Xcitium CNAPP / XDR

Cloud Security Essentials
Application & Infra Posture Management
Runtime Workload Protection

April 2024

xcitium

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

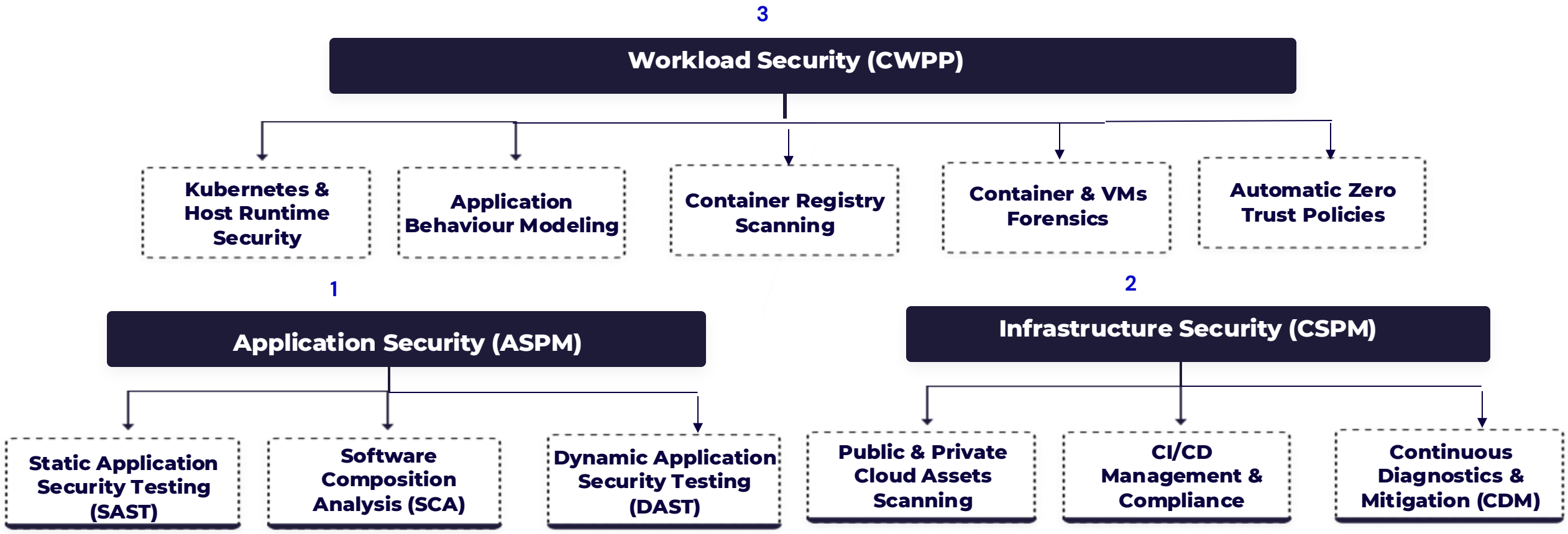
xcitium

