



Xcitium CNAPP / XDR

Cloud Security Essentials
Application & Infra Posture Management
Runtime Workload Protection

April 2024

What problem are we solving?

- Cloud Migration is accelerating, Cloud Footprints are expanding,
- Increasing adoption of BYOD and remote work
- Organizations are going -> Multi-Cloud Hybrid-IT
- Attack surface getting bigger & more complex, making organizations porous and vulnerable
- More and more cyber attacks are cloud borne or have a cloud component

Legacy Tools and Simple Perimeter Defenses cannot thwart Modern-Day
Cloud Borne Advanced Attacks (i.e. xzUtils / SSH vuln.)

Adoption of a **CLOUD SECURITY PLATFORM**
that centralizes all cloud security controls management is a must

What are the requirements?

- Advanced attacks require advanced defenses such as Zero Trust Security for Zero Day Attacks
- Support modern workloads (**Kubernetes**) and traditional workloads (**Virtual Machines, Bare-metal**)
- Security needs to be portable across
 - **Public Clouds** (AWS, Azure, GCP)
 - **Private Clouds** (RedHat OpenShift, VMWare Tanzu, Nutanix, Mirantis)
- **DevSecOps** - Shift left and protect apps from code to production
- **GRC** - Continuous compliance
- **Cloud Security Essentials** - Basic Cloud Security Hygiene

Xcitium CNAPP delivers on all of this

Features Provided



3

Workload Security (CWPP)

Kubernetes &
Host Runtime
Security

Application
Behaviour Modeling

Container Registry
Scanning

Container & VMs
Forensics

Automatic Zero
Trust Policies

1

Application Security (ASPM)

Static Application
Security Testing
(SAST)

Software
Composition
Analysis (SCA)

Dynamic Application
Security Testing
(DAST)

2

Infrastructure Security (CSPM)

