FORTINET

Agile Cybersecurity

Simplify and strengthen cloud security

Customers' Cloud Cybersecurity **Challenges**

THE INCONVENIENT TRUTH

Cloud has **broken the cybersecurity status quo…**

50% of cloud identities are super admins, and cloud workloads outnumber human users 10:1

Source: **Microsoft**

Every 18-minutes a new CVE (common vulnerabilities and exposures) is published

Source: **CVE.org**

Ransomware will cost around $265 billion (USD) annually by 2031, with a **new attack every 2 seconds**

Source: **Cybersecurity Ventures**

By 2027, 75% of employees will acquire, modify or create technology **outside IT's visibility** – up from 41% in 2022

Source: **Gartner**

68% of data breaches involve stolen credentials and social engineering

Source: **Verizon**

Protecting Cloud Applications & Data Requires a Holistic Approach

Unified Platform

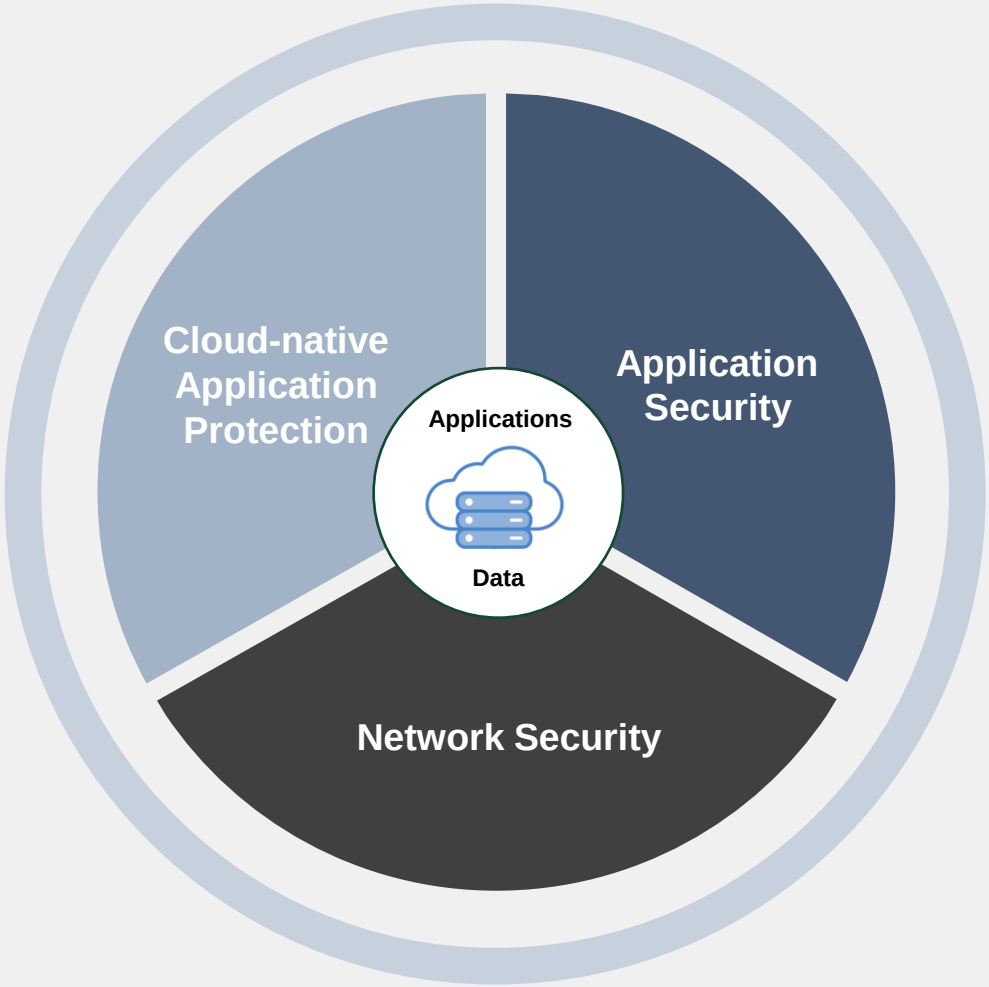
Single unified platform for all cloud security and secure CI/CD application development needs, consolidating multiple disparate tools

Integrated

Ability to **see <u>AND</u> protect** everything from coding, deploying, and running applications across hybrid and multi-clouds

Consistent Security

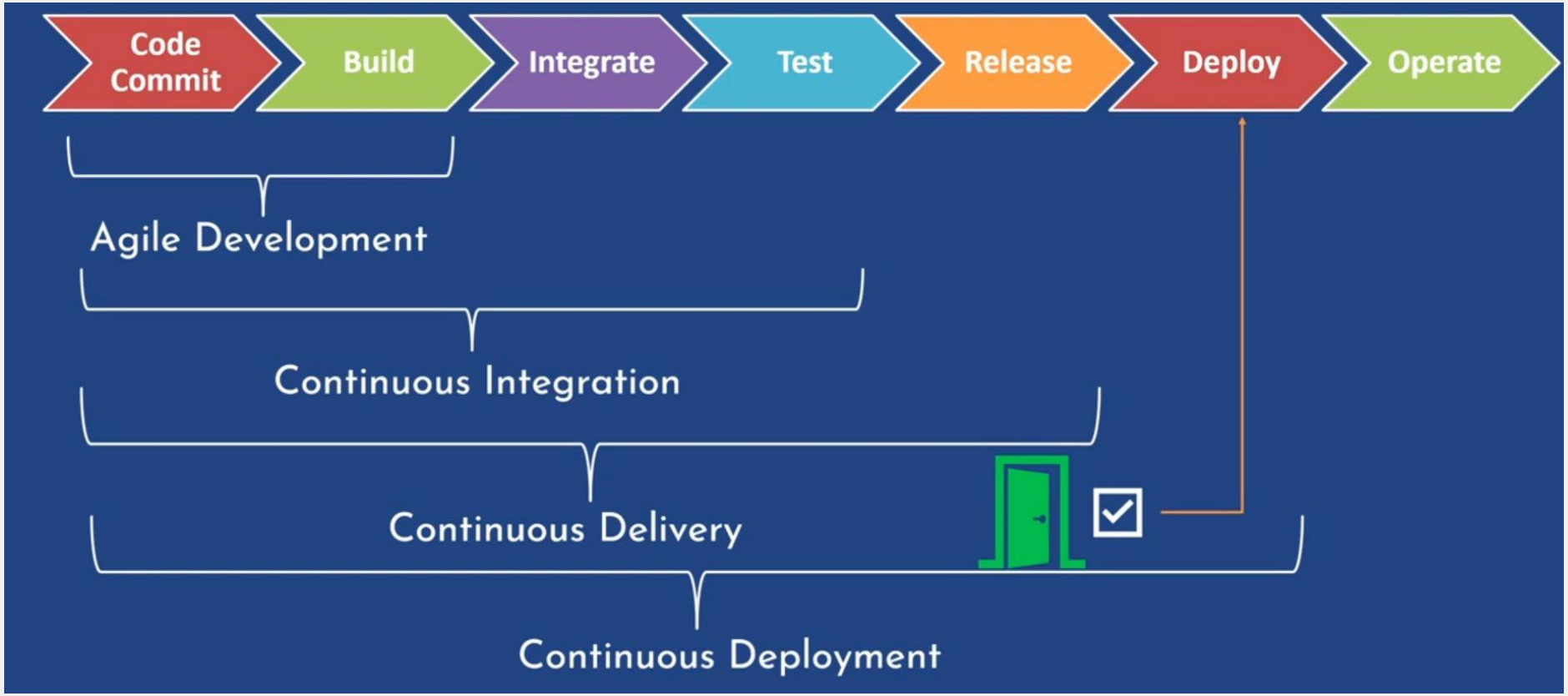
Simplified AI-driven security across integrated solutions with deep visibility and context across hybrid and multi-cloud



What is Agile Cybersecurity ?

Agile cybersecurity illustrated

Agile cybersecurity, often referred to as “Agile Security” or “DevSecOps” (Development, Security, Operations), is an approach incorporating Agile principles and practices.