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

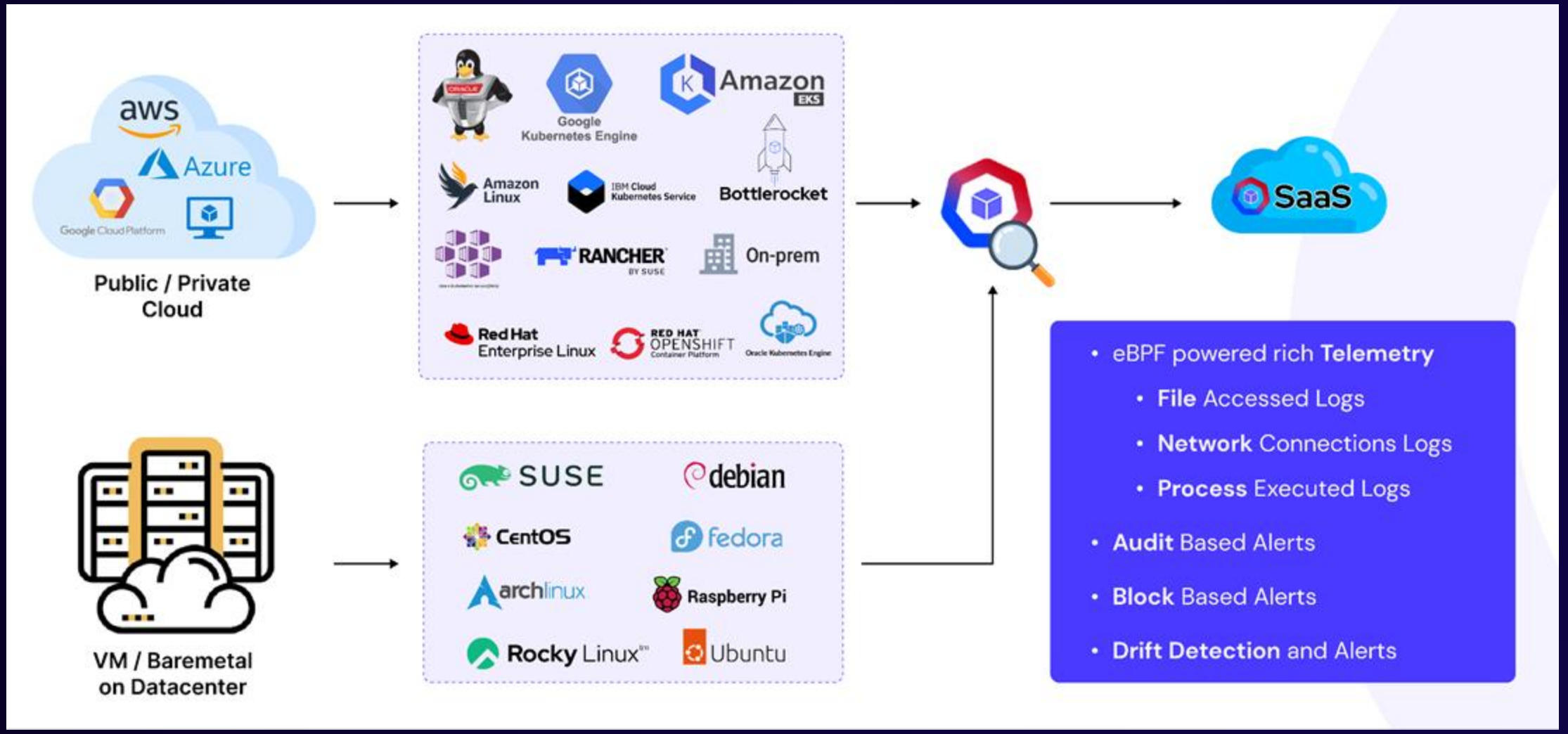
Xcitium CNAPP delivers on all of this

Features Provided



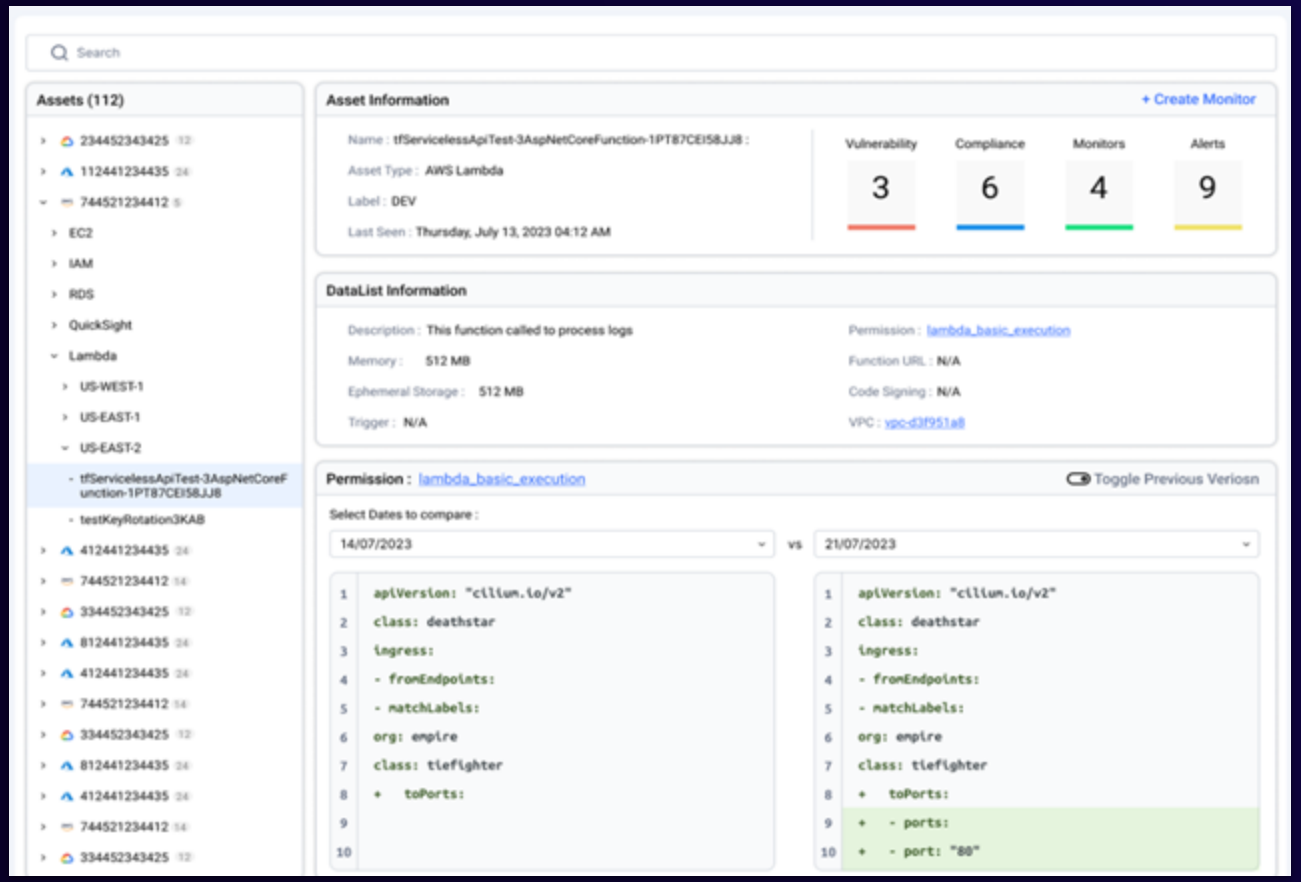
Xcitium Zero Trust CNAPP
Cloud Security Essentials & Basic Risk Analysis

