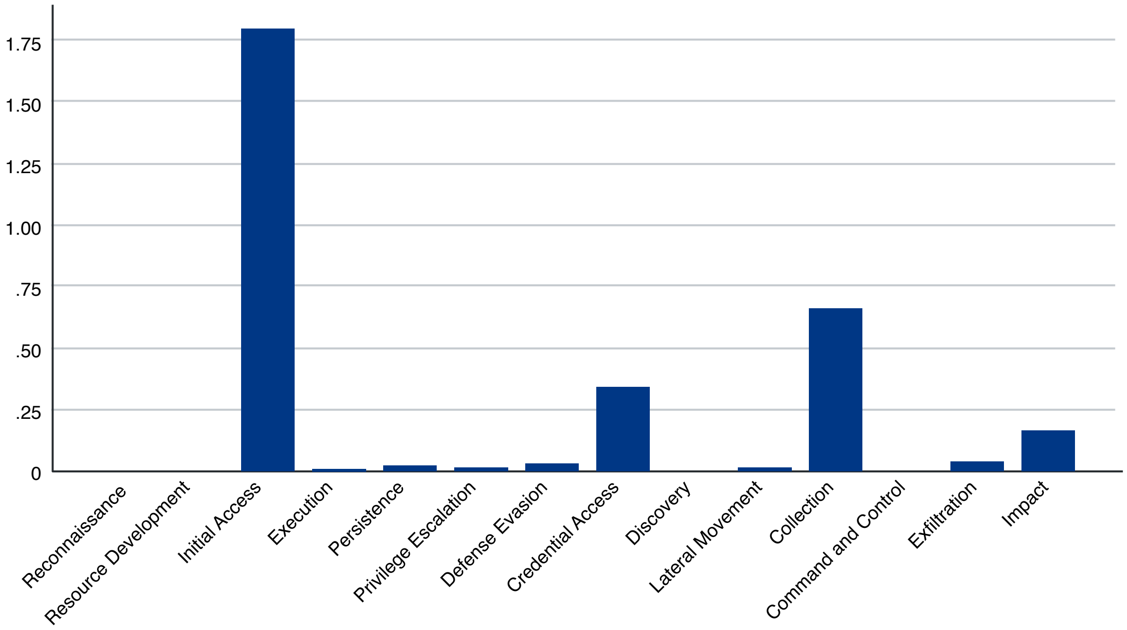
Build a program that protects your attack surface, then identifies activity