In a nutshell, agile cybersecurity is implementing an adaptive and iterative approach to securing information systems.

The five challenges:

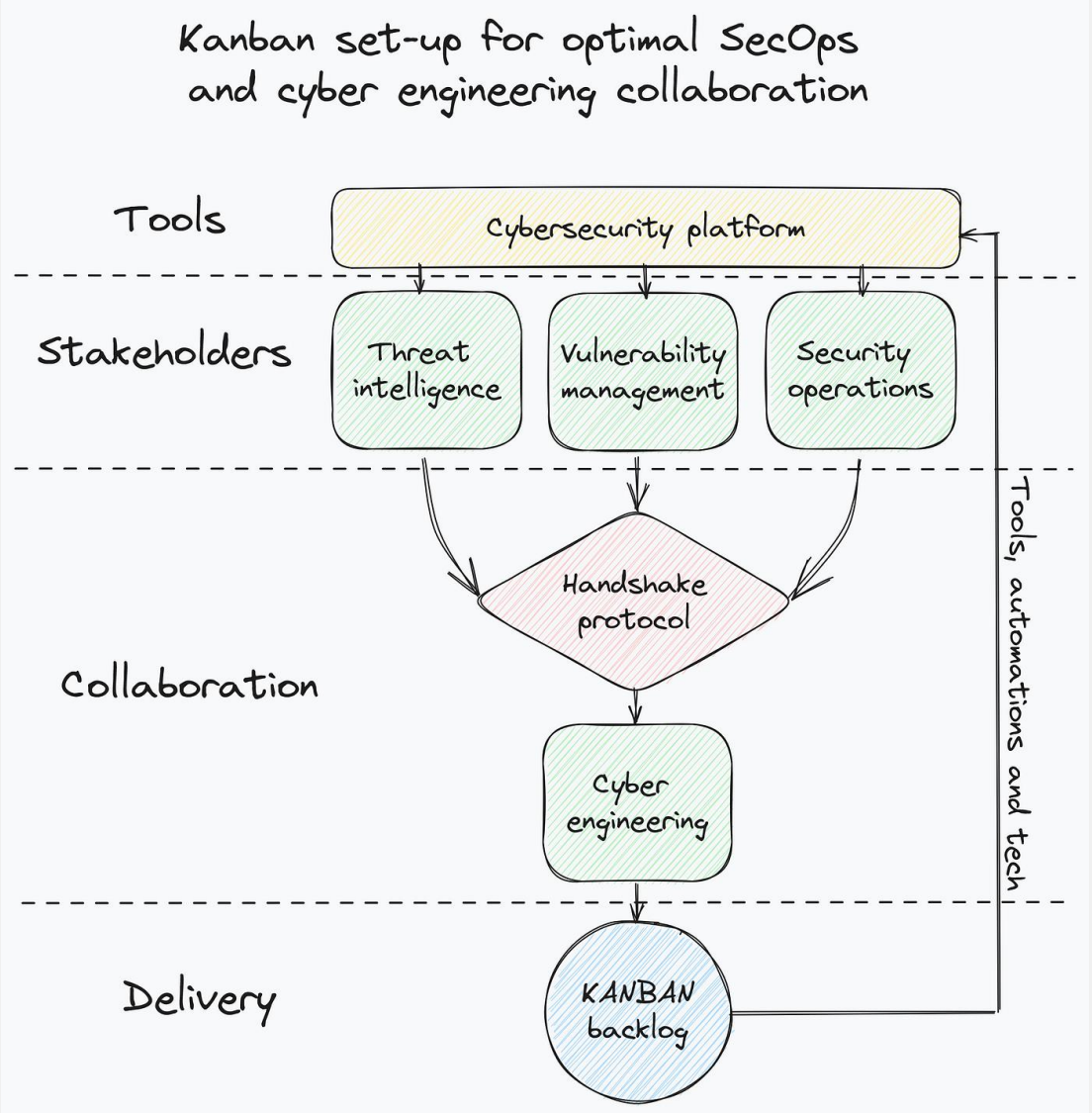
1: preparing your security team for Agile

2: hiring leaders with Agile experience

3: applying the right framework (SCRUM vs Kanban)

4: prioritising operations

5: developing a low-disruption QBR process



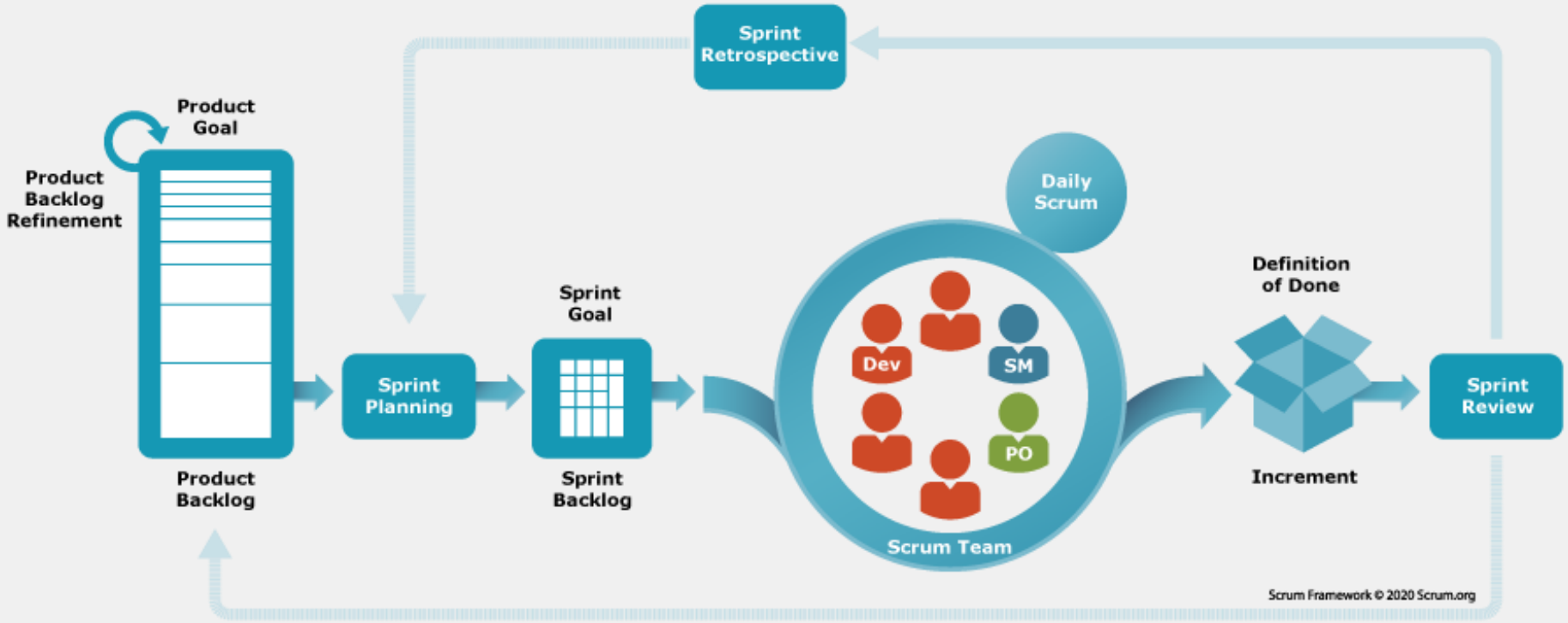
Agile cybersecurity pillars:

