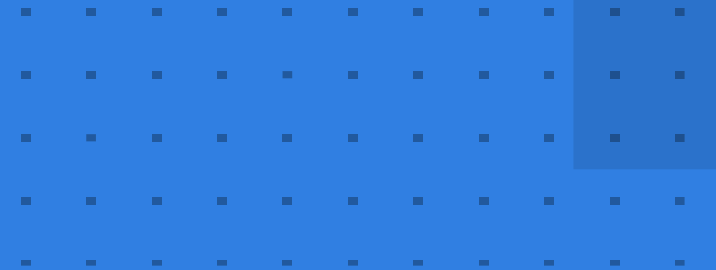




Agile Cybersecurity

Simplify and strengthen cloud security

Customers' Cloud Cybersecurity Challenges



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

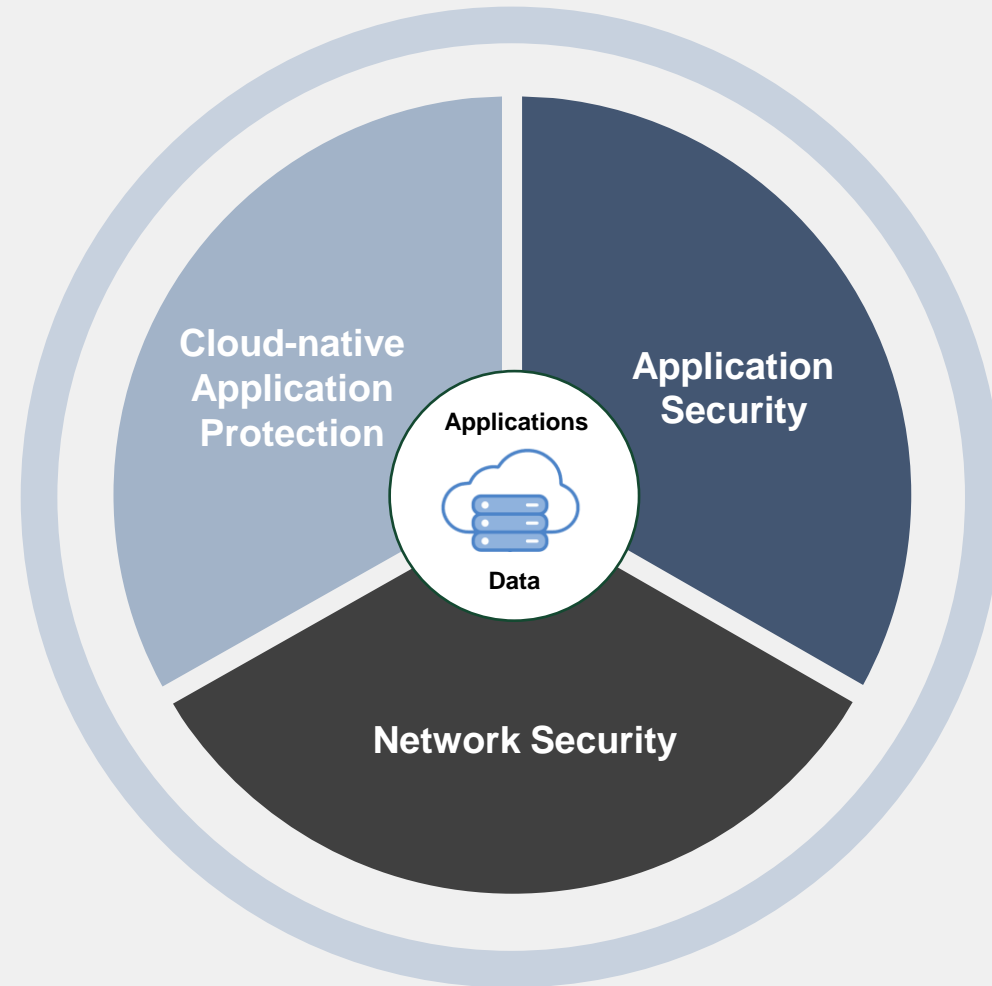
Single unified platform for all cloud security and secure CI/CD application development needs, consolidating multiple disparate tools