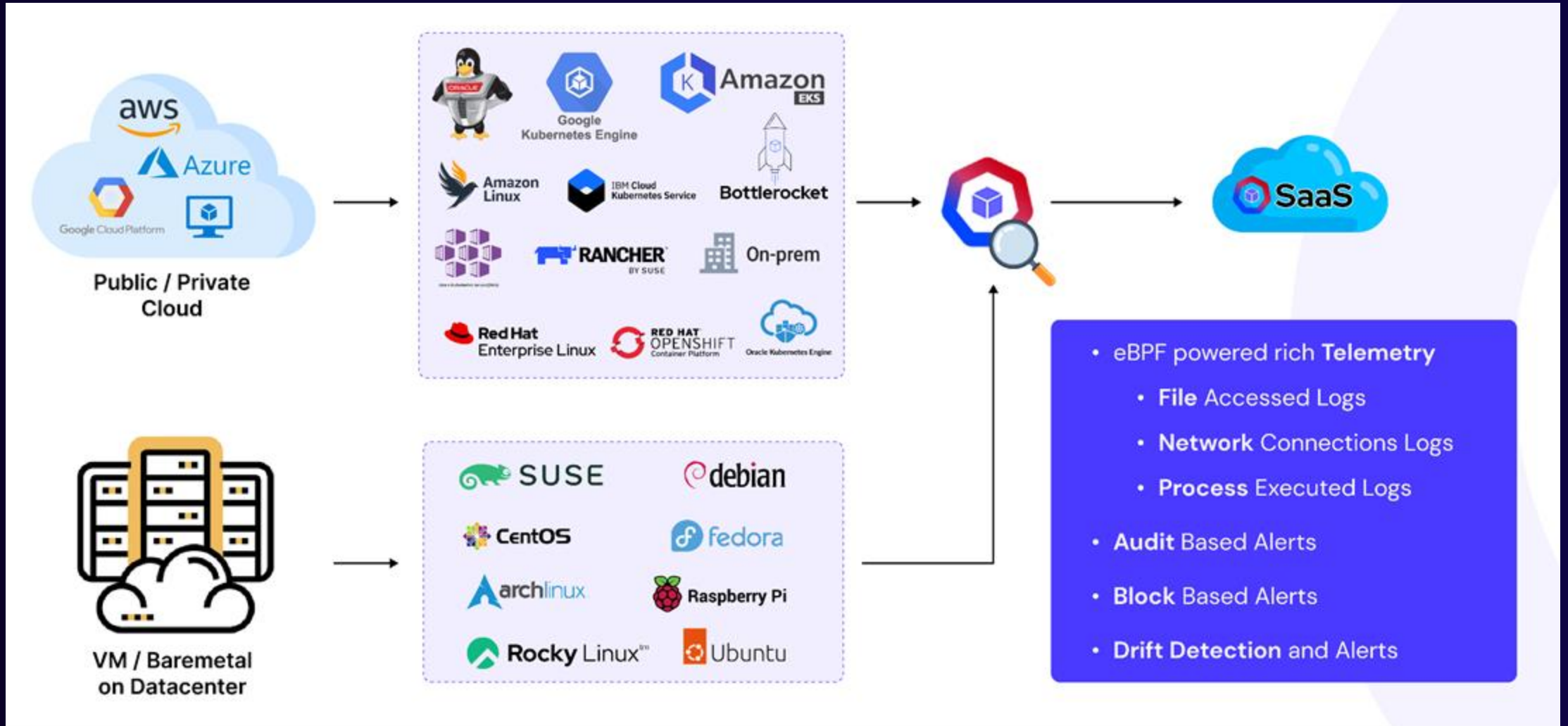
Public & Private
Cloud Assets
Scanning

CI/CD
Management &
Compliance

Continuous
Diagnostics &
Mitigation (CDM)

Xcitium Zero Trust CNAPP
Cloud Security Essentials & Basic Risk
Analysis

We Secure: Multi-Cloud, Air-Gapped, On-Prem



CSE – Cloud Security Essentials

Features/Functions

Connect with read-only API. No agents.

Gain visibility to your cloud environment and understand your footprint

Enumerate, sort and classify all of your assets

Identify malware, vulnerabilities, misconfigurations, over privileged accounts, network & storage exposures, unprotected secrets or lack of encryption

Prioritize high risk items for remediation

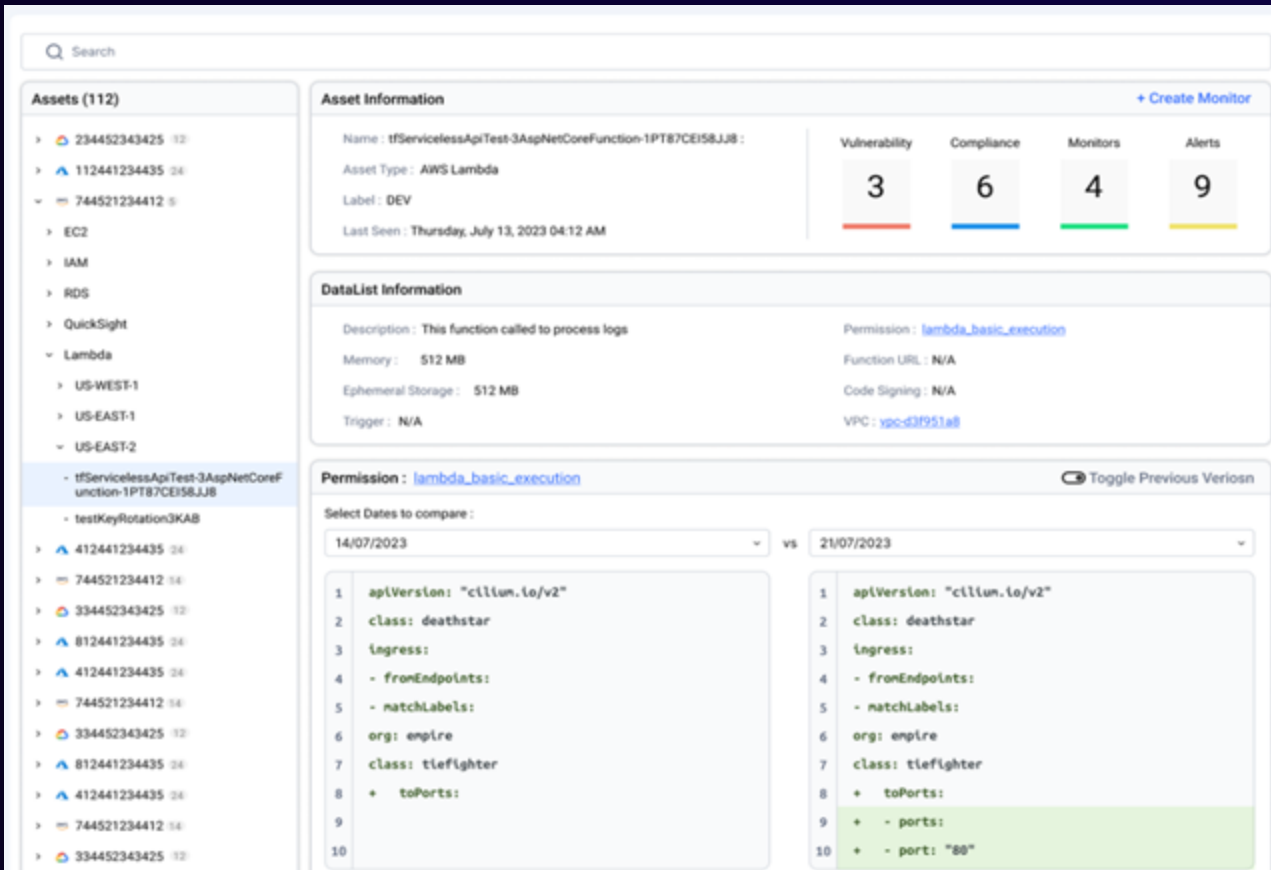
Key Differentiators

Multi-cloud – ability to assess all of your cloud instances from the most popular public cloud providers

Agentless from the same unified Xcitium platform.