~70%

of alerts from initial and credential access

~28%

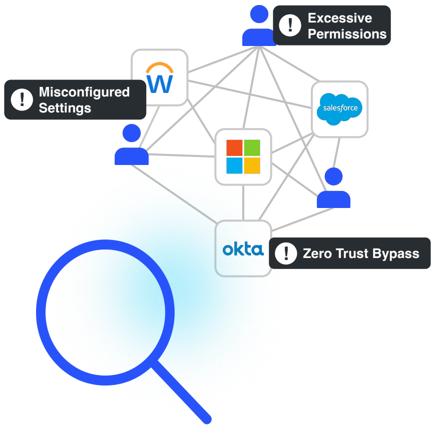
of alerts from collection & exfil



A Modern Approach To Secure SaaS

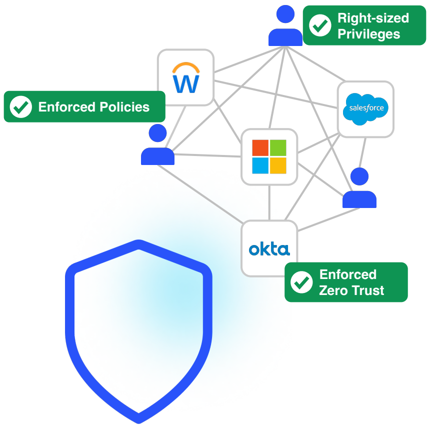
1

Gain Instant Visibility



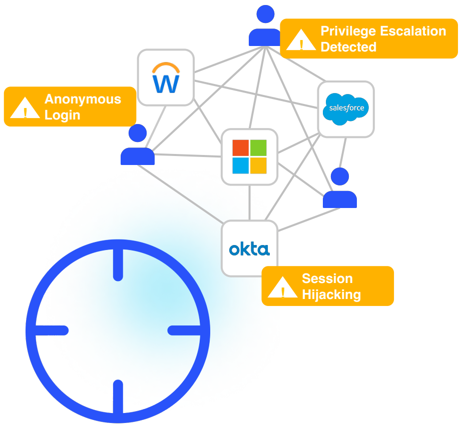
2

Implement a Secure-by-Design Program



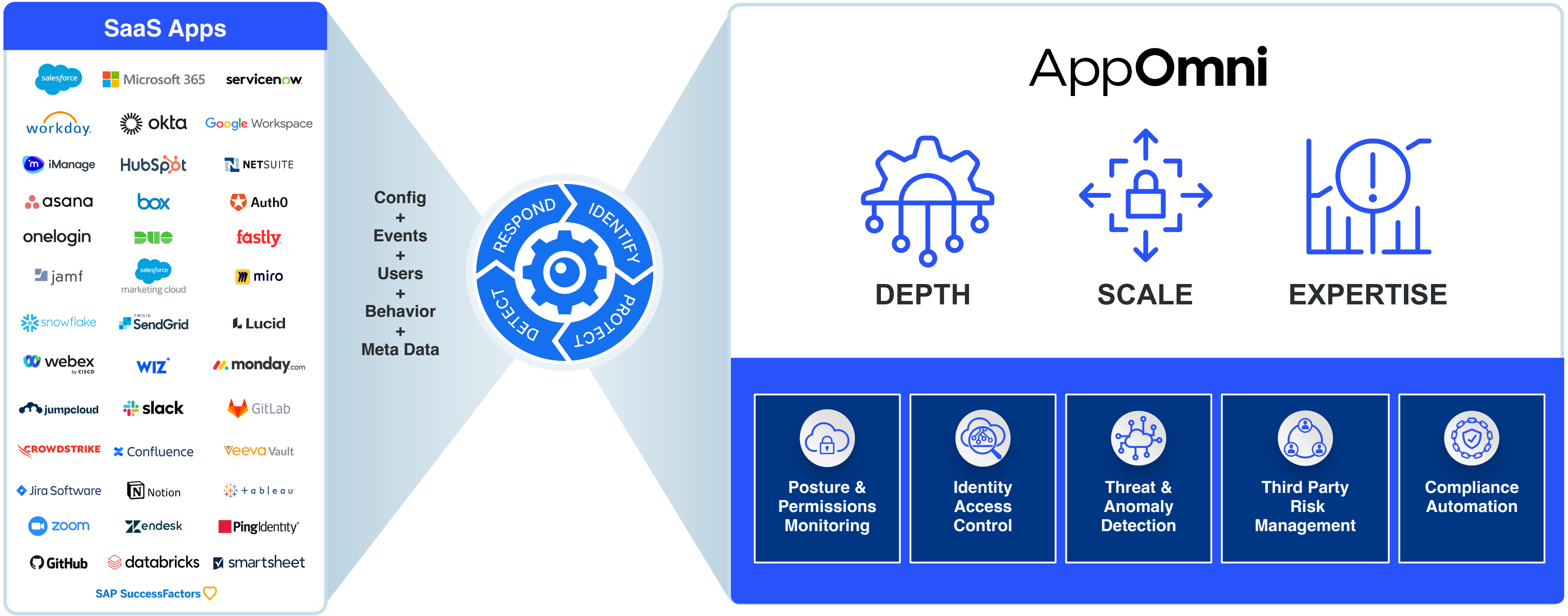
3

Integrate and Respond to SaaS threats



Identify → Protect → Detect → **Respond**

Elevate SaaS Security



SaaS Apps

salesforce, Microsoft 365, servicenow, workday, okta, Google Workspace, iManage, HubSpot, NETSUITE, asana, box, Auth0, onelogin, DUO, fastly, jamf, salesforce marketing cloud, miro, snowflake, Twilio SendGrid, Lucid, webex by cisco, WIZ, monday.com, jumpcloud, slack, GitLab, CROWDSTRIKE, Confluence, Veeva Vault, Jira Software, Notion, tableau, zoom, zendesk, PingIdentity, GitHub, databricks, smartsheet, SAP SuccessFactors