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



xcitium

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

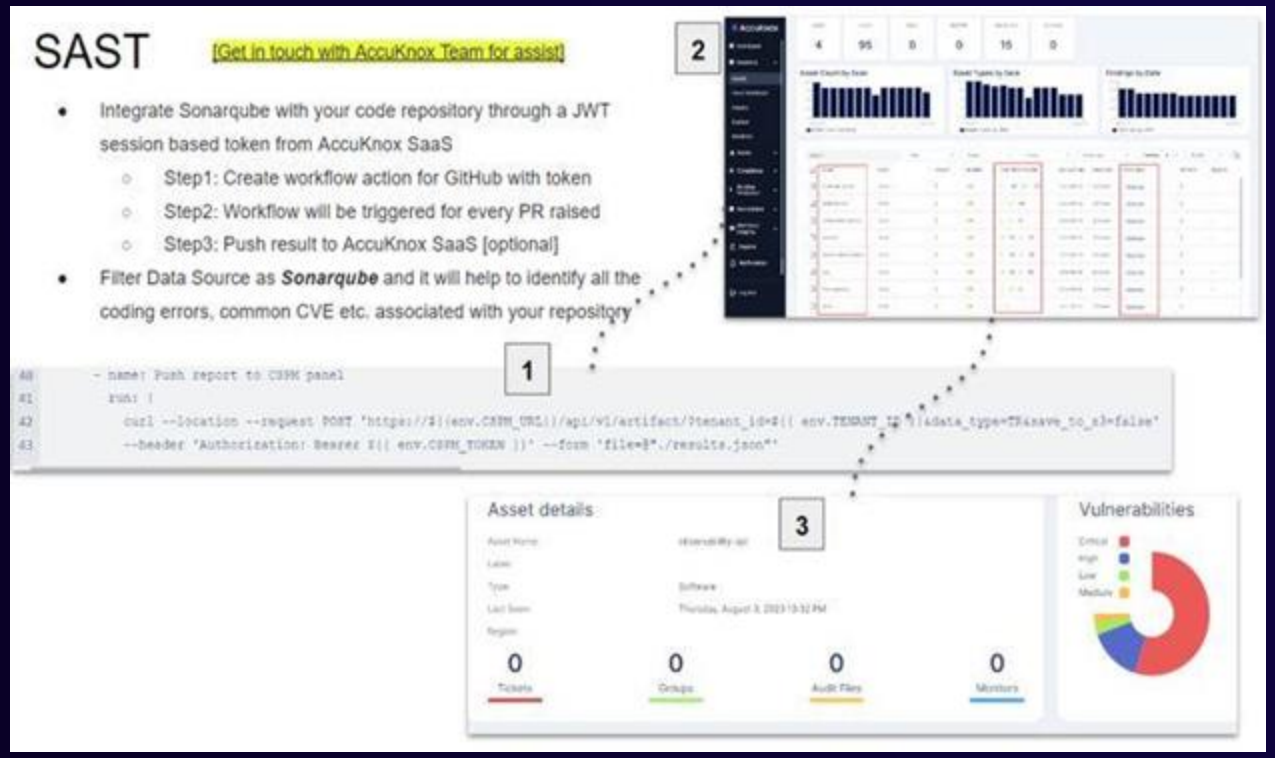
Agentless from the same unified Xcitium platform.