Establish foundational security hygiene and prepare for compliance

Flexibility & Expandability



ASPM - Application Security Posture Management

Features/Functions

Analyzes source code for potential security vulnerabilities without running application

Simulate attack scenarios at running app to find vulnerabilities

Analyzes 3rd party dependencies/lib in open source

Check IaC scan based on Terraform and Dockerfile

Key Differentiators

Leverage wide range of tools for SCA, SAST, DAST, IaC with a single pane of glass view

Prioritize vulnerabilities based on exposure at runtime, exploitability, environmental factors and others..



Flexibility & Expandability

SAST [\[Get in touch with AccuKnox Team for assist\]](#)

- Integrate Sonarqube with your code repository through a JWT session based token from AccuKnox SaaS
 - Step1: Create workflow action for GitHub with token
 - Step2: Workflow will be triggered for every PR raised
 - Step3: Push result to AccuKnox SaaS [optional]
- Filter Data Source as **Sonarqube** and it will help to identify all the coding errors, common CVE etc. associated with your repository

```
1  - name: Push report to CSPM panel
2  run: |
3    curl --location --request POST 'https://s((env.CSPM_URL))/api/v1/artifact/tenant_id=2(( env.TENANT_ID ))&data_type=TfKnox_no_x3=false'
4    --header 'Authorization: Bearer S(( env.CSPM_TOKEN ))' --form 'file=@./results.json'
```

2

3

Asset details:

Asset Name: Vulnerability id

Location: Software

Type: Thursday, August 3, 2023 10:32 PM

Last Seen: Region

0 Tickets **0** Groups **0** Audit Files **0** Monitors

Vulnerabilities

Error High Low Medium

CSPM - Cloud Security Posture Management

Features/Functions

Agentless scan

Continuous Compliance Coverage

GRC Roadmap and Security Frameworks

CIS, HIPAA, PCI, SOC2, ISO27001 etc.

See the delta in Configuration Drift and get alerted

Get Assistive Remediation and a single pane of management

Key Differentiators

Continuous Monitoring

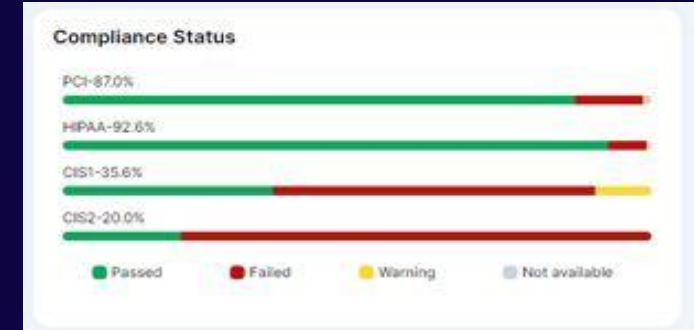
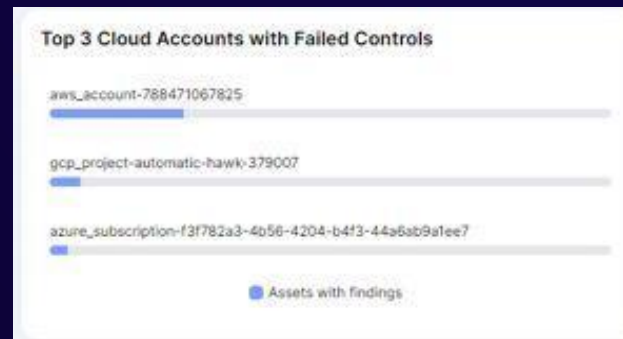
1-click Remediation assistance