1: Operating pillar

2: Planning pillar

3: Developing pillar

4: Releasing pillar



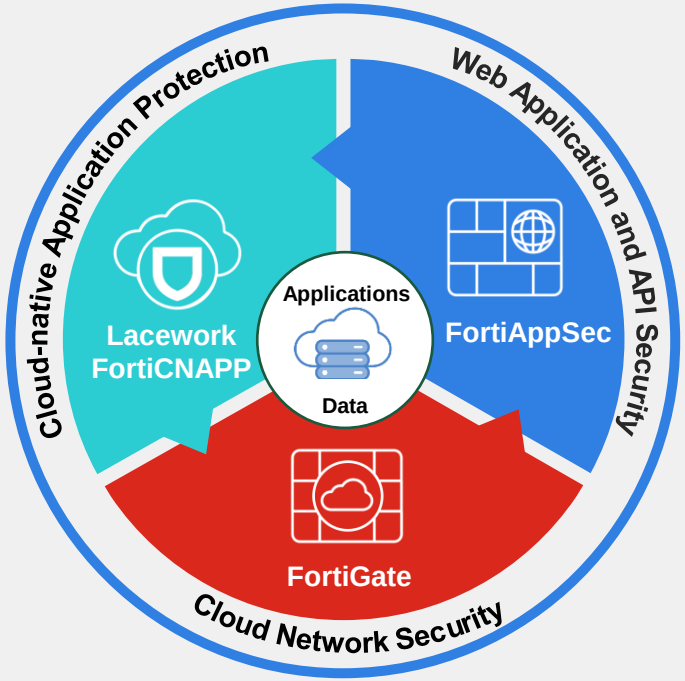
Let’s Dive into Cloud Cybersecurity

Comprehensive Integrated Code-to-Cloud Security

360-degree cloud defense-in-depth protection against all threat and risk vectors

Secure everything from code to cloud faster with **unparalleled context and visibility with a single unified platform**.

- CSPM
- KSPM
- CWP
- CIEM
- IaC
- Code Security



Integrated AI/ML-driven platform to protect business-critical web applications and APIs from attacks that target known and unknown vulnerabilities.

- WAAP
- GSLB
- Bot Mitigation Management
- Threat Analytics
- DAST

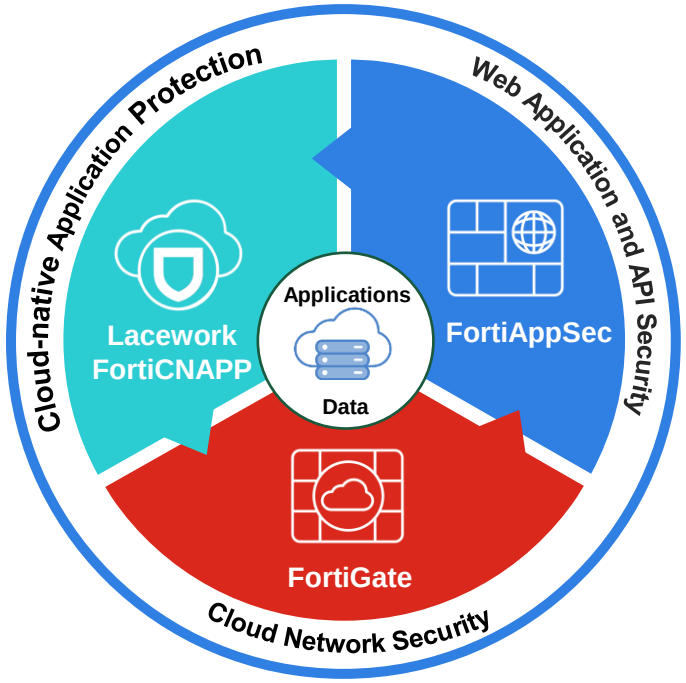
Achieve network visibility and enforcement of **consistent security policies** across private, public, and telco clouds.

- Virtual FW
- Cloud-native FW
- Centralized Management
- Analytics

Competitive Advantage of a Cloud Security Platform

Fragmented Cloud Security Challenges

Cloud Security Platform



Comprehensive
Centralized, integrated, code-to-cloud security platform

Consistent Security
Reduce operational complexity, gain predictable outcomes

AI/ML-driven deep context, visibility
Gain unparallel understanding of your cloud environments and rapidly identify and mitigate threats and risks

Optimize Cloud Spend
Broad catalog of solutions with flexibility of usage-based licensing

Business Outcomes of Cloud Security

Comprehensive Integrated Code-to-Cloud Security

360-degree cloud defense-in-depth protection against all threat and risk vectors

VISIBILITY & PROTECTION

Deep visibility combined with AI-powered security services deliver greater security effectiveness

5mins

Reduced investigation time from 10 hours to as little as five mins

ENHANCED EFFICIENCY

Increase productivity and prioritization of security teams

98%

Reduction in alert volumes

COST OPTIMIZATION

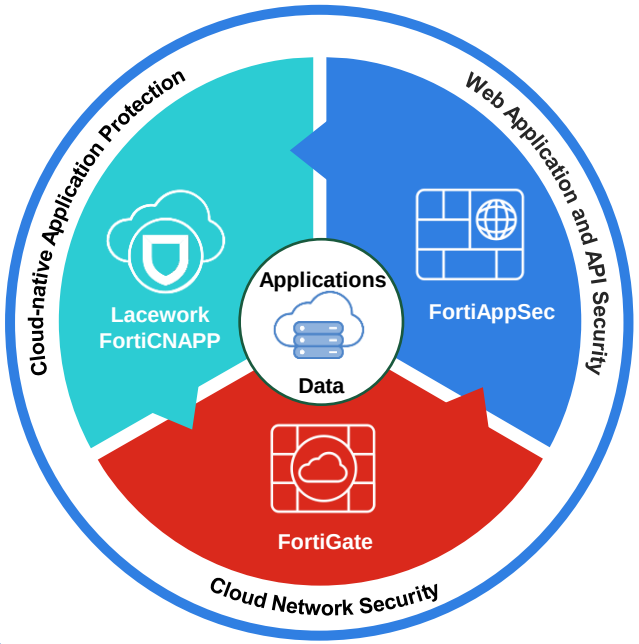
Reduce siloed, point products with integrated cloud platforms

3X

ROI by reducing point products

Cloud Security

Securely modernize applications and digital acceleration across hybrid and multi-clouds with comprehensive integrated code-to-cloud security that delivers deep visibility and protection — all from a single vendor.



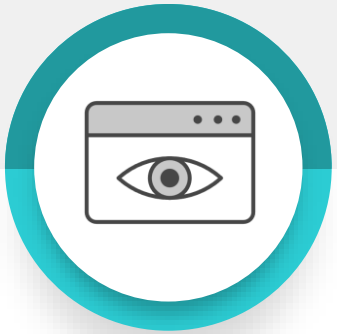
Our approach

How to Address the Cloud Security Challenge

Identifying, Prioritizing and Resolving Risks and Threats in Cloud-native Applications

Minimize Attack Surface

Gain comprehensive visibility and proactively reduce vulnerabilities, misconfigurations and excessive privileges without slowing down development.