Establish foundational security hygiene and prepare for compliance

Flexibility & Expandability

xcitium

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

xcitium

CSPM - Cloud Security Posture Management

Features/Functions

Agentless scan

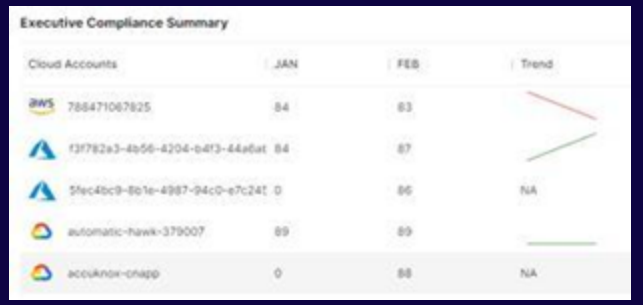
Continuous Compliance Coverage

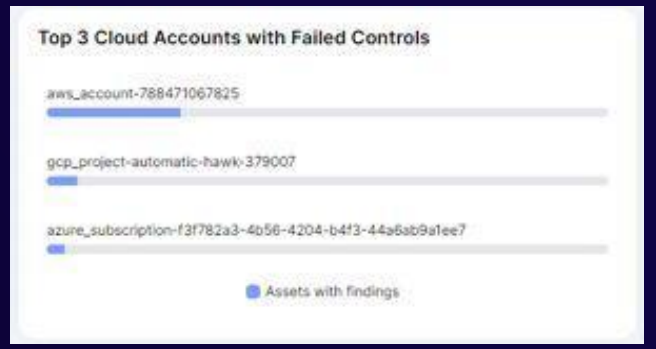
GRC Roadmap and Security Frameworks

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

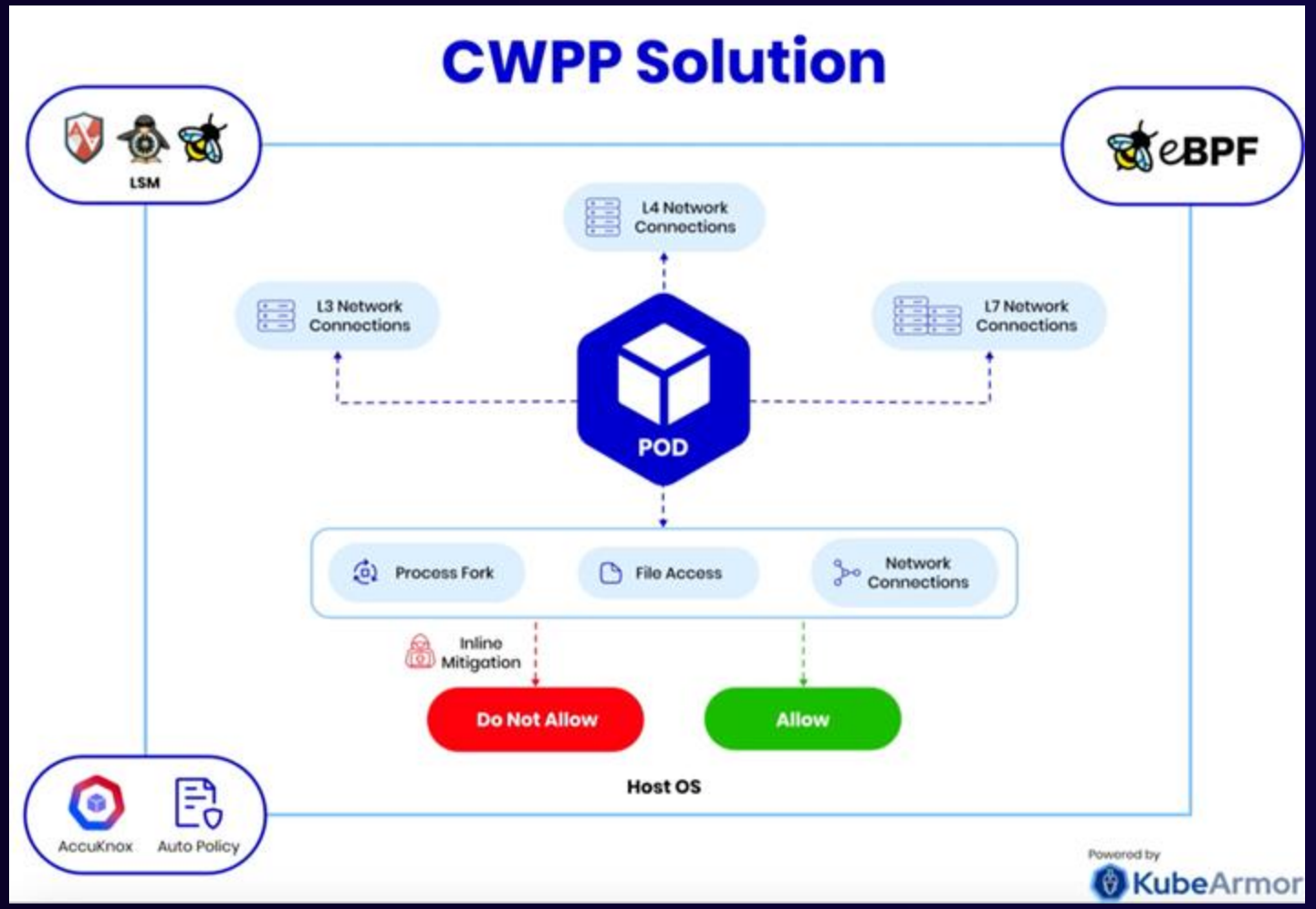
Continuous updating Compliance Dashboard