Configuration Drift View

Continuous updating Compliance Dashboard

Comprehensive Reporting

Customizable Dashboard & Reporting

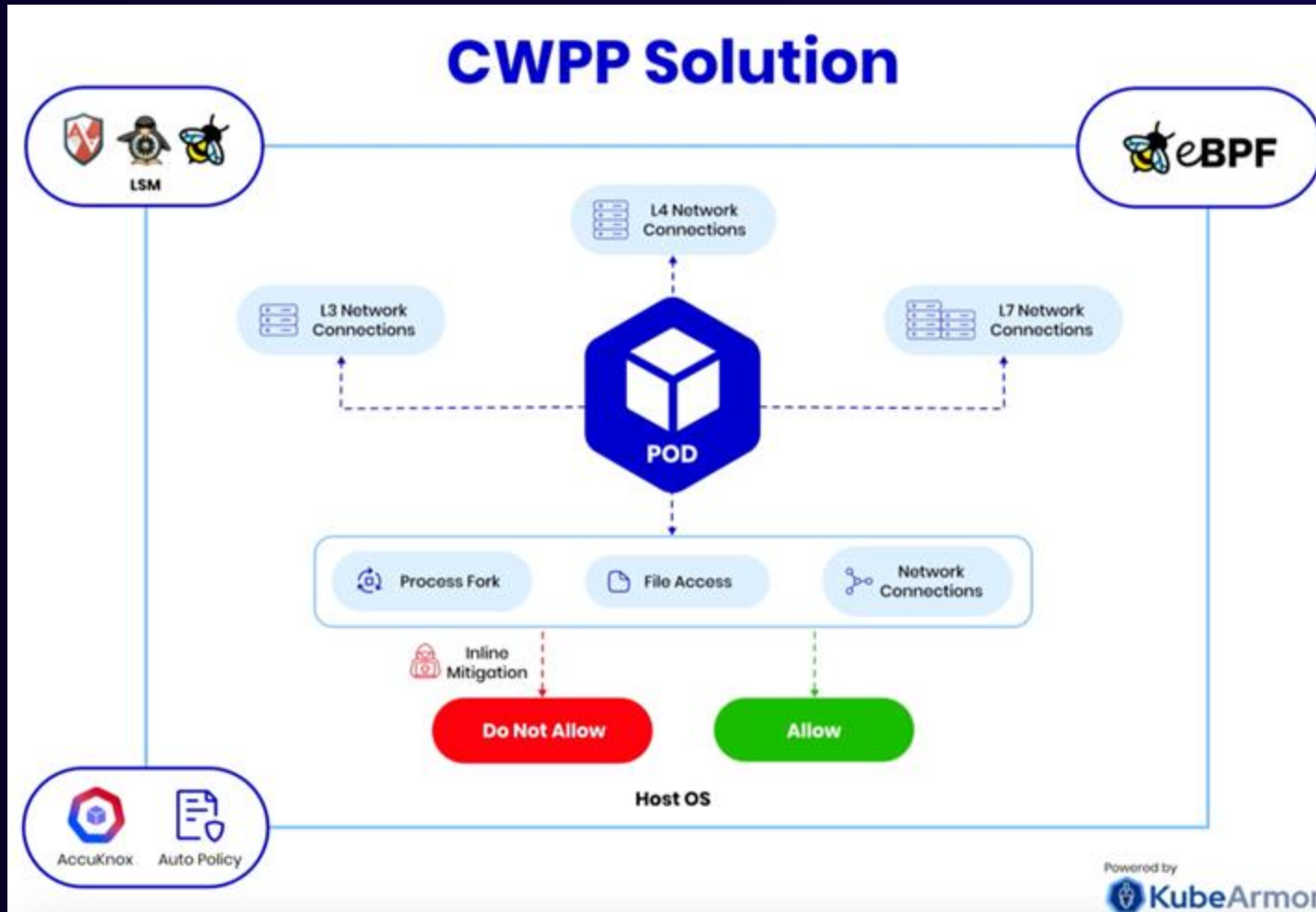


Executive Compliance Summary

Cloud Accounts	JAN	FEB	Trend
aws_788471067825	84	83	
f3f782a3-4b56-4204-b4f3-44a6ab9a1ee7	84	87	
5fec40c9-801e-4987-94c0-e7c241	0	86	NA
automatic-hawk-379007	89	89	
accuknox-cnapp	0	88	NA