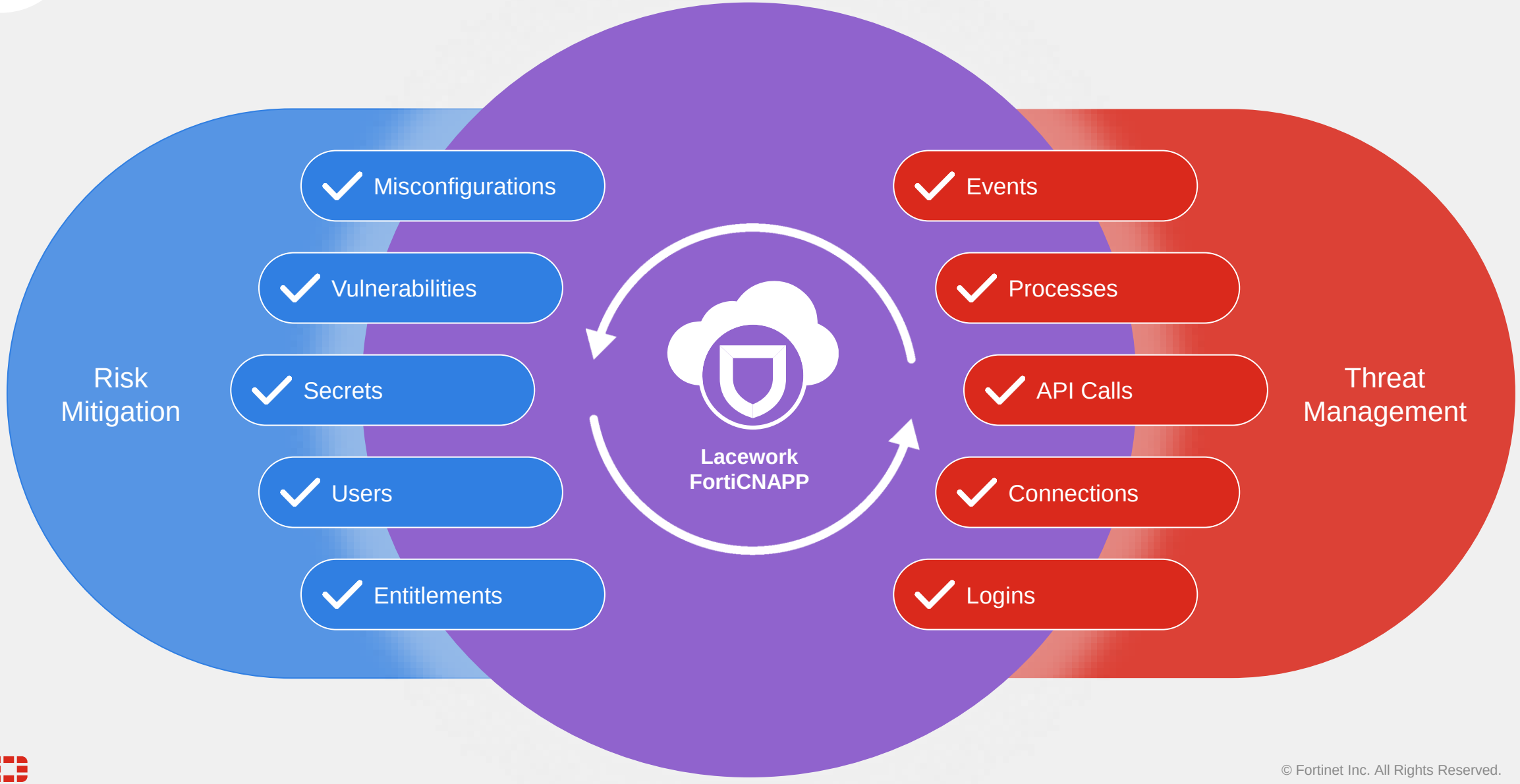
Continuously Monitor Risks

Continuously assess virtual machines, containers and Kubernetes workloads to address active risks before they are exploited.

Reduce Threat Impact

Quickly detect, investigate and respond to unusual behavior and active threats including the use of compromised credentials, cloud ransomware and cryptomining.

Prioritization Requires Combining Risk and Threat Context



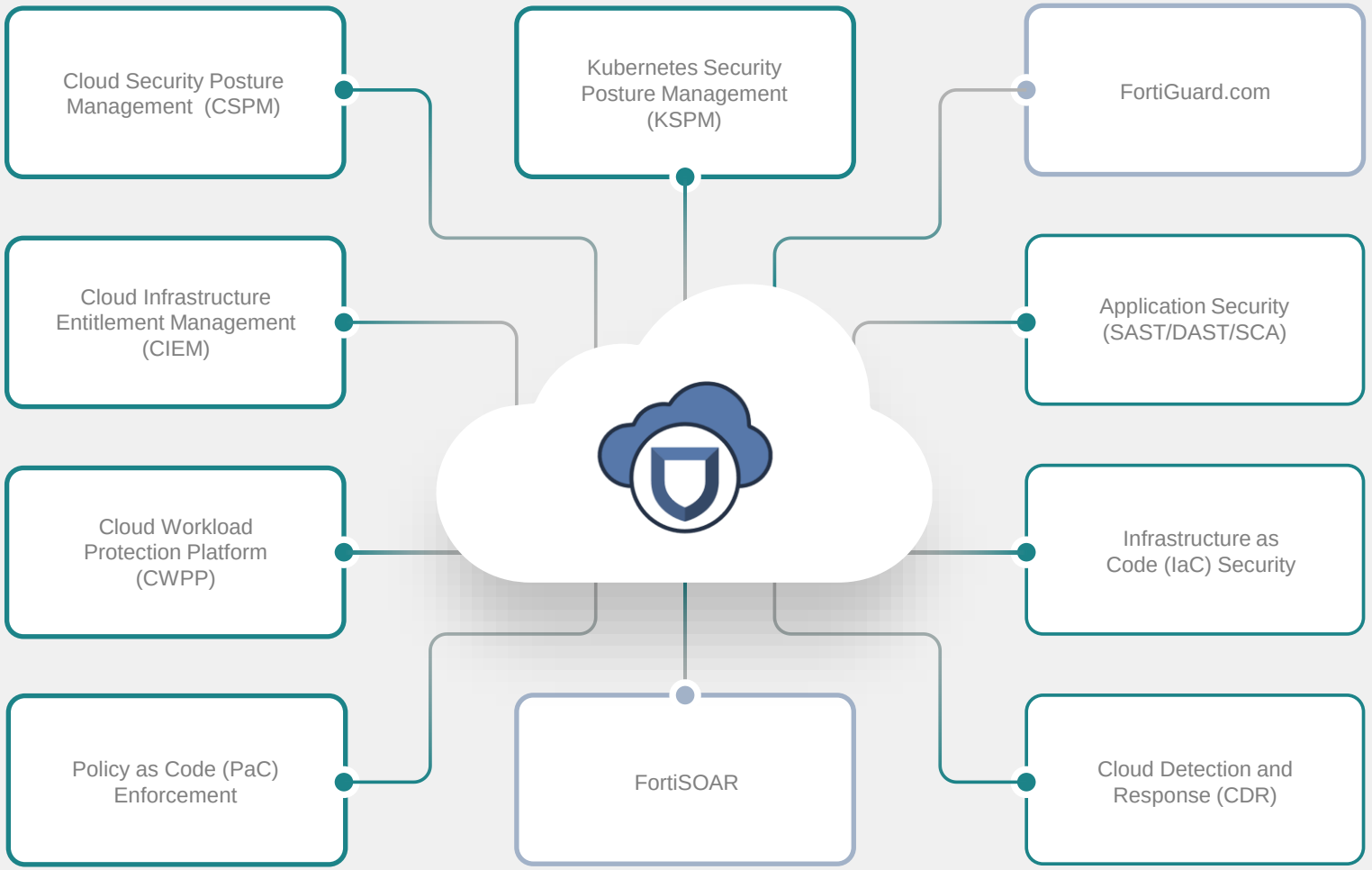
Lacework FortiCNAPP

The Most Complete AI-driven Cloud-Native Application Protection Platform

Single vendor for all cloud security and secure CI/CD application development needs.

See AND protect everything from coding, deploying, and running applications across hybrid and multi-clouds.

Simplify security with AI-driven platforms from both Lacework FortiCNAPP and Fortinet.