Comprehensive Reporting

Customizable Dashboard & Reporting

xcitium

CWPP - Cloud Workload Protection Platform



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

MITRE

DoD CYBER EXCHANGE PUBLIC

STIGs

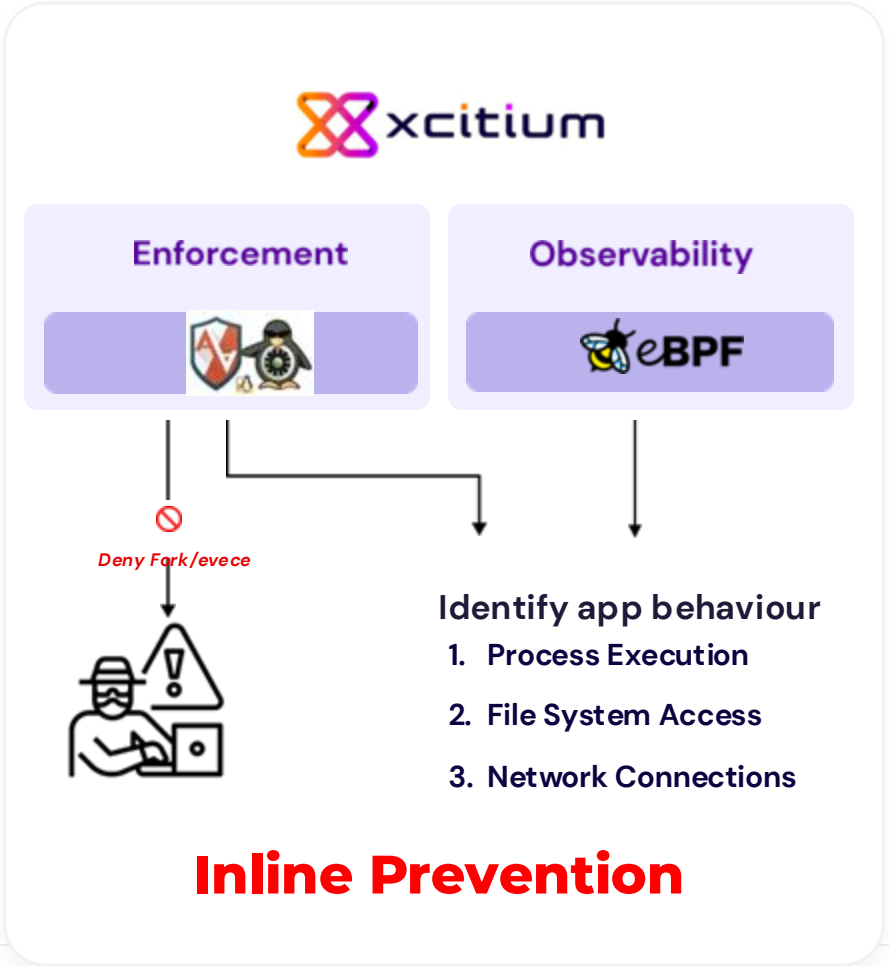
CIS Center for Internet Security

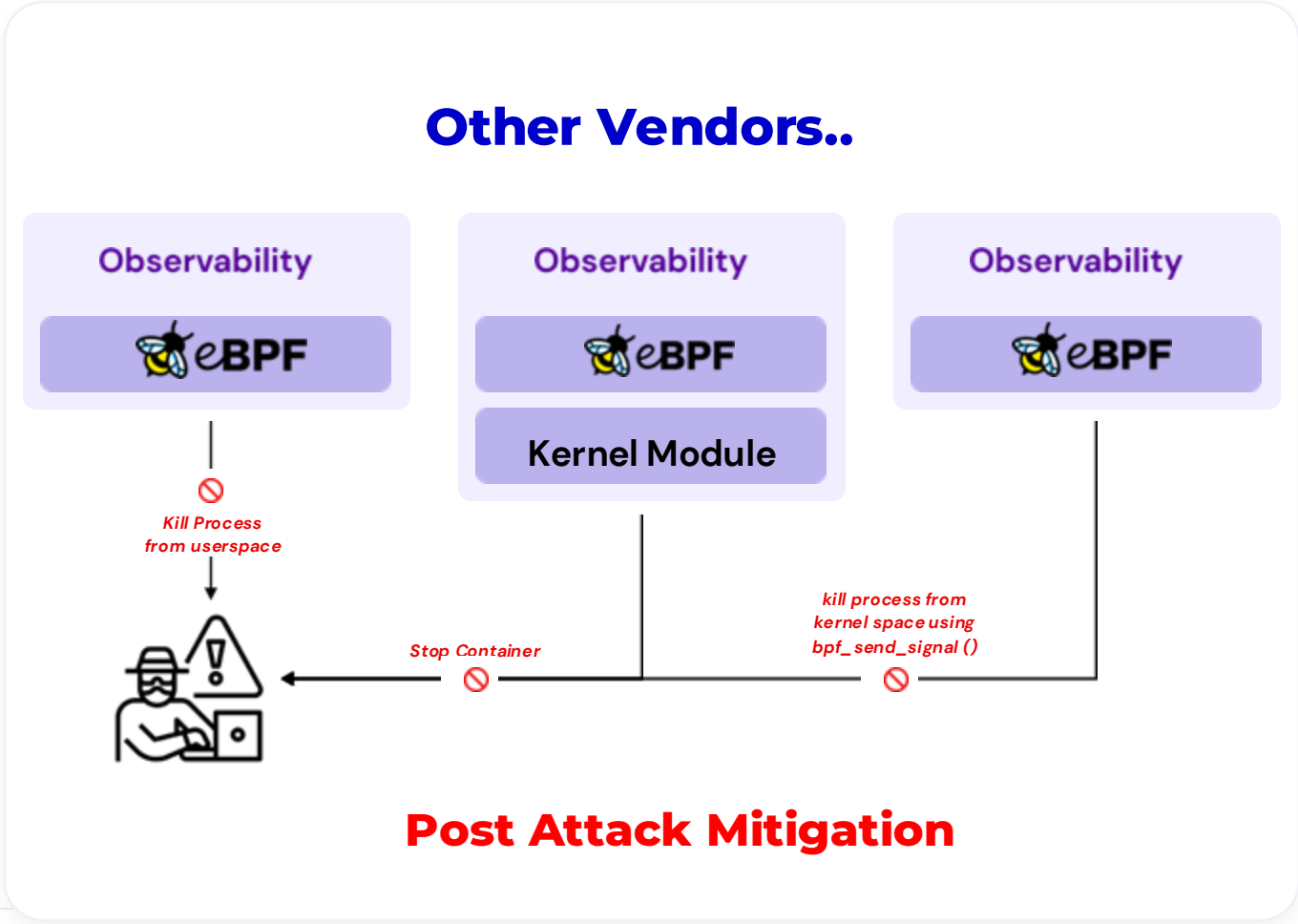
NIST

xcitium

Our Unique Differentiation

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





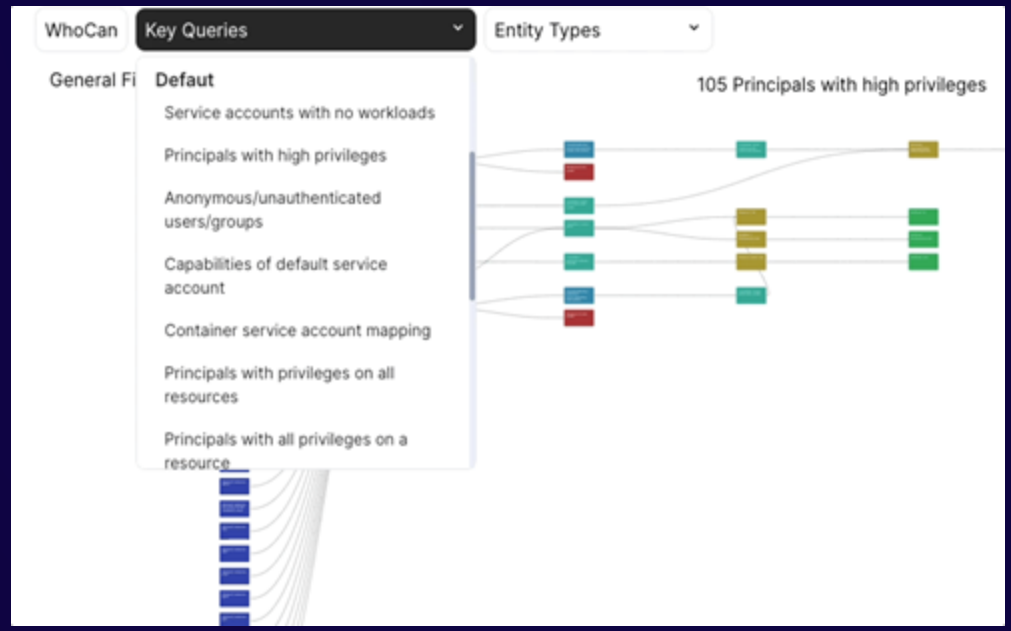