Integrated

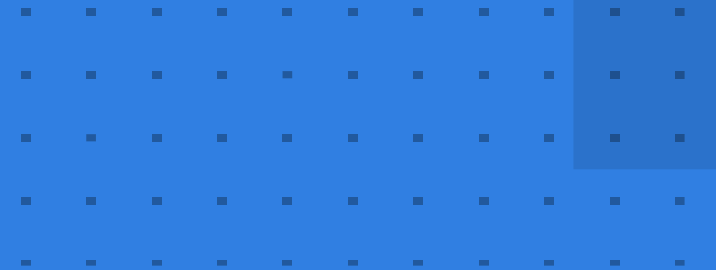
Ability to **see AND protect** everything from coding, deploying, and running applications across hybrid and multi-clouds

Consistent Security

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

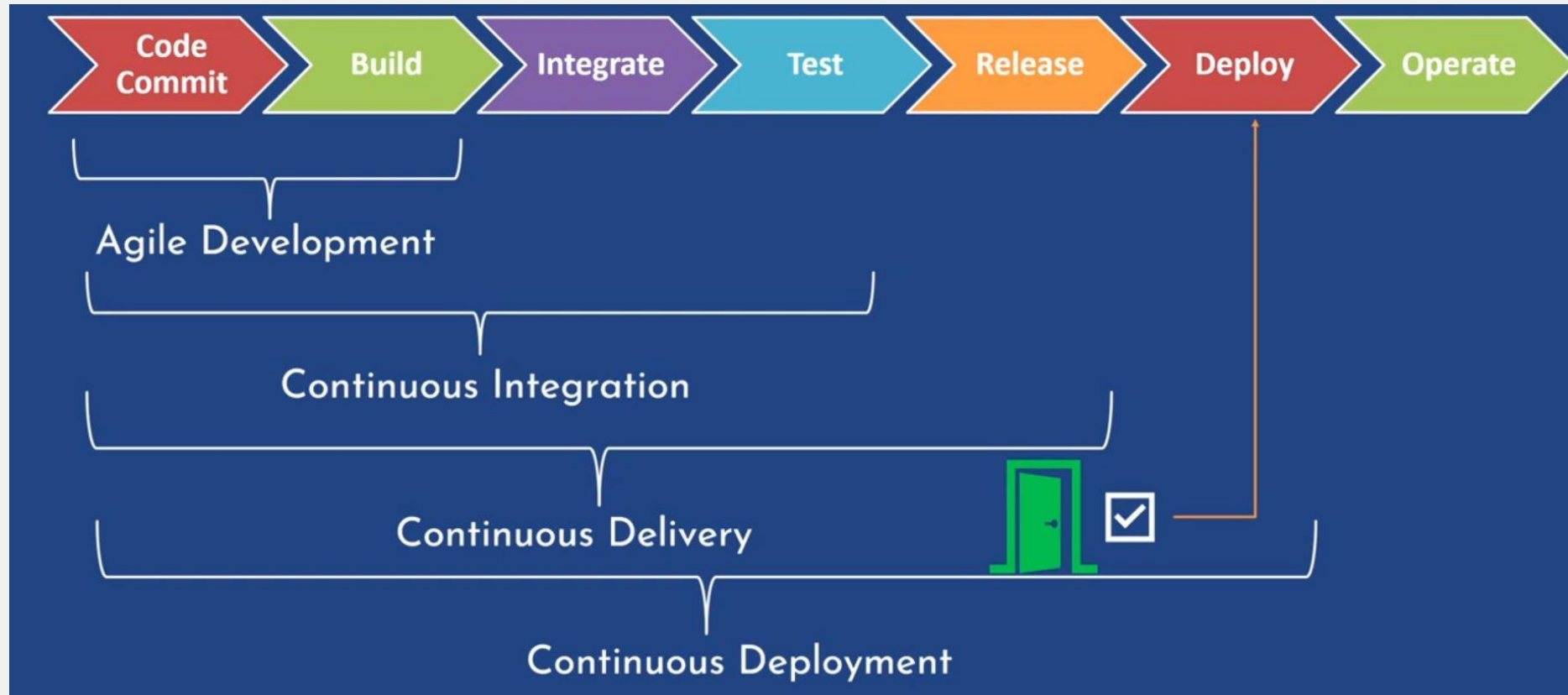


What is Agile Cybersecurity ?