Config
+
Events
+
Users
+
Behavior
+
Meta Data

AppOmni

DEPTH

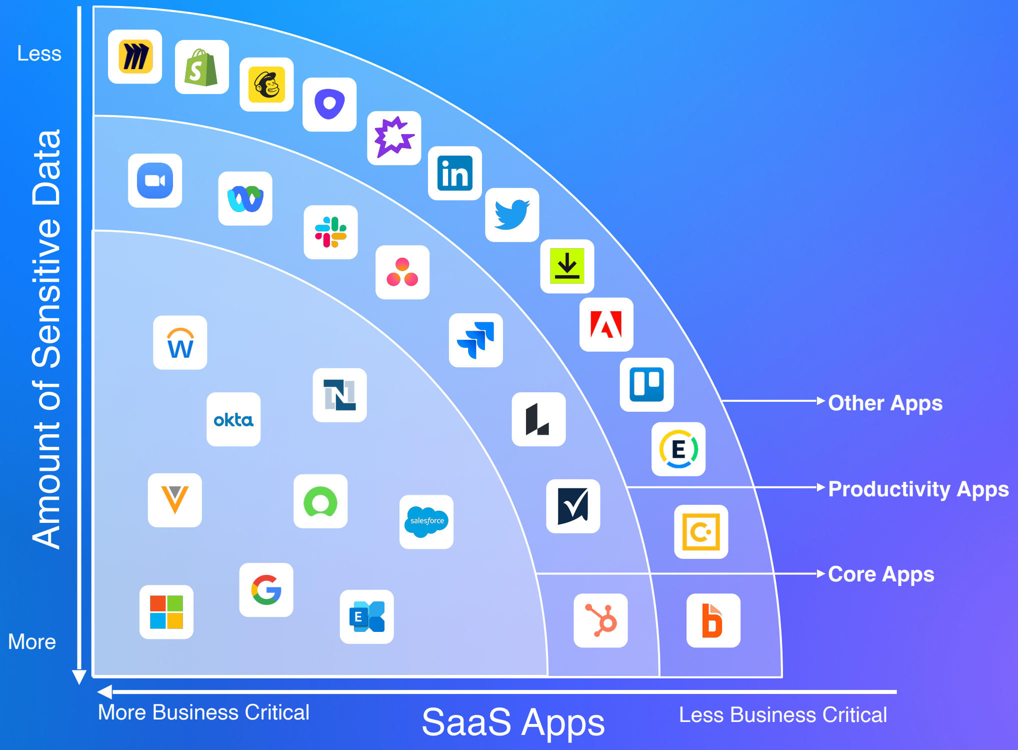
SCALE

EXPERTISE

- Posture & Permissions Monitoring
- Identity Access Control
- Threat & Anomaly Detection
- Third Party Risk Management
- Compliance Automation

Not All SaaS Apps Are Equal

Most sensitive data is stored in a handful of business-critical apps



AppOmni

Trusted by 5 of the Fortune 10

And Securing Saas for 25% of the Fortune 100

> “We’ve been able to accelerate the identification and remediation of key security issues that would have otherwise led to potential data exposures and, potentially, fines or other penalties.”
>
> *- Financial Services Company*

101M+
SaaS Users Protected

260M+
Exposed Data Records Secured

2B+
Events Analyzed Daily

80K+
3rd Party App Installations Found

absa amazon airbnb

AT&T cisco cencora

CVS pharmacy databricks Google

JPMorgan Chase & Co. Johnson & Johnson novo nordisk®

Meta Prudential PEPSICO

Pfizer stripe verizon

NDA

Global Leaders Across Industries Choose AppOmni

Technology

verizon
cisco
Meta
AT&T
ARCTIC WOLF
airbnb
AUTODESK
amazon
stripe
Ping Identity
DRUMMOND
GUIDEWIRE
databricks
IRON MOUNTAIN