Creating Amazing Customer Outcomes

100:1

Reduction in the number of daily alerts

2 to 5

Fewer cloud security tools via consolidation

80%

Faster investigation of incidents and alerts

90%

Reduction in manual cloud security efforts

50%

Reduction in SIEM data ingestion cost

0-Day

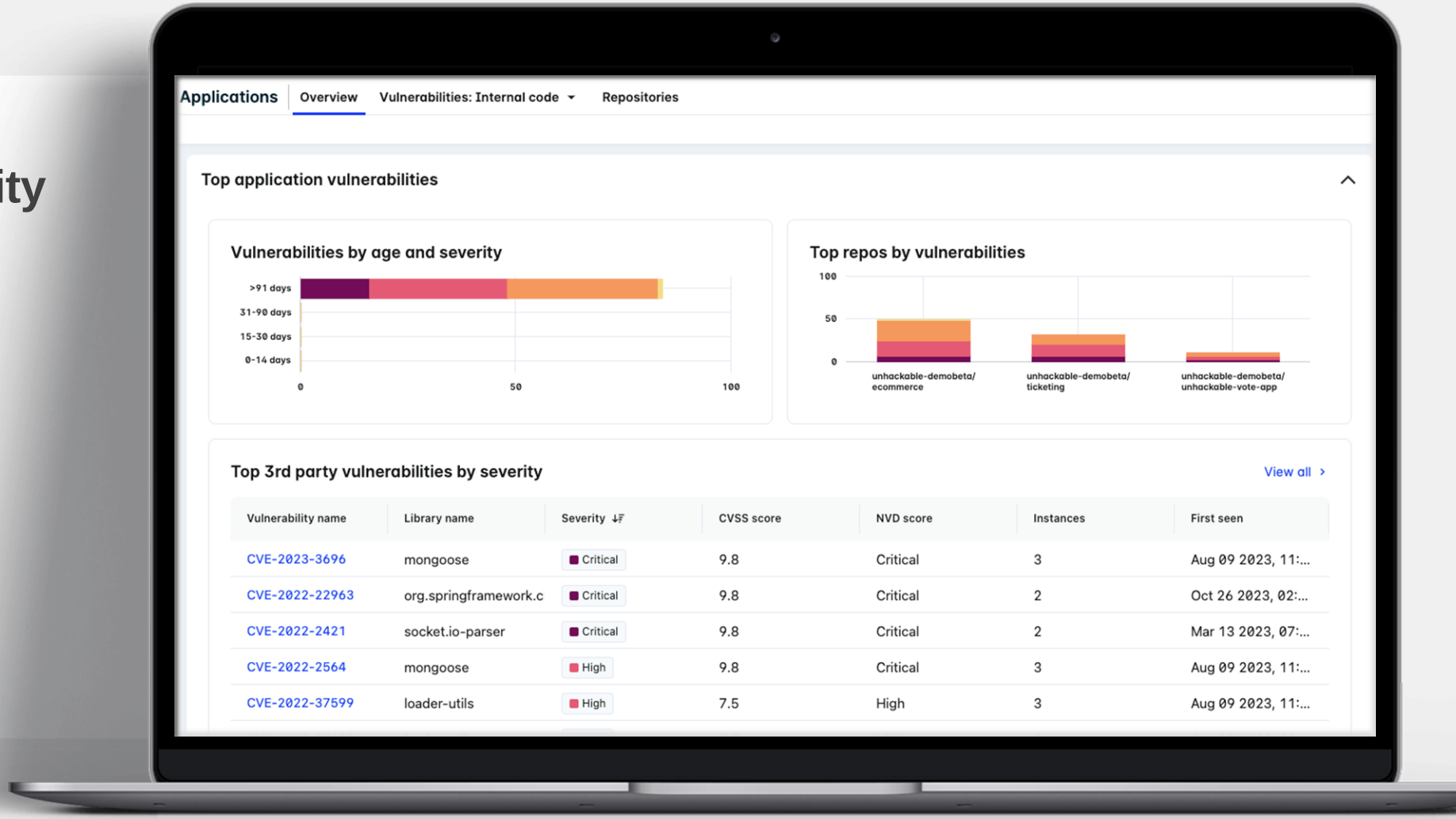
Detection of active threats and attacks

How does it look like?

Shift Security Left to Reduce Risk and Remediation Costs

Application and Infrastructure Security

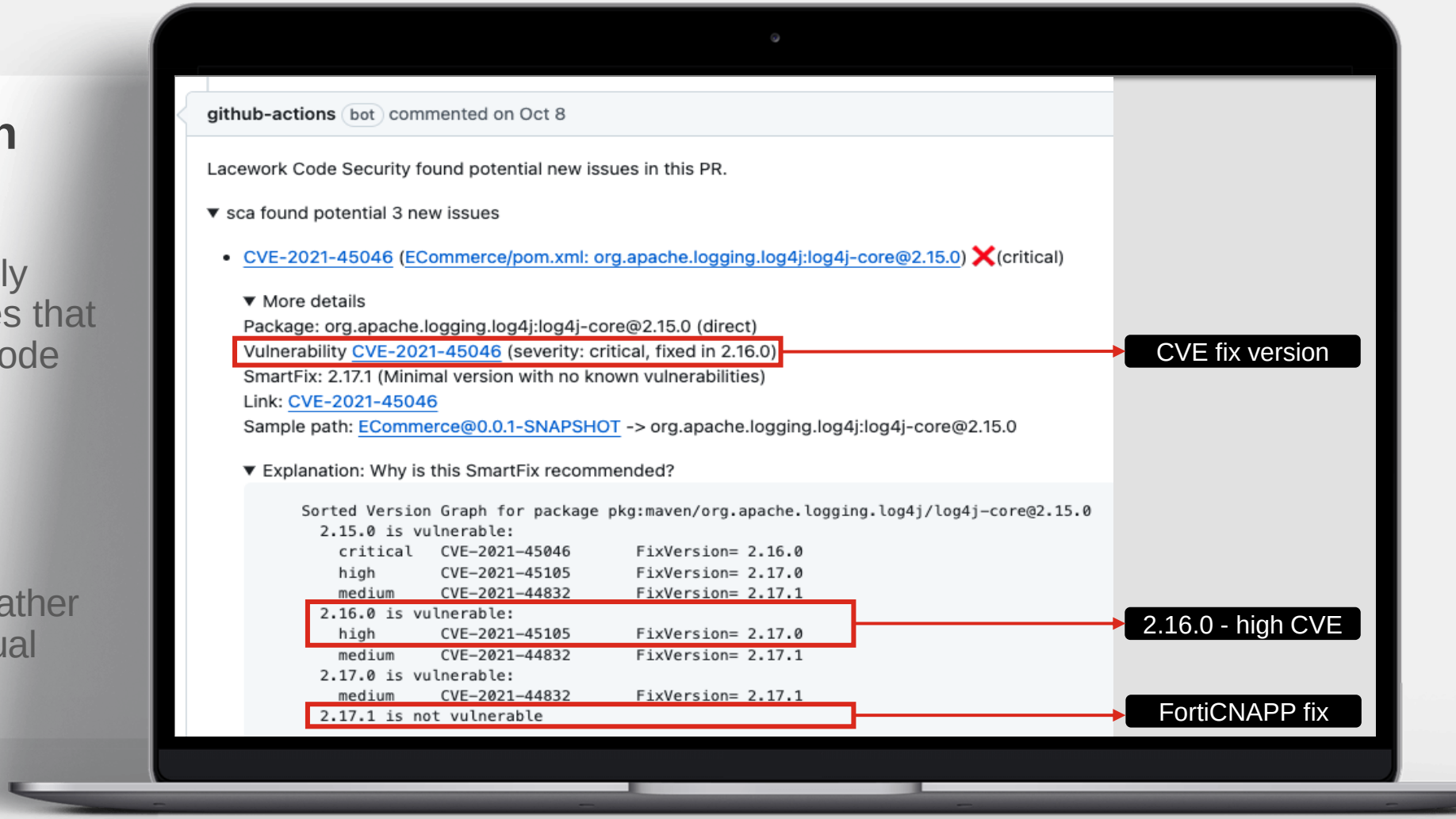
- Gain visibility of software supply chain (SBOM)
- Identify third-party code CVEs (SCA)
- Detect first-party code weaknesses (SAST)
- Secrets detection
- Verify cloud infrastructure configuration (IaC)