CWPP - Cloud Workload Protection Platform



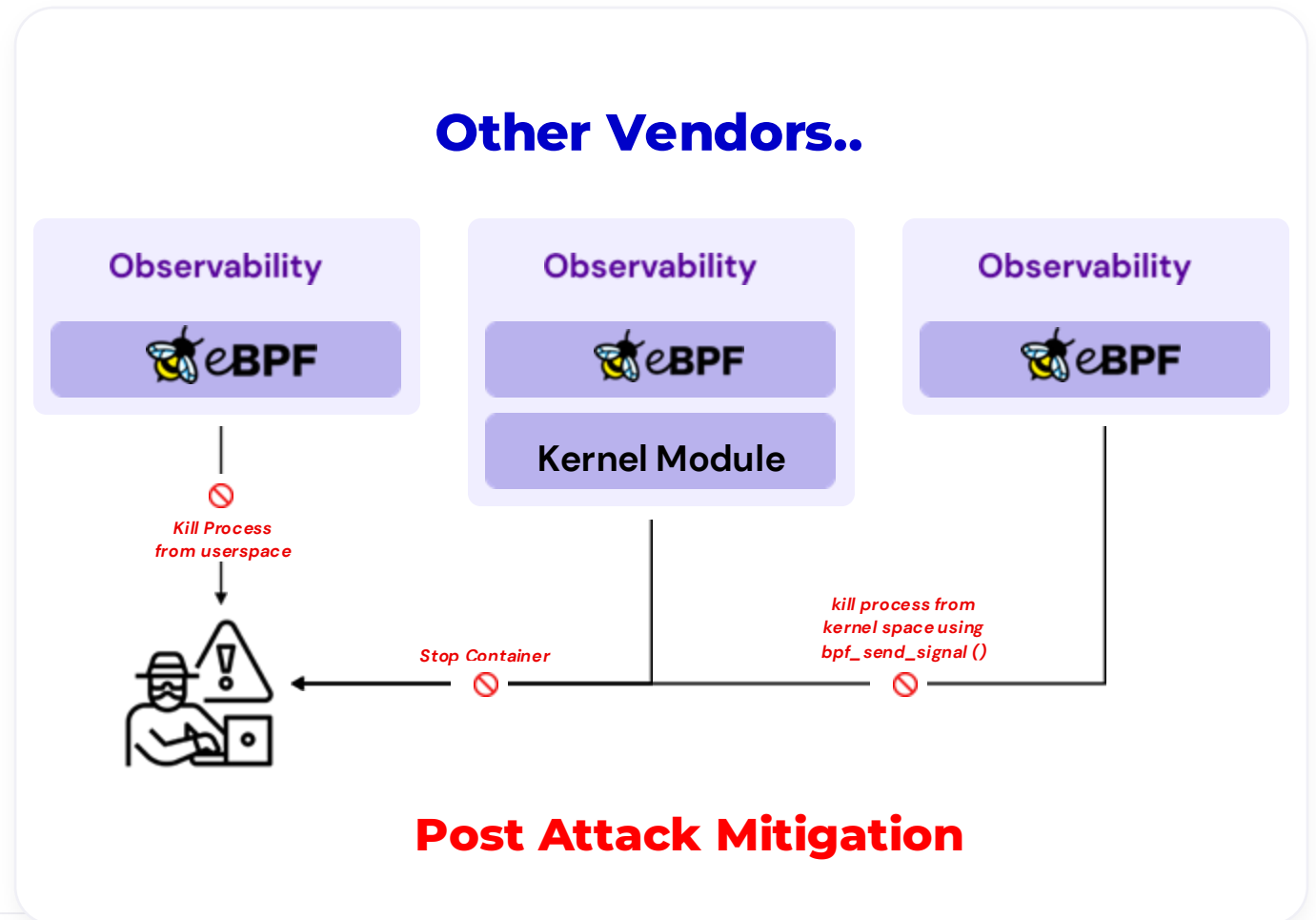
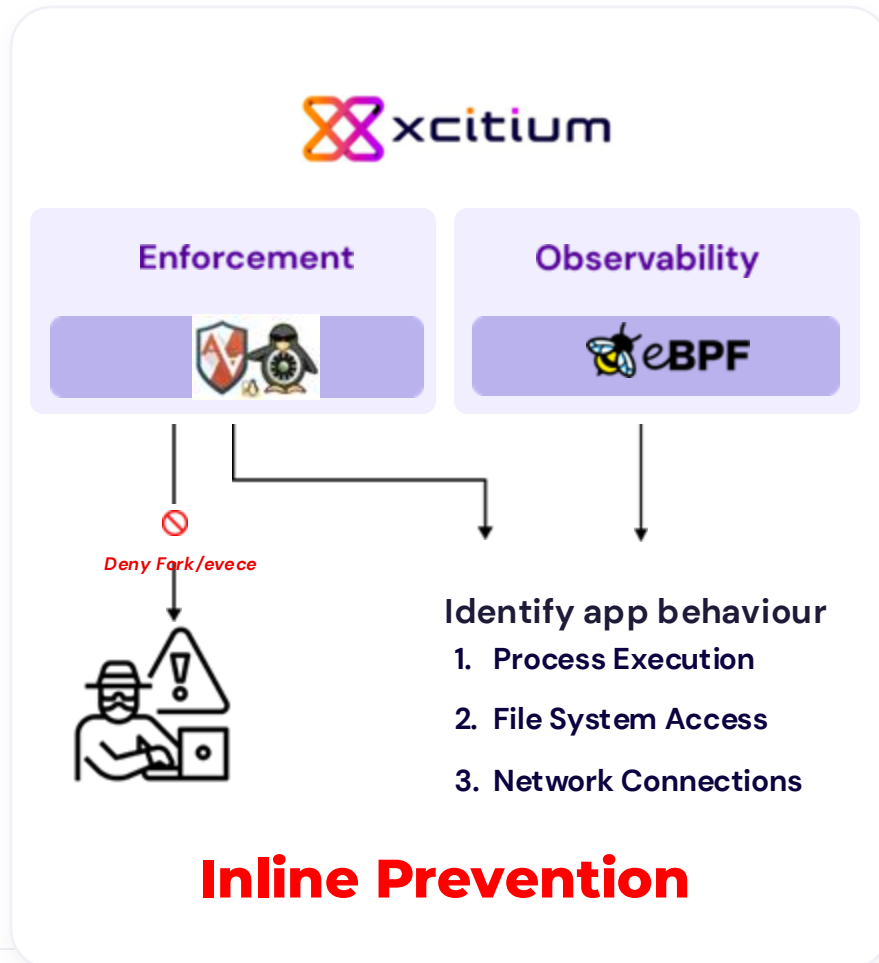
- Application Behavior Modeling
- Application & Workload Hardening
- Network Segmentation
- Automatic Zero Trust Policies
- Multi-Cloud & Multi-Cluster Support