Finance/Banking

J.P.Morgan
Capital One
ally
BARCLAYS
absa
citi
APOLLO
TD Bank
Fannie Mae
London Stock Exchange
sallie mae
CAPITAL GROUP
Allstate
NAVY FEDERAL Credit Union
SCALE
LiveOakBank
Standard Bank
St James's Place
EMPOWER RETIREMENT
Insulet Corporation
MOELIS & COMPANY

Healthcare

Pfizer
CVSHealth
cencora
novo nordisk
EmblemHealth
MIRATI THERAPEUTICS
Humana
KAISER PERMANENTE
blue california
BHG BANKERS HEALTHCARE GROUP

Consumer & Others

P&G
IQVIA
urenco The Energy to Succeed
NBA
UNITED AIRLINES
DFPS
TOYOTA CENTRAL R&D LABS
FORRESTER
accenture
Robert Half
American Airlines
reckitt
IATA
SIGILLUM REIPUBLICAE MASSACHUSETTENSIS
DOORDASH
PEPSICO
MORGAN SINDALL GROUP
FANDUEL
MATTEL
AIPAC

Thank You

Learn more at appomni.com

NDA

How Customers Are Using AppOmni To Secure SaaS

CVS pharmacy	novo nordisk	cisco
Pain Point: No security, visibility, or monitoring for strategic SaaS applications **Need:** Establish an end-to-end, and SaaS Security Program to protect critical SaaS applications. **Incumbents:** Existing SSE deployment	**Pain Point:** Growing complexity of SaaS **Need:** Greater control and visibility into SaaS configs, posture, user behavior; GxP, FDA compliance **Incumbents:** ZScaler, PANW, Microsoft - offered only CASB solution	**Pain Point:** Unable to detect SaaS data exposure **Need:** Comprehensive SSPM solution to detect SaaS data exposure and mis-configuration risks **Incumbents:** Basic SSPM - missed significant data exposure

NDA

University of Cincinnati Reduces Data Exposure, Gains Greater Visibility with AppOmni

University of CINCINNATI

KEY RESULTS

- Reduced data exposure of sensitive data, including vaccination records Salesforce Community Portal
- Visibility across 13 Salesforce instances previously unmonitored
- Quick implementation and collaborative support without the need of team expansion

> ❝ *There were roughly 68,000 users who had access to 900,000 vaccination records we did not know about.* ❞ - CISO to CIO after POV

ENVIRONMENT

salesforce servicenow okta DUO snowflake CROWDSTRIKE

PROBLEM

- **Data exposure** risks presents awareness and monitoring problem in complex SFDC, environments
- **Blind spots** in critical SaaS apps prevented awareness of potential vulnerabilities

WHY APPOMNI

- **Data exposure prevention** protect critical student data and data access
- **SaaS expertise** ongoing support for limited staff across University system
- **Scale** configuration management, streamline across multiple app instances

What other teams have to say

“

Previously, manual reviews took weeks, but with AppOmni's help, we’ve shortened this process to a few hours, significantly enhancing our efficiency and response time.

- Gerald Beuchelt
CISO, Sprinklr Inc.

“

The depth of the coverage that AppOmni provides for SaaS apps was the differentiating feature on why we selected AppOmni for our data security practice.