Agile cybersecurity illustrated

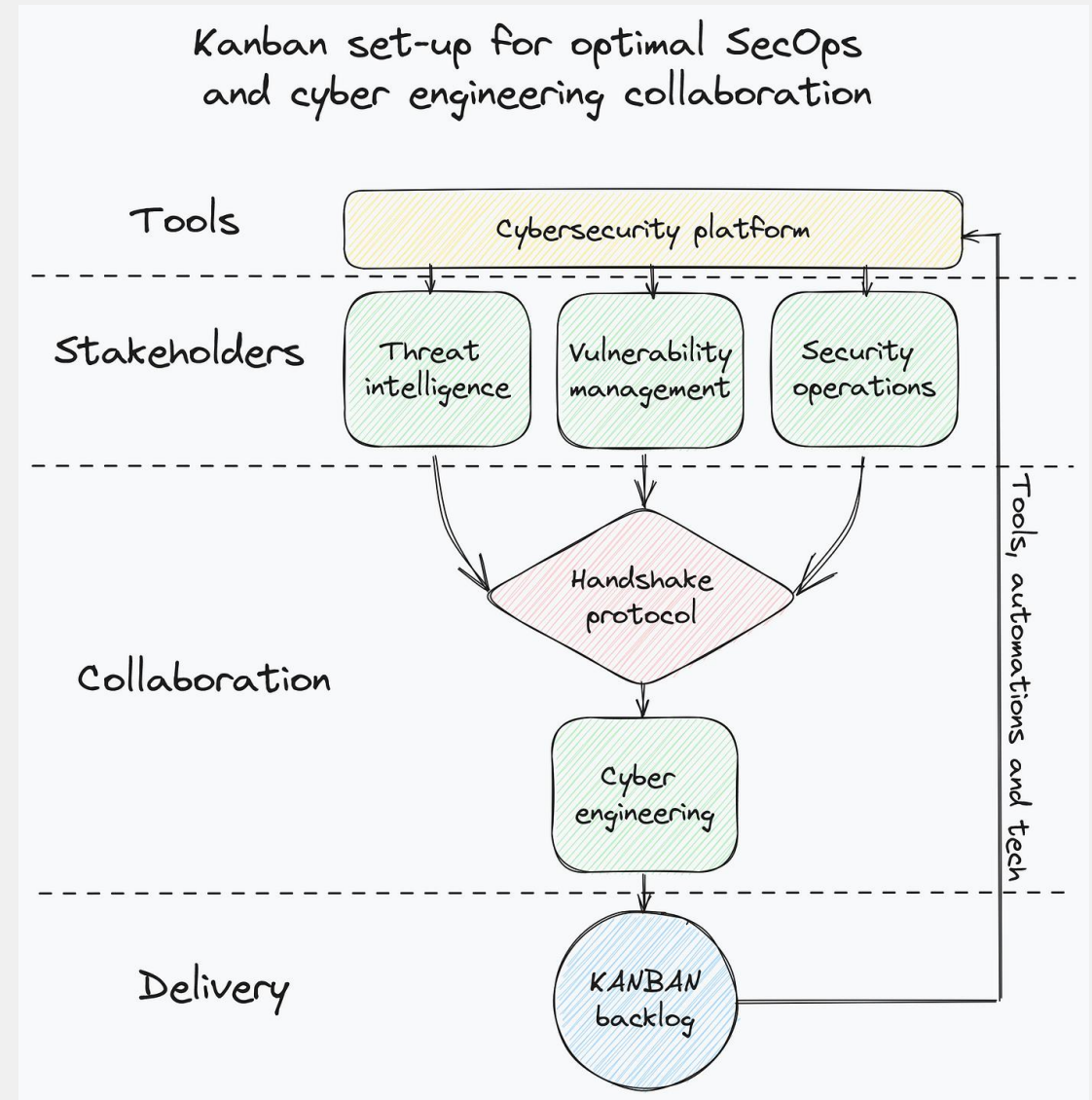
Agile cybersecurity, often referred to as “Agile Security” or “DevSecOps” (Development, Security, Operations), is an approach incorporating Agile principles and practices.