Quickly Remediate Vulnerabilities

Instantly know which packages are safe

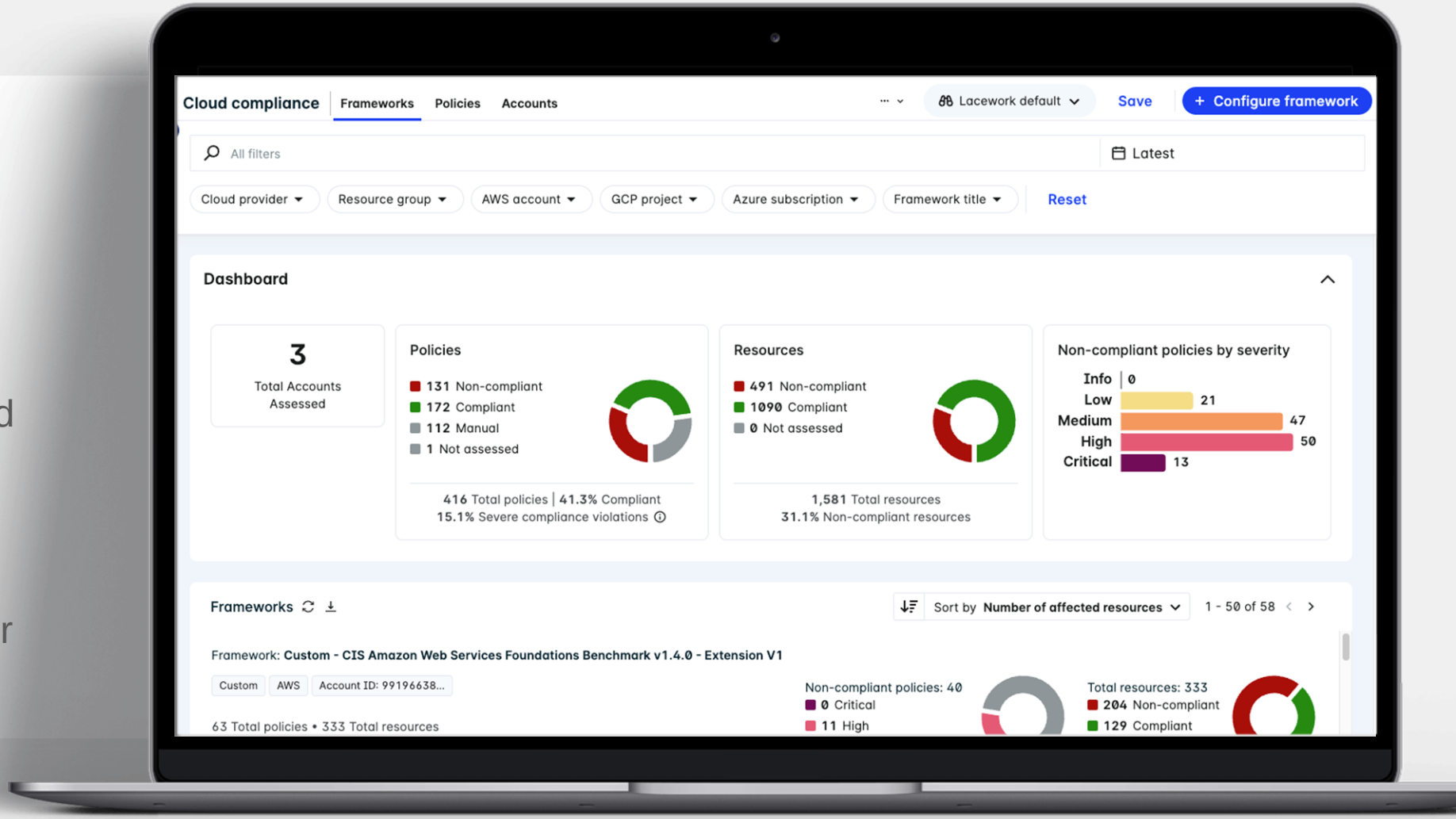
- Save time by immediately identifying safe packages that are required to secure code
- Establish trust and transparency with development teams
- Take a comprehensive approach to risk mgmt, rather than dealing with individual CVEs



Gain Visibility of Cloud & K8s Configuration Risk

Security Posture Management CSPM and KSPM

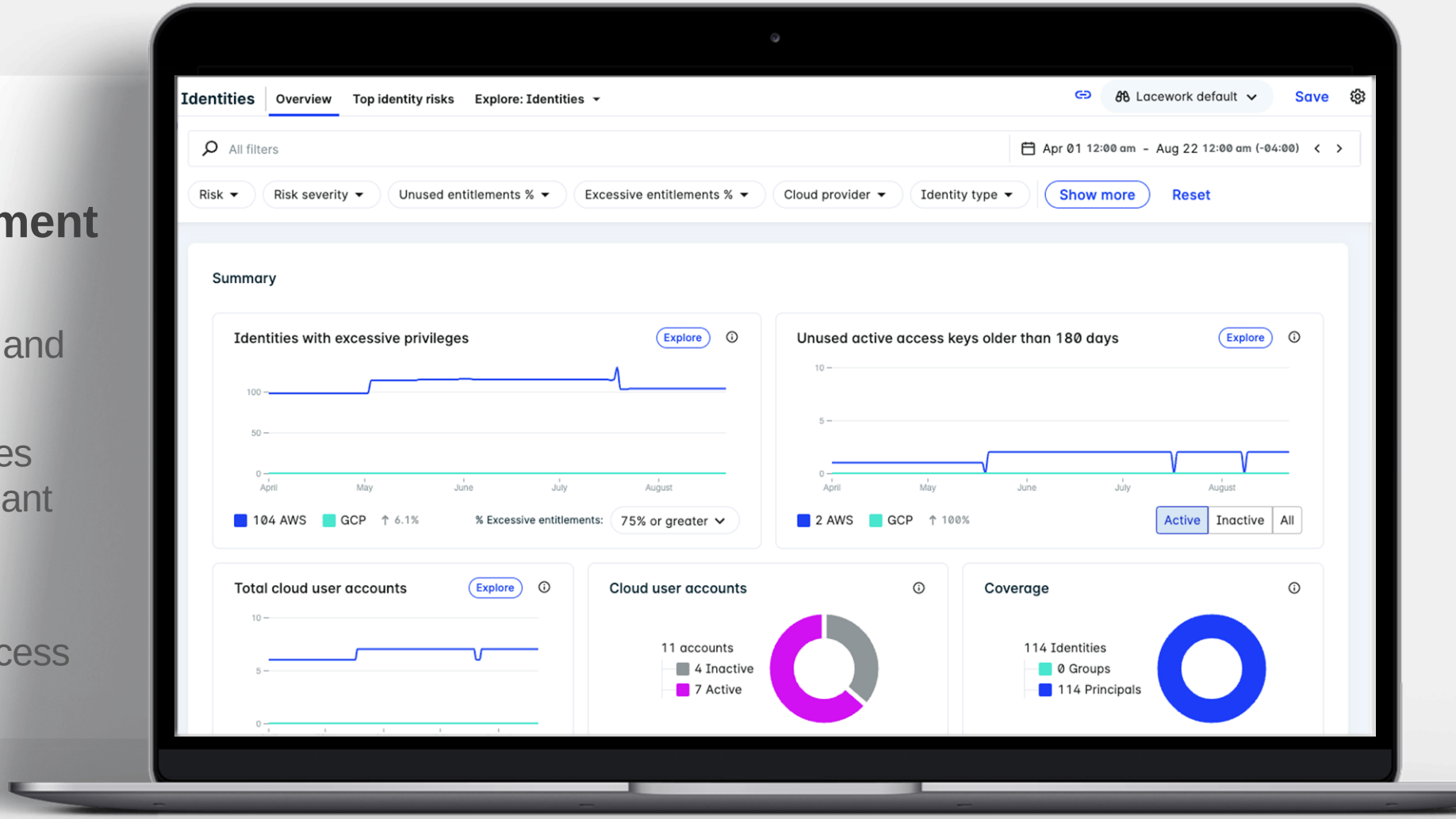
- Gain complete visibility of continually changing cloud resources
- Continuously monitor for misconfigurations
- Achieve compliance faster



Reduce Identity Risk and Achieve Least Privilege Access

Cloud Infrastructure Entitlement Management (CIEM)