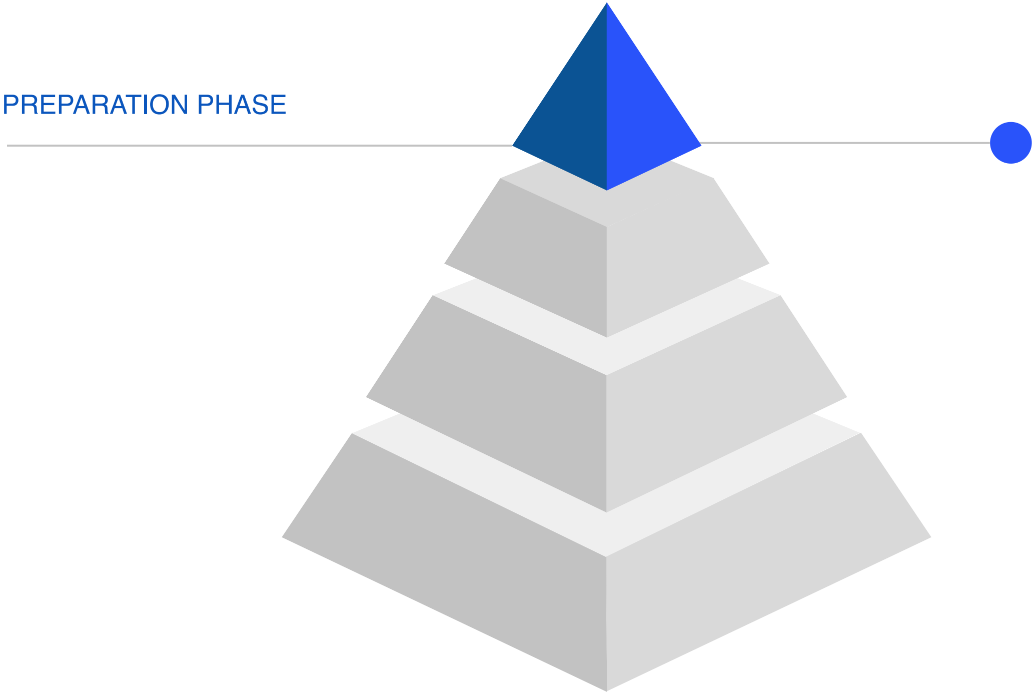
- Arthur Hedge
President, Castle Ventures

“

AppOmni will help you solve the risks you never knew about that could result in a breach or data exposure. The AppOmni platform solves this in a painless, efficient, and programmatic lifecycle way.

- Mark Butler
Advisory CISO, Trace3

SaaS **Program Implementation**



PREPARATION PHASE

1. **Deployment Planning:**

   Review of existing deployment, current security controls and perceived gaps to define a risk-rated operationalization plan.

1. **Identify Primary Stakeholders:**

   Identify stakeholders from each LoB, and also from each org.

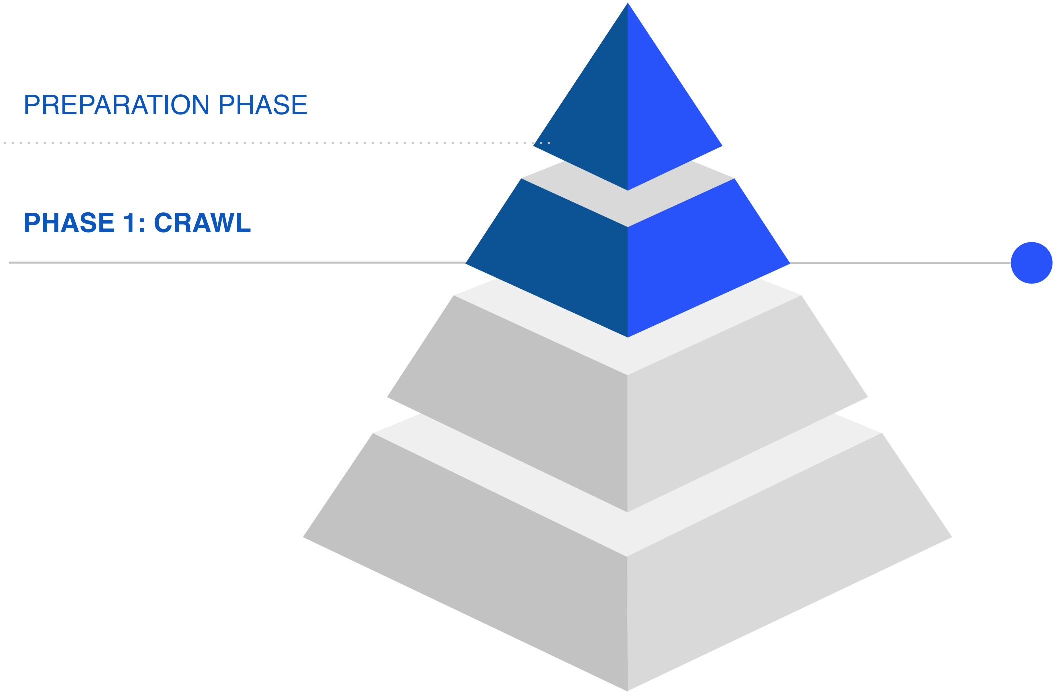
1. **Project Goals and Success Criterias**

   Identify, and document key project goals and success criterias.