KIEM - Kubernetes Identity & Entitlement Management

Agentless scan of Kubernetes Identities

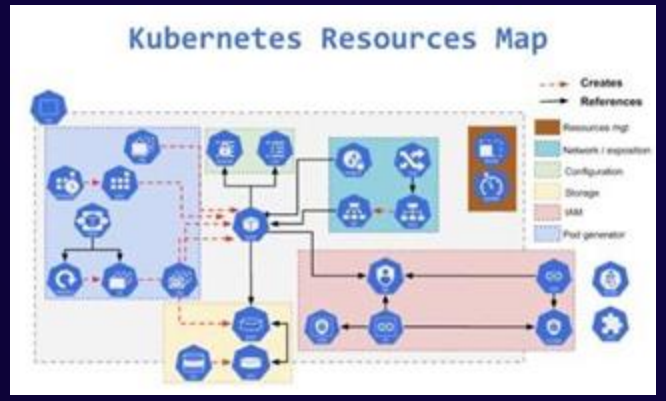
Misconfigurations

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



xcitium

How we Secure Software DevOps Life Cycle?

CODE → **IMAGE** → **CLOUD** → **RUNTIME**

- Static Code Analysis
- Software Composition Analysis
- Secret Scanning

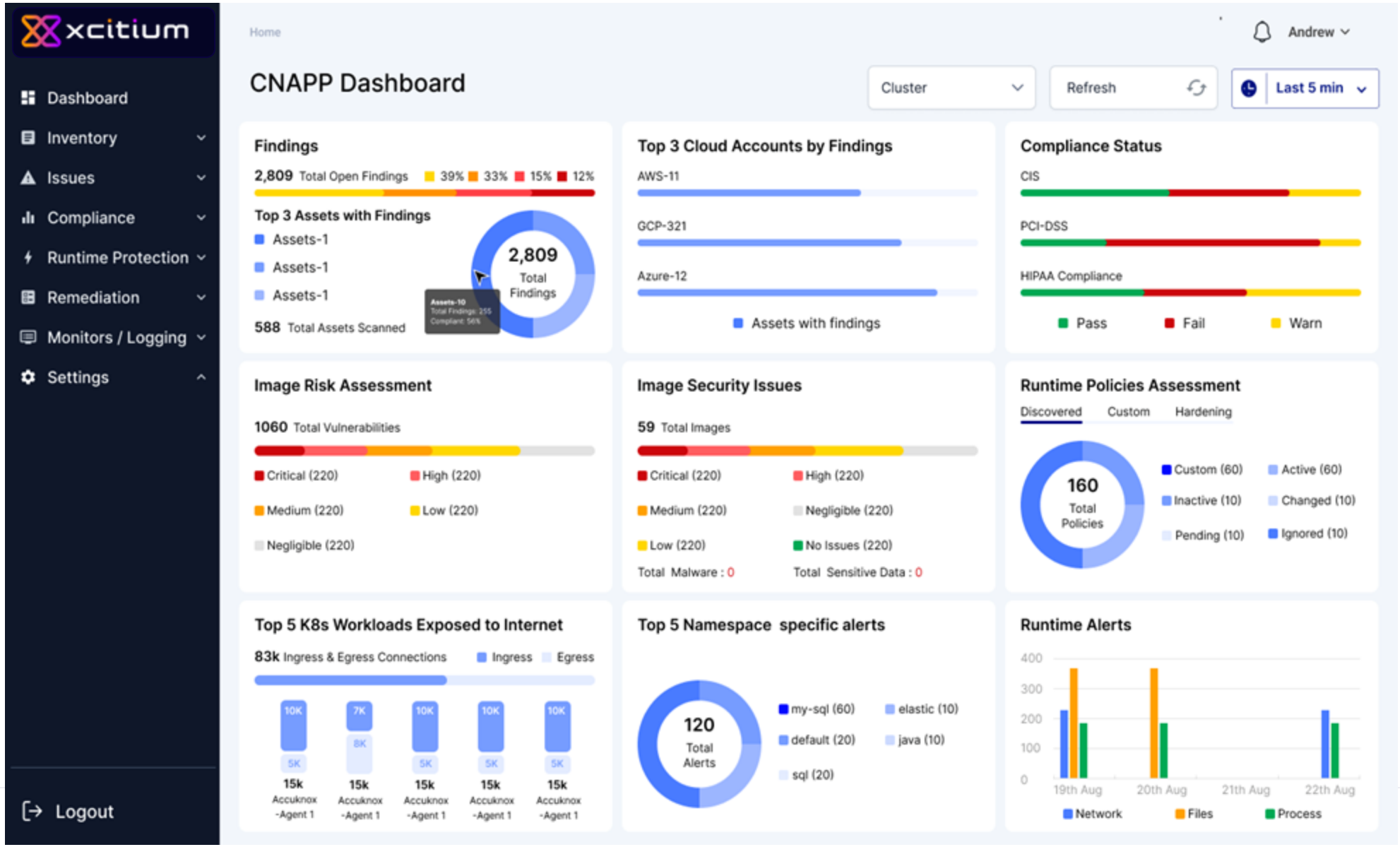
- Container Image Scanning
- Risk Prioritization
- Sensitive Assets
- Container Compliance