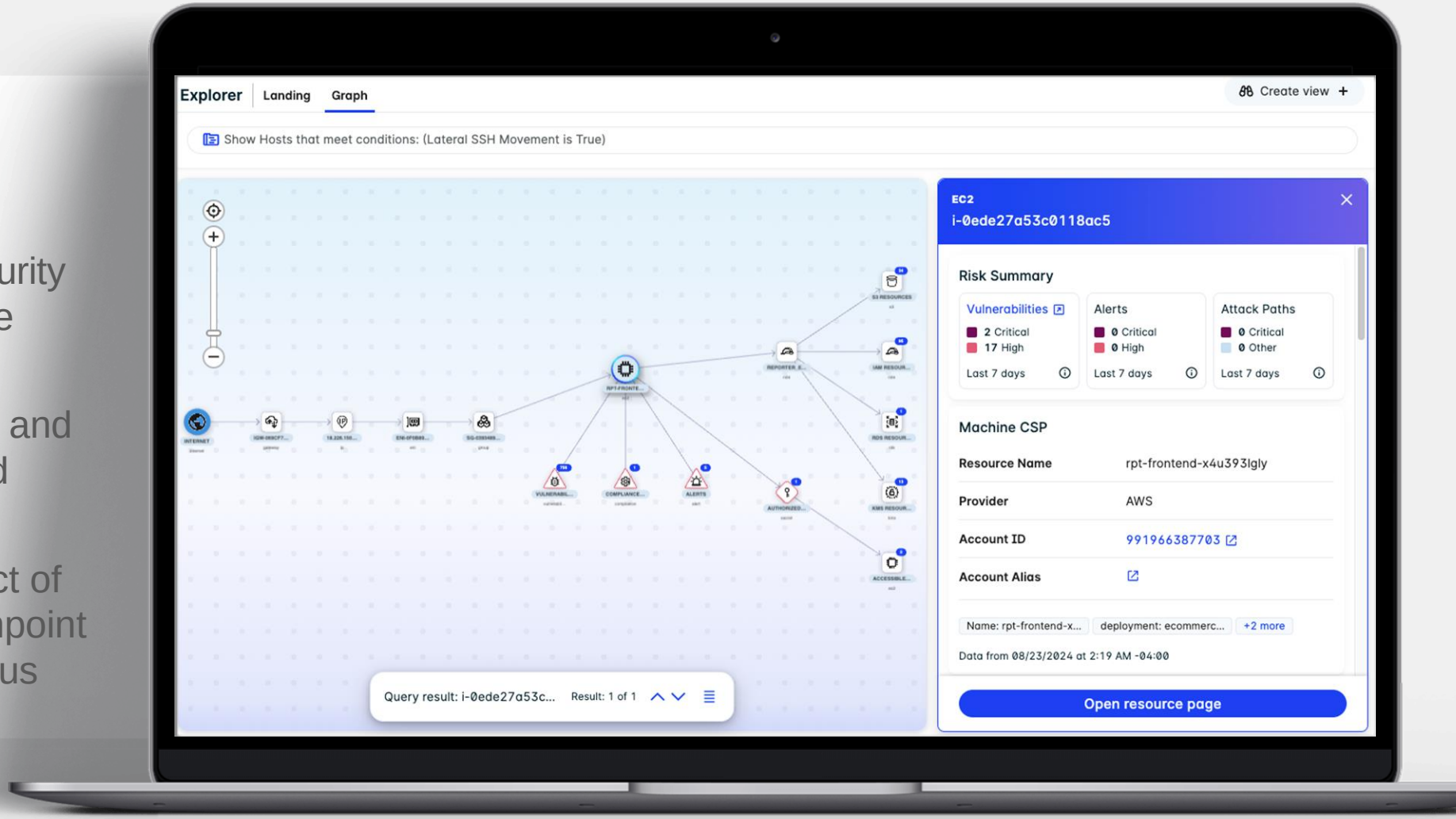
- Gain visibility of identities and their permissions
- Understand which identities have excessive and dormant permissions
- Right-size permissions to achieve least privilege access



Prioritize Risks That Matter Most

Visualize and Contextualize Risk

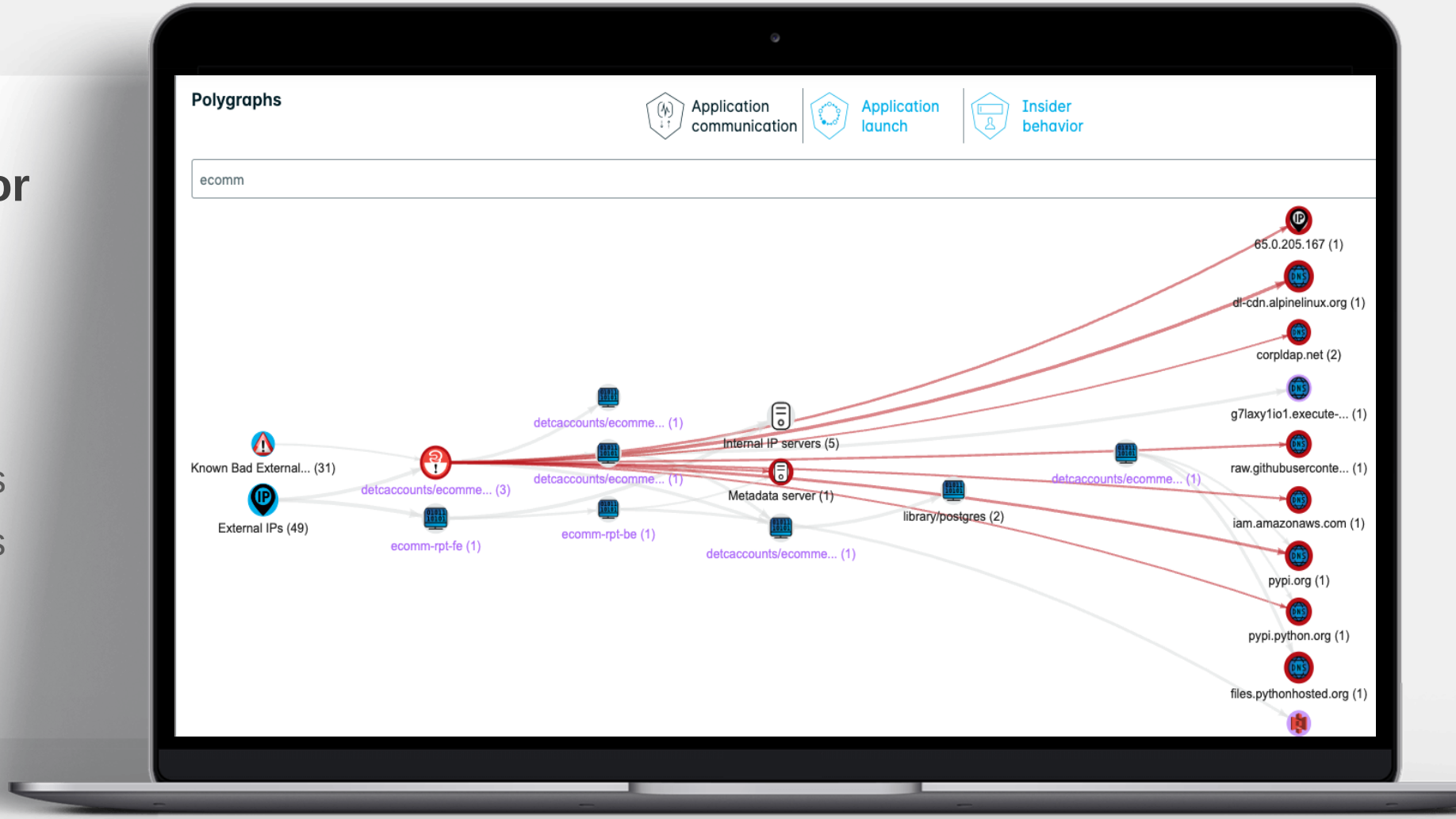
- Easily navigate cloud security data with natural language queries
- Instantly see how entities and their risks are related and interconnected
- Quickly assess the impact of risks and threats, and pinpoint how to limit the blast radius