1. **Project timelines and milestones**

   Agree on, and document project timelines, deliverables and milestones.

SaaS **Program Implementation**



PHASE 1: CRAWL

1. **Engage key SaaS Security Stakeholders:**

   Engage with key stakeholders, such as SaaS application owners to ensure representatives from different departments and levels of the organization have visibility.

1. **Onboard Your SaaS applications:**

   Onboard your SaaS applications into AppOmni for central SaaS security monitoring and visibility.

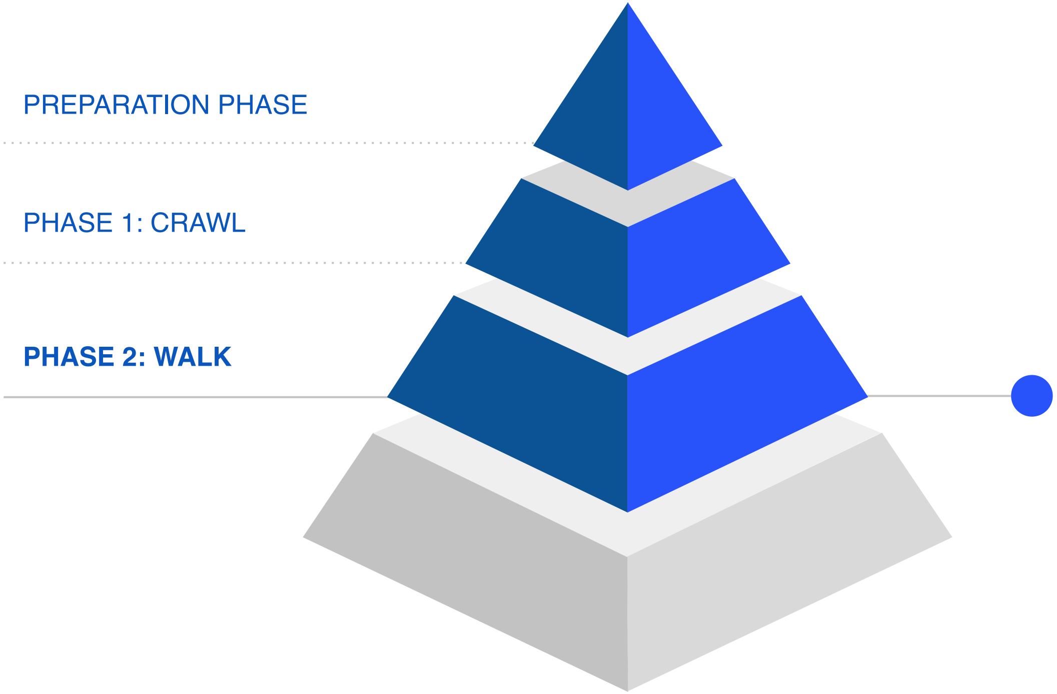
1. **Deploy AppOmni out-of-the-box SaaS security best practices or map to Royal Mai's custom minimum control framework:**

   Leverage AppOmni out-of-the-box SaaS security best practices to quickly identify security gaps, and to evaluate the organization's security posture against industry best practices & standards.

1. **Review initial findings / current state, and remediate or tune SaaS security policies:**

   Assess and review the initial findings, and develop (tune) baseline policies based on cybersecurity maturity model and initial scan findings i.e. highest risk SaaS Apps. Remediate critical findings.

SaaS **Program Implementation**



PHASE 2: WALK

1. **Establish corporate security policies & procedures:**

   Review & update initial AppOmni policies as/if needed. Define, and implement AppOmni operational procedures, roles + responsibilities, and communicate to all stakeholders involved.