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

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

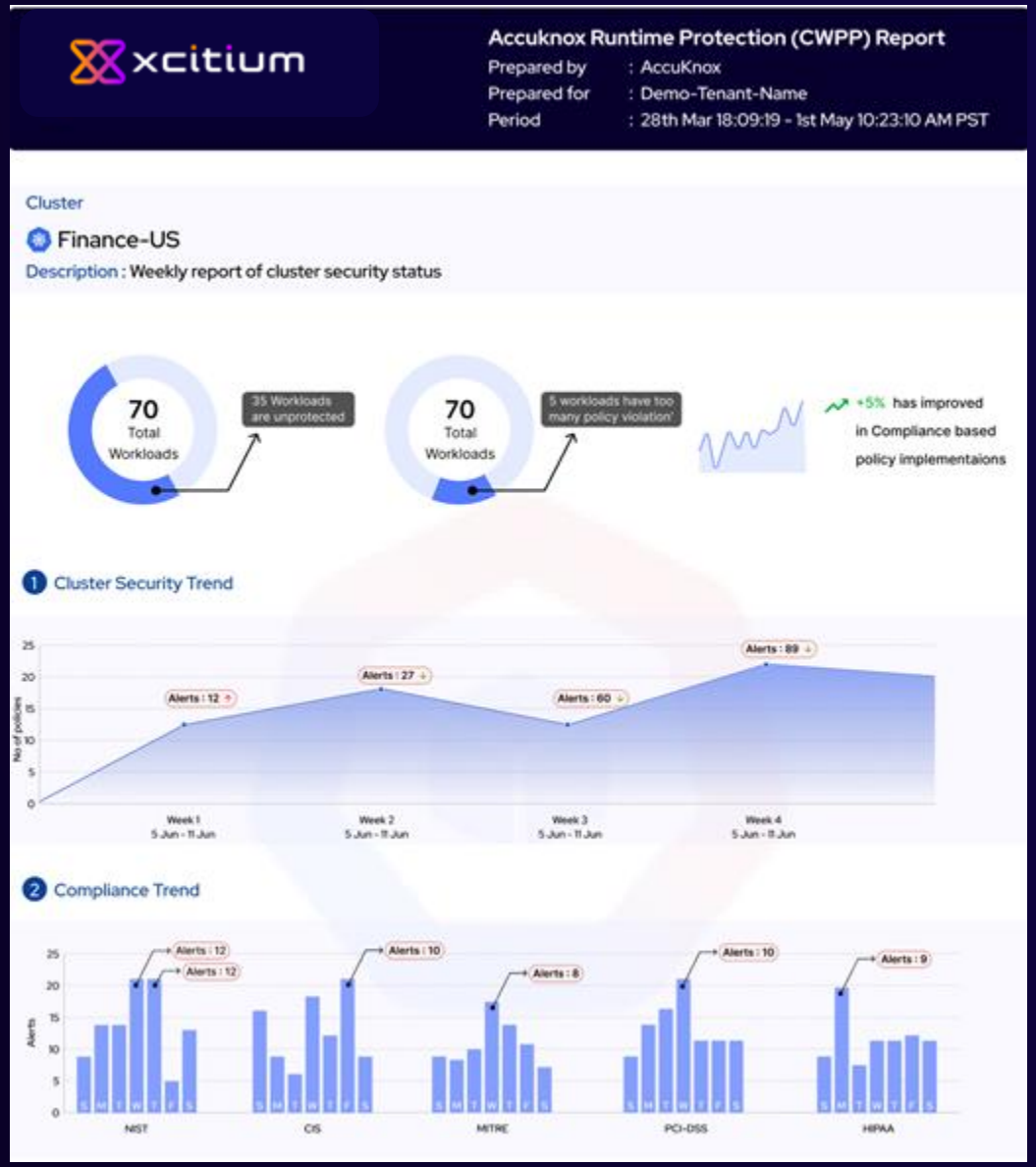
xcitium

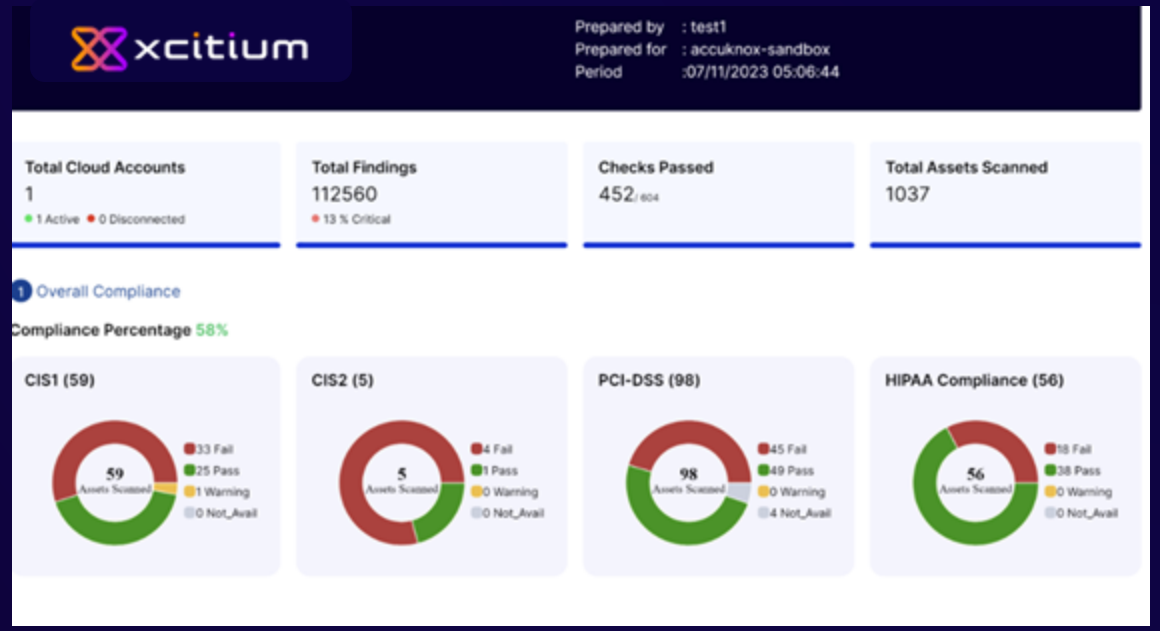