Our Unique Differentiation



We can “**Observe**” > “Automatically Generate “**Policies**” > “**Enforce**”



KIEM - Kubernetes Identity & Entitlement Management

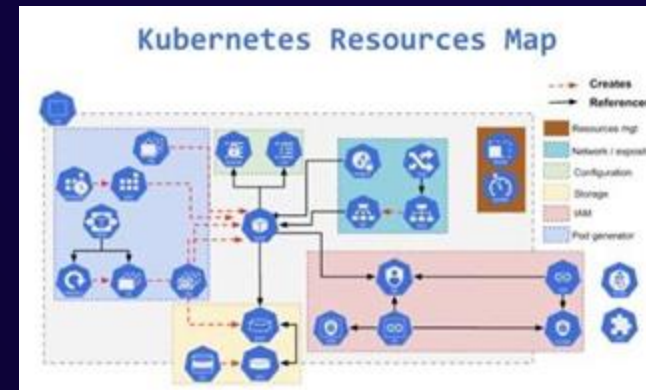
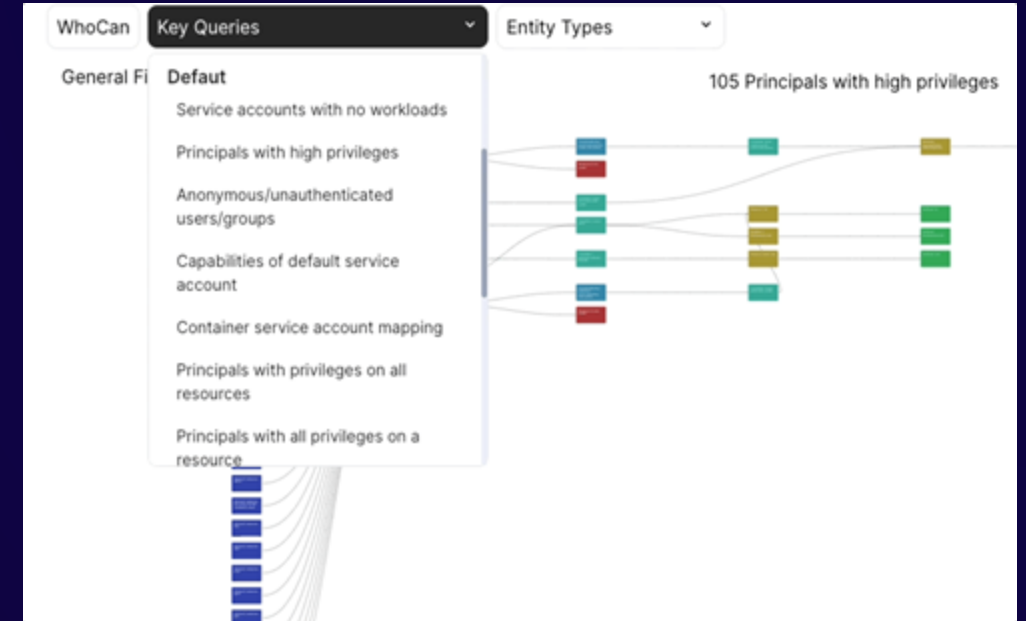
Agentless scan of Kubernetes Identities

Misconfigurations

Unravel hidden patterns between entities and resources through graph visualization.

AccuKnox KIEM provides a predefined set of critical queries related to entitlements such as

Principals with Extra & High Privileges
Service Accounts with no Workloads
Principals with access to all resources
Principals with all permissions



How we Secure Software DevOps Life Cycle?