Identify Anomalies and Malicious Activity

Continuously Monitor Workloads

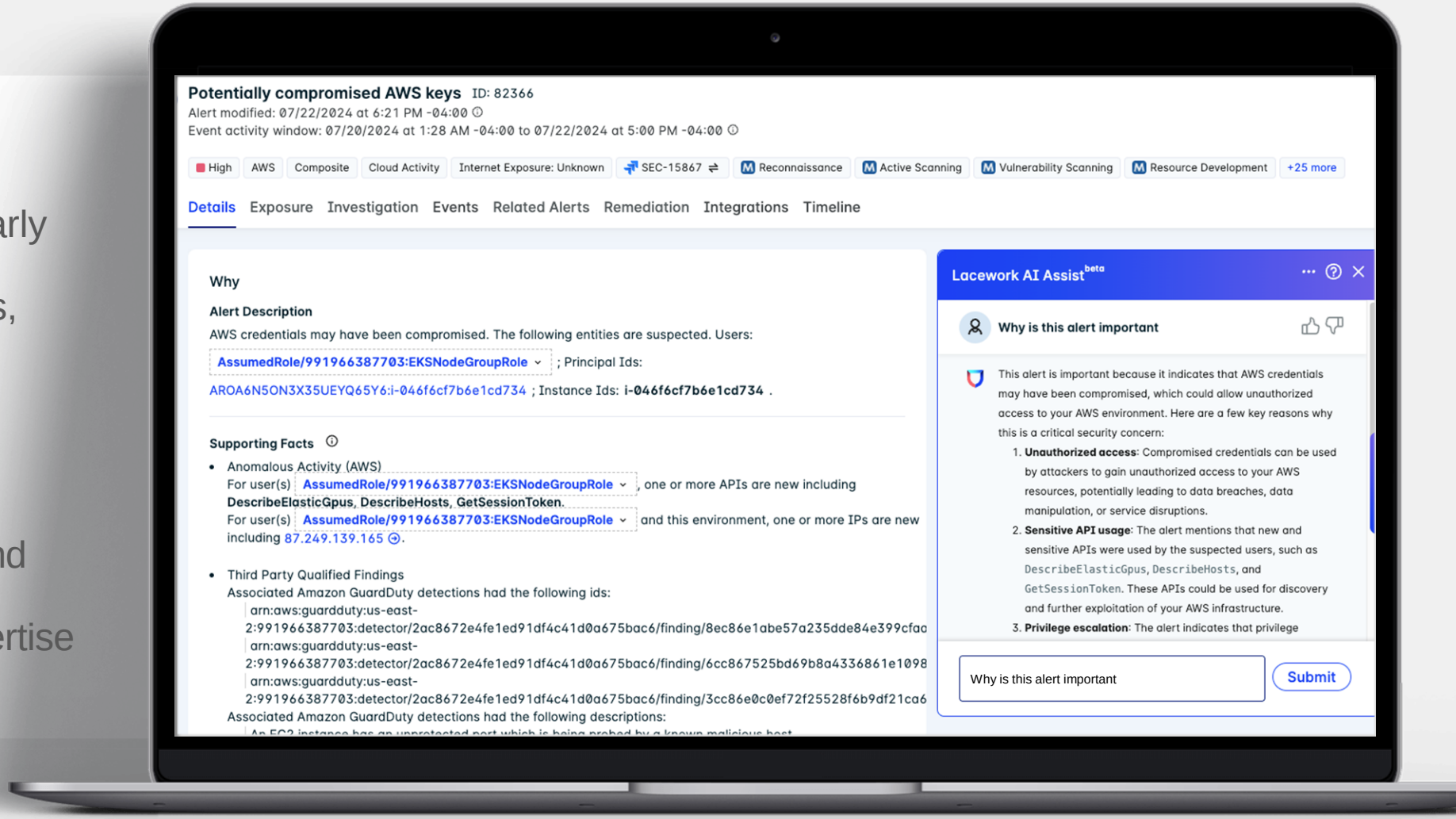
- Map network connections
- Discover anomalous behaviors
- Detect in-progress threats
- Find vulnerabilities across hosts, containers and Kubernetes (K8s)



Detect Active Attacks - Compromised Credentials

Composite Alert

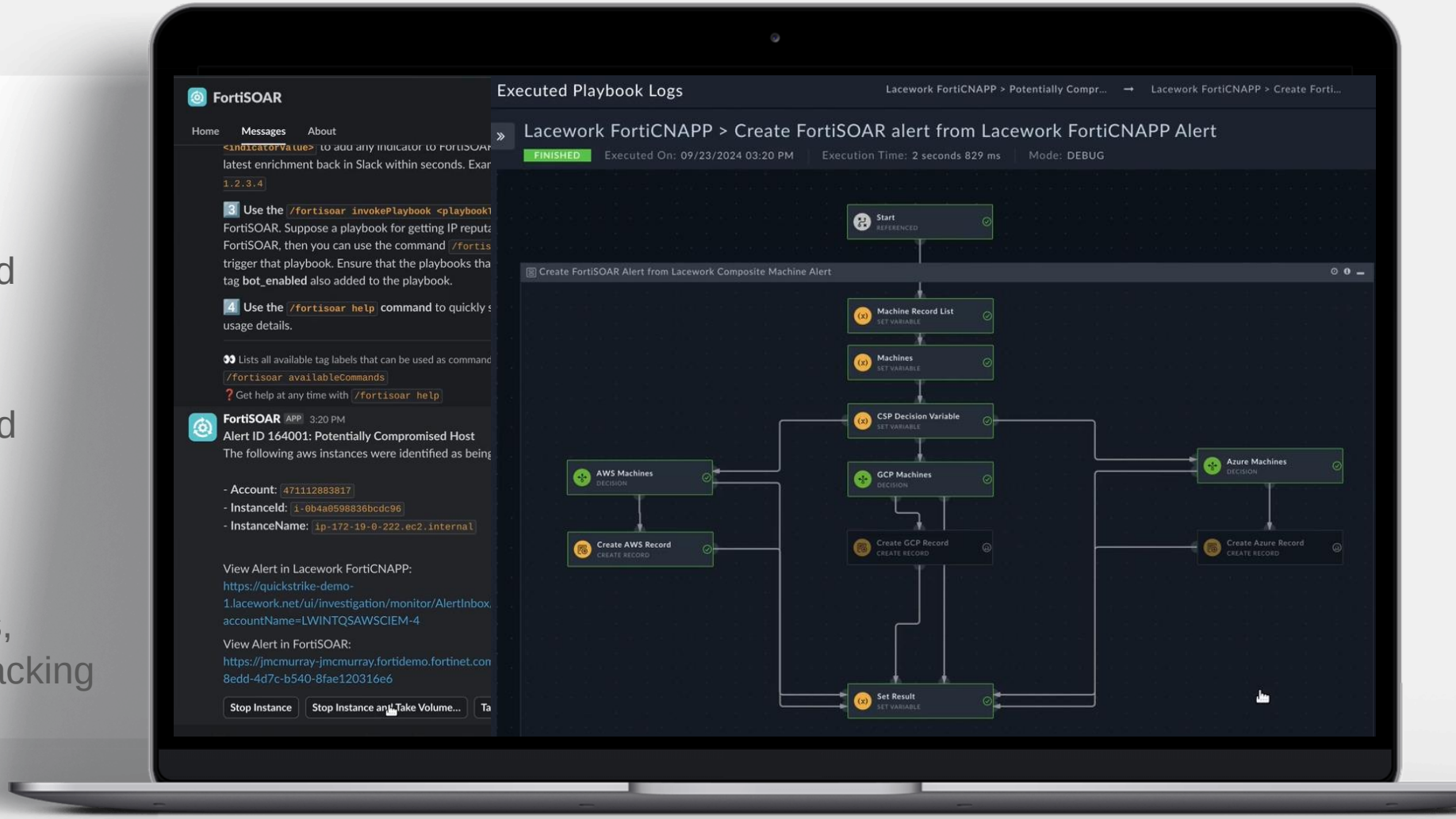
- Automatically detects early signs of attacks like compromised credentials, ransomware and more
- Combines multiple low-severity signals into one priority alert
- Reduces alert volume and eliminates the need for extensive querying, expertise and manual effort



Automate Threat Response

Accelerate Alert Response Times

- Automate remediation and blocking of active runtime threats
- Easily customize and build granular playbooks for FortiCNAPP alerts
- Quickly respond to compromised credentials, ransomware and cryptojacking




FORTINET