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

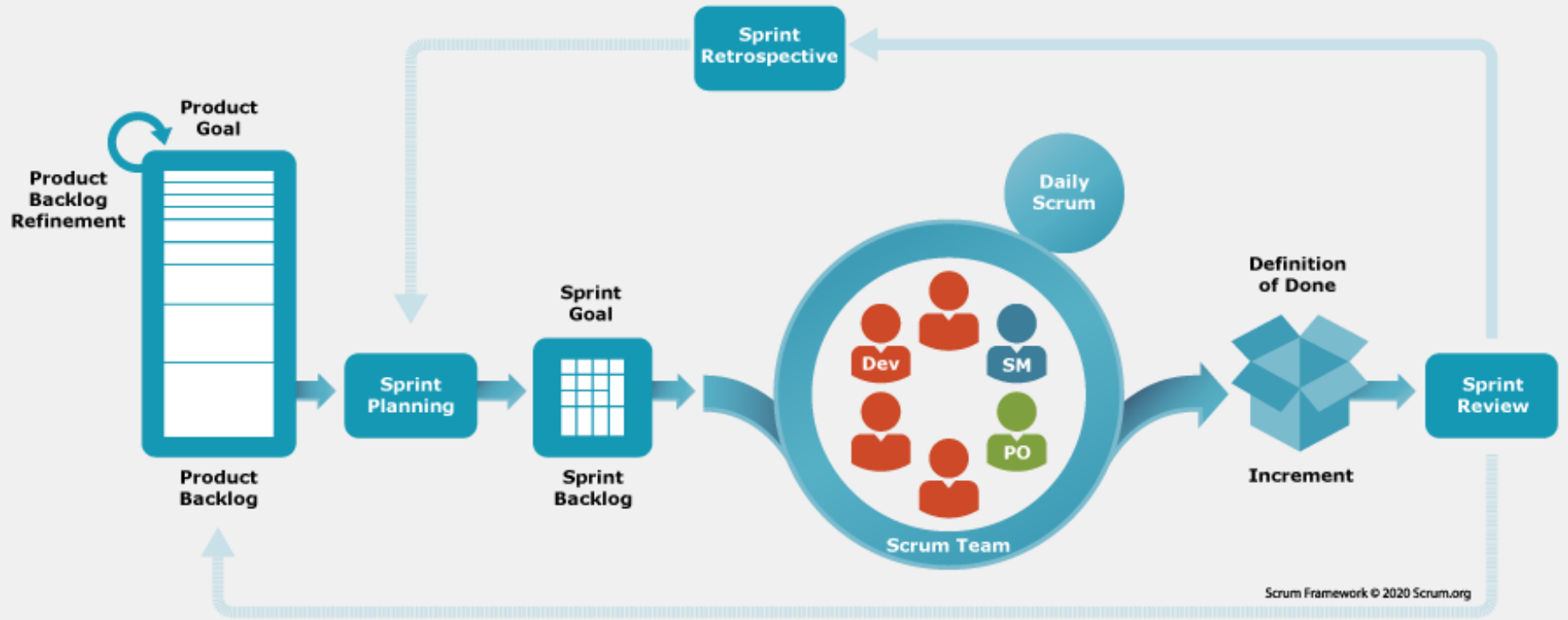
The five challenges:

- 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

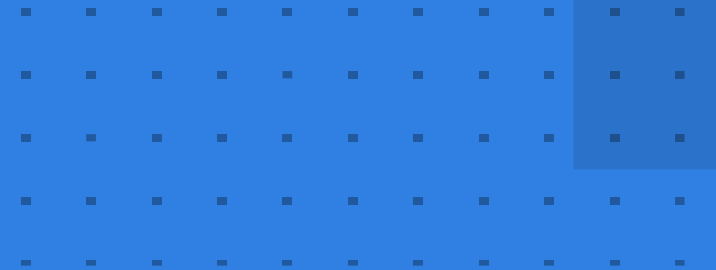


Agile cybersecurity pillars:

- 1: **Operating pillar**
- 2: Planning pillar
- 3: **Developing pillar**
- 4: Releasing pillar