CODE

- Static Code Analysis
- Software Composition Analysis
- Secret Scanning



IMAGE

- Container Image Scanning
- Risk Prioritization
- Sensitive Assets
- Container Compliance



CLOUD

- Cloud Account Misconfiguration
- CI/CD Pipeline Security
- CIS Benchmarking

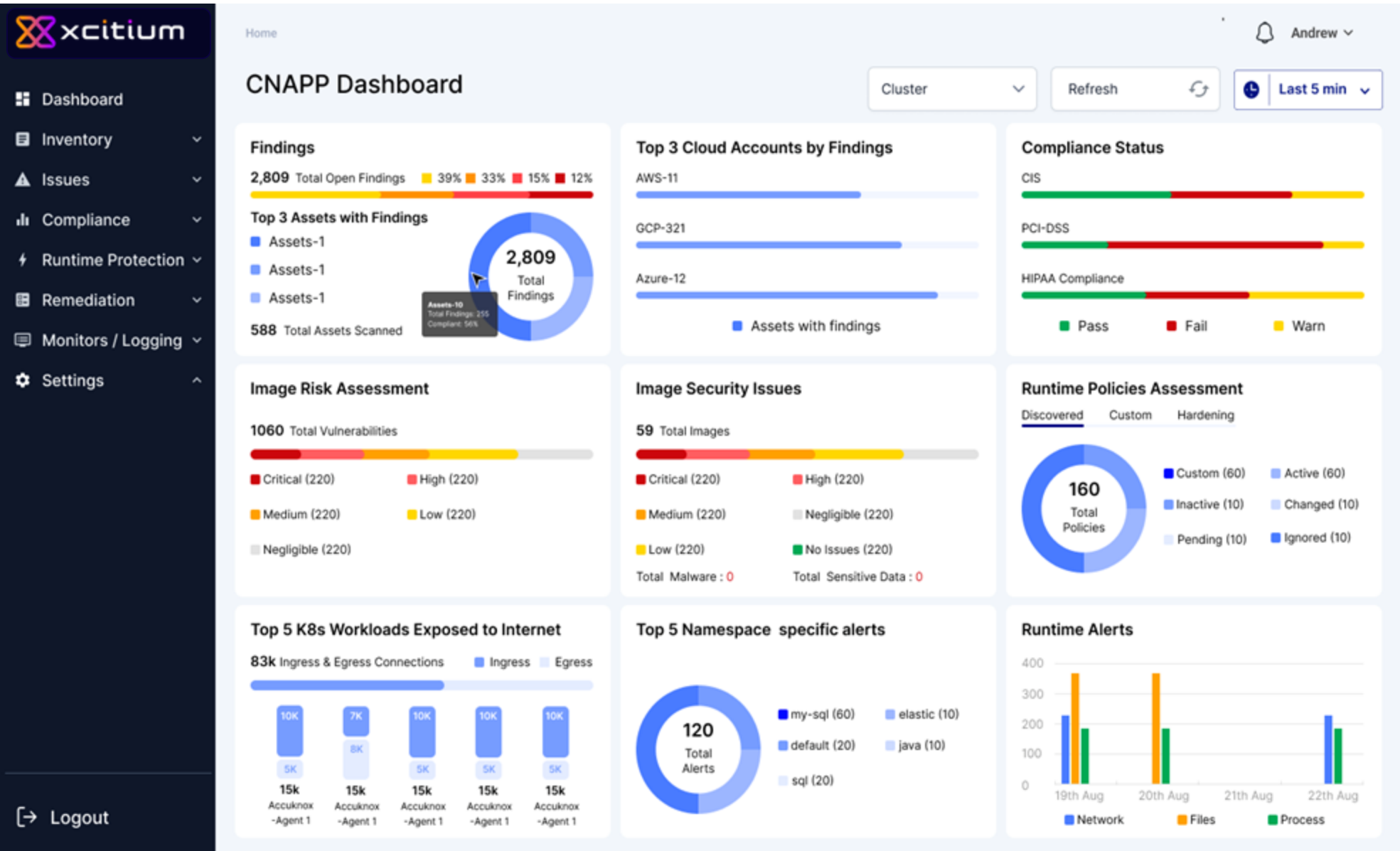


RUNTIME

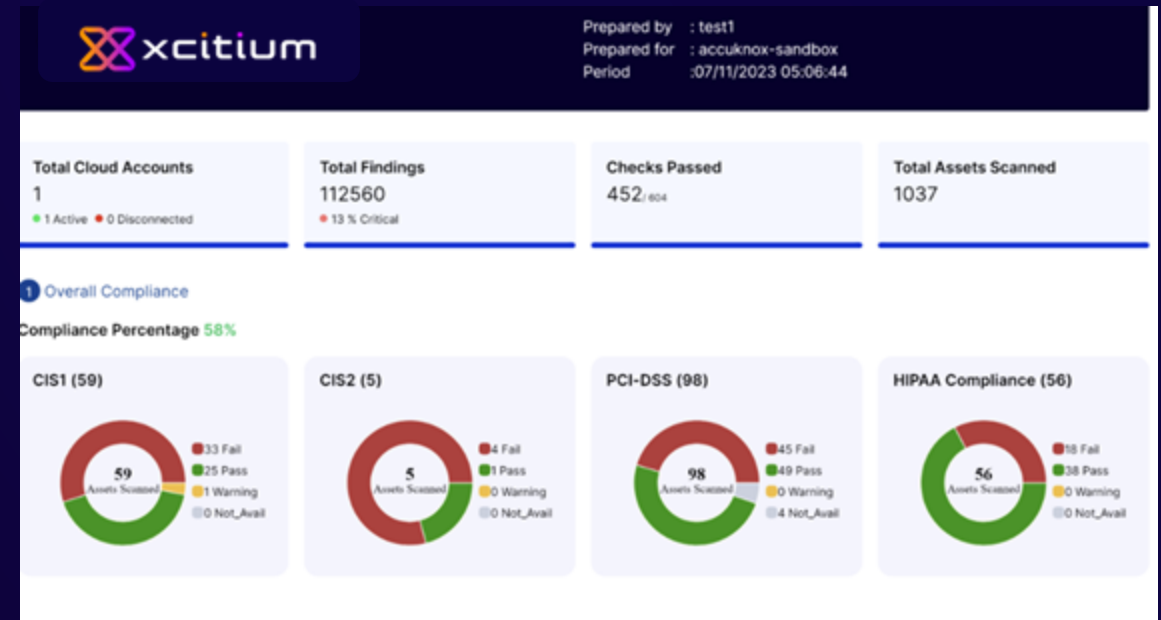