Comprehensive Dashboards



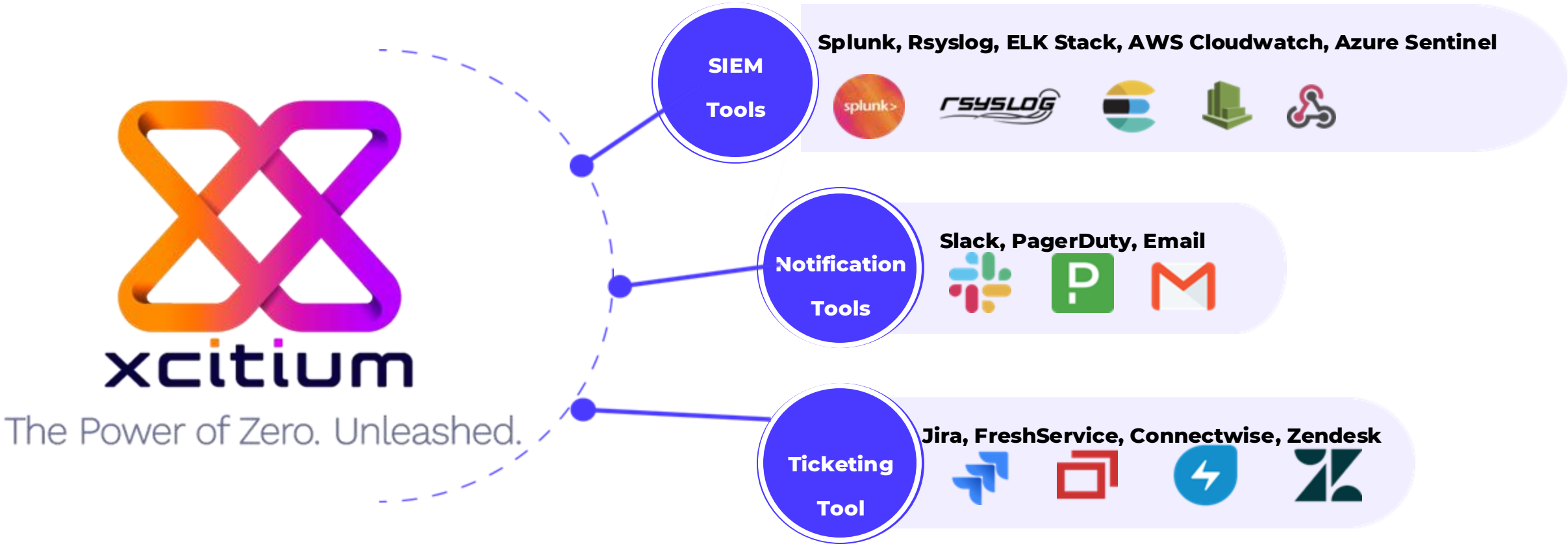
Comprehensive Reports

xcitium





Integrations we support



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