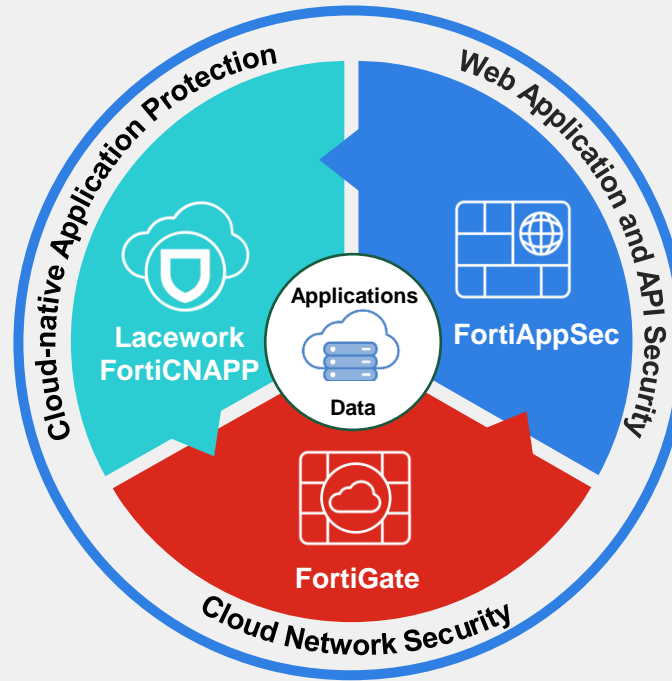
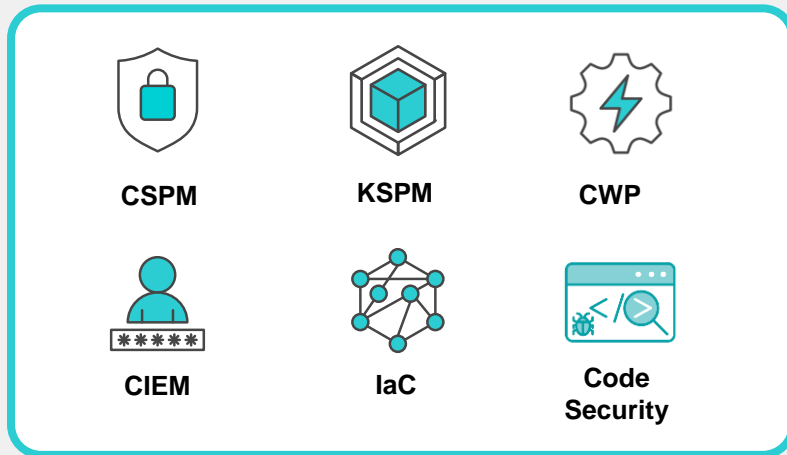
Let's Dive into Cloud Cybersecurity



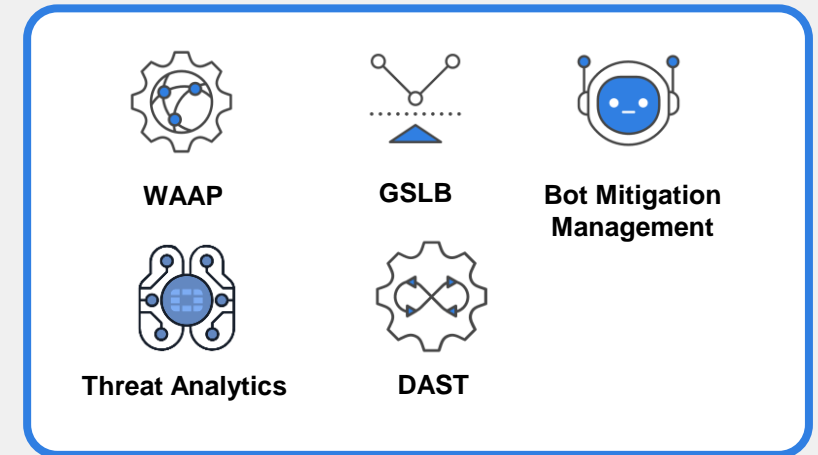
Comprehensive Integrated Code-to-Cloud Security