- App behavior analysis
- Workload hardening
- Zero Trust Policy
- File Integrity Monitoring
- Network Segmentation



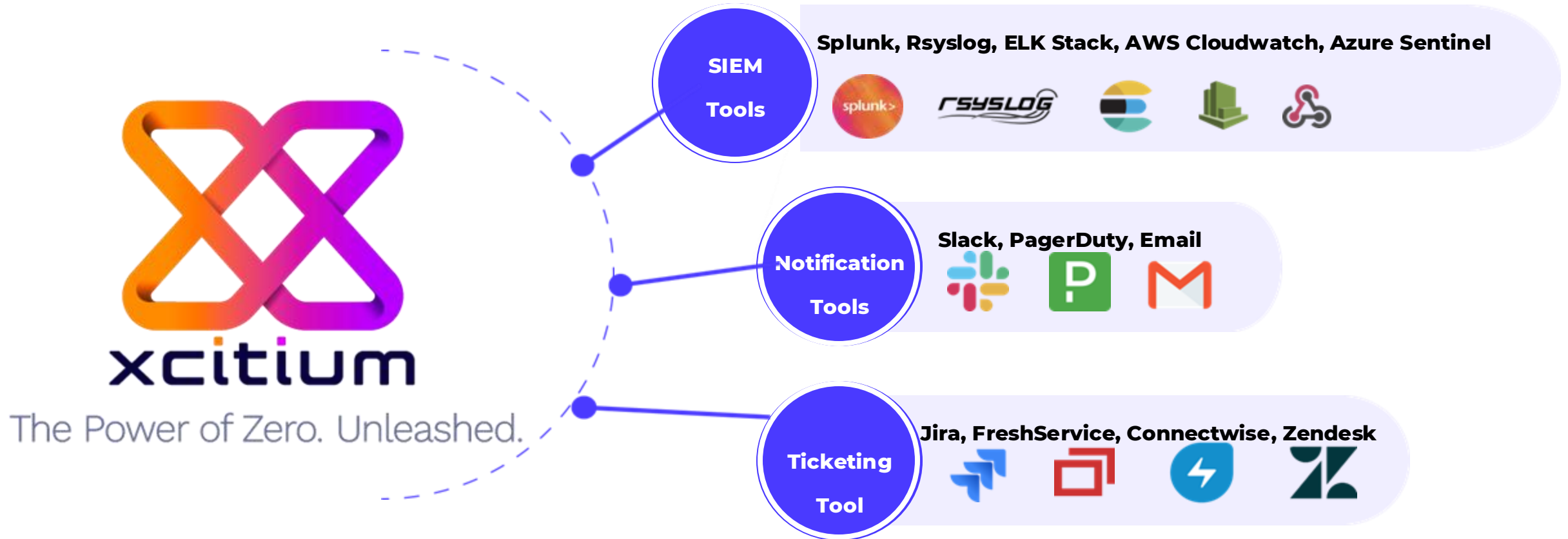
Comprehensive Dashboards



Comprehensive Reports



Integrations we support



The *only* Unified Zero Trust Security Solution for Endpoints and Cloud
on a single platform and policy framework