1. **Project milestones, goals, awareness and training:**

   Define realistic SaaS security milestones based on initial findings. Develop specific, measurable, achievable, relevant, and time-bound project goals. Provide the initial education and training to all involved employees.

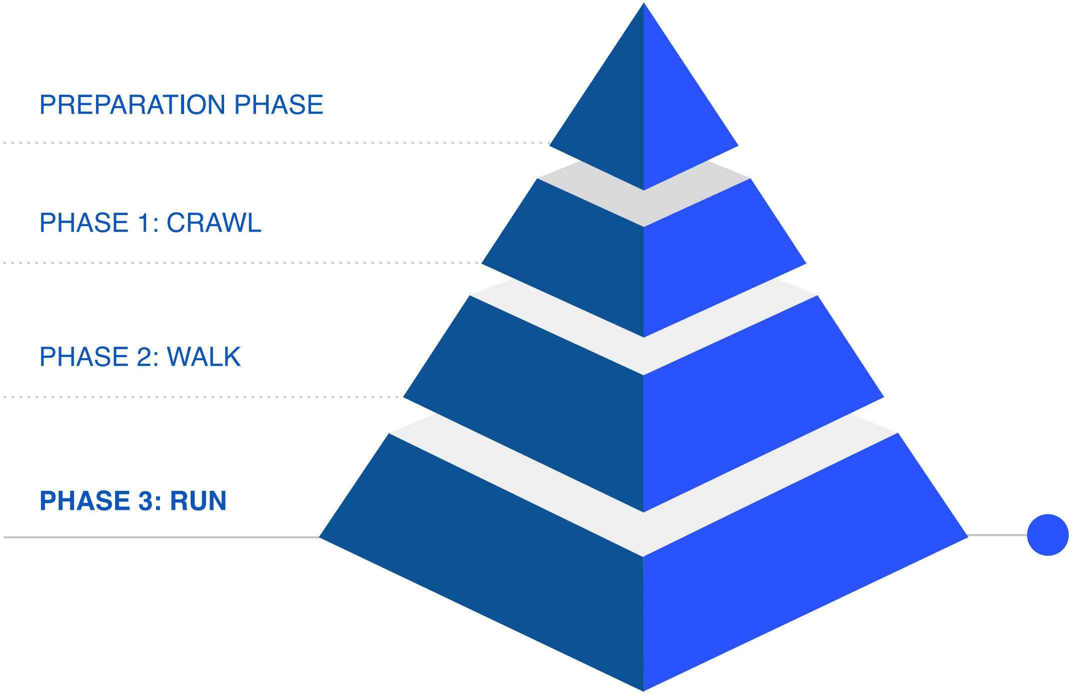
1. **Corporate workflows and integrations:**

   Review, and define SaaS security corporate workflows and integrations.

1. **Metrics & reporting criteria:**

   Identify KPIs & define reporting framework.

SaaS **Program Implementation**



AppOmni Onboarding & Implementation Plan Here

PHASE 3: RUN

1. **Implement, and adopt end-to-end SaaS security workflows and integrations:**

   Ensure AppOmni findings can be consumed and reviewed via existing SaaS security workflows and tools.

1. **Metrics & reporting:**

   Ensure AppOmni findings and metrics can be tracked via the required reporting framework.

1. **Continuous policy reviews, adjustments and testing:**

   Ongoing policy & findings assessments to identify risks & ensure the SaaS security program remains aligned with business strategy & objectives.