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.**



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



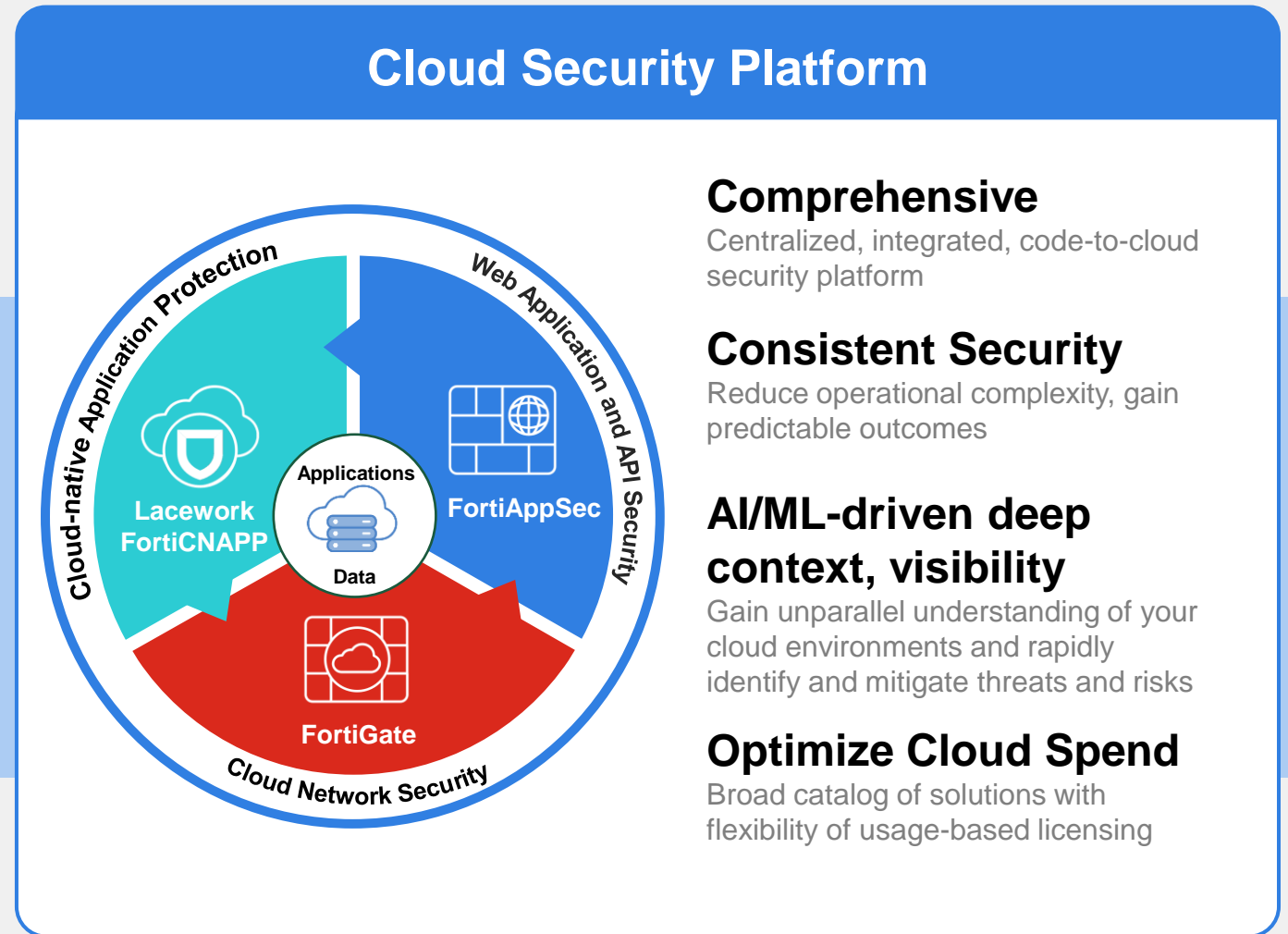
Achieve network visibility and enforcement of **consistent security policies** across private, public, and telco clouds.



Competitive Advantage of a Cloud Security Platform



Fragmented Cloud Security Challenges



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

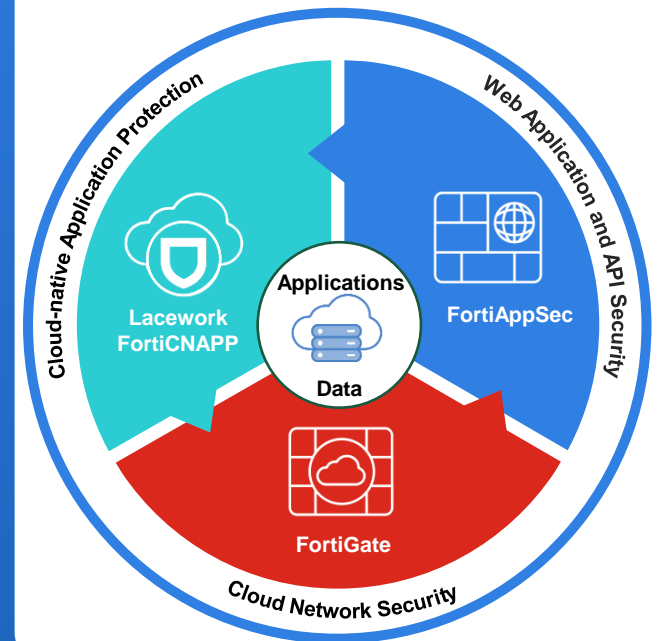
Reduce siloed, point products with integrated cloud platforms

3X

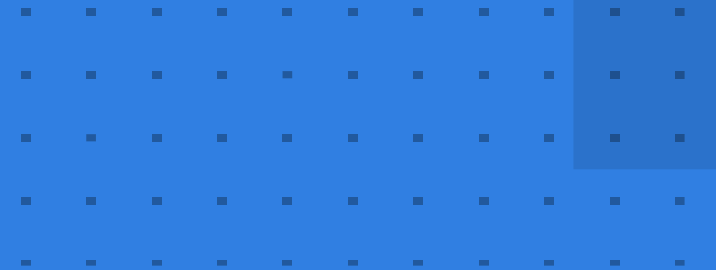
ROI by reducing point products

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.