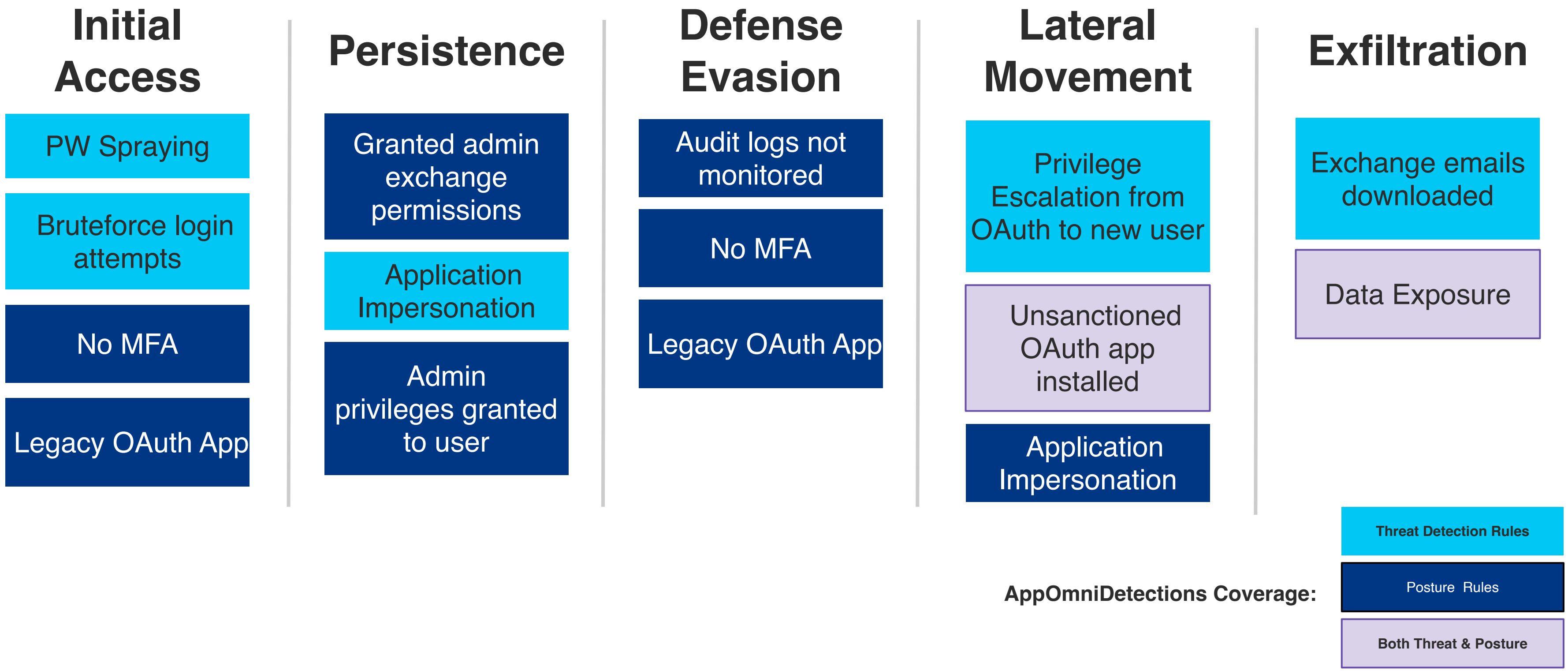
1. **Continuous education and awareness program:**

   Provide ongoing education & awareness training to all employees involved.

Midnight Blizzard Tactics, Techniques and Procedures

Initial Access	Persistence	Defense Evasion	Lateral Movement	Exfiltration
PW Spraying	Granted admin exchange permissions	Audit logs not monitored	Privilege Escalation from OAuth to new user	Exchange emails downloaded
Bruteforce login attempts	Application Impersonation	No MFA	Unsanctioned OAuth app installed	Data Exposure
No MFA	Admin privileges granted to user	Legacy OAuth App	Application Impersonation	
Legacy OAuth App				

Midnight Blizzard TTPs



Initial Access

- PW Spraying
- Bruteforce login attempts
- No MFA
- Legacy OAuth App

Persistence

- Granted admin exchange permissions
- Application Impersonation
- Admin privileges granted to user

Defense Evasion

- Audit logs not monitored
- No MFA
- Legacy OAuth App

Lateral Movement

- Privilege Escalation from OAuth to new user
- Unsanctioned OAuth app installed
- Application Impersonation

Exfiltration

- Exchange emails downloaded
- Data Exposure

AppOmniDetections Coverage:

- Threat Detection Rules
- Posture Rules
- Both Threat & Posture