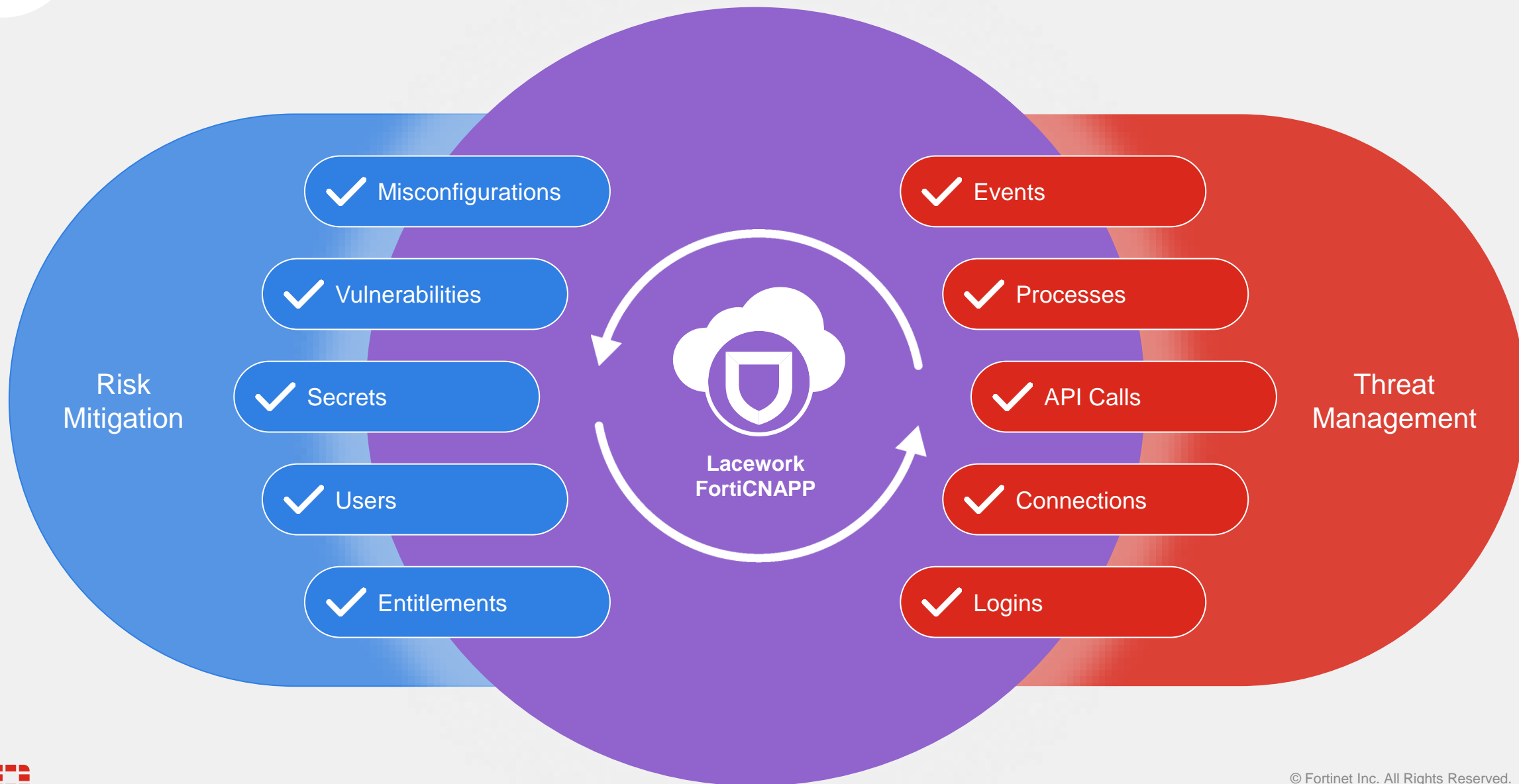


Reduce Threat Impact

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



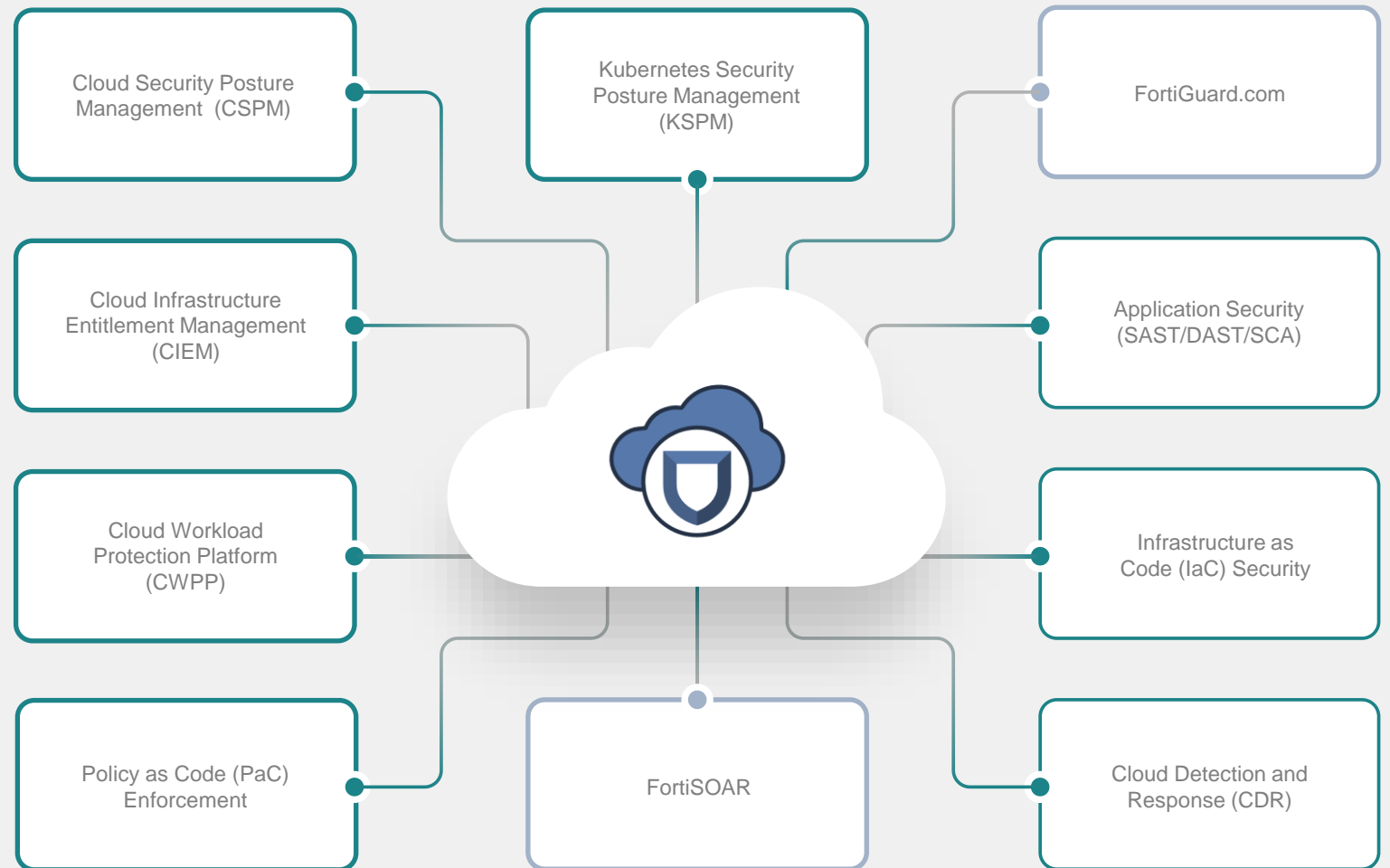
Lacework FortiCNAPP

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%

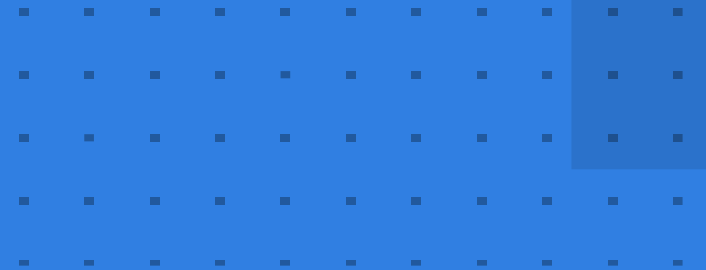
Reduction in SIEM
data ingestion cost



0-Day

Detection of active
threats and attacks

How does it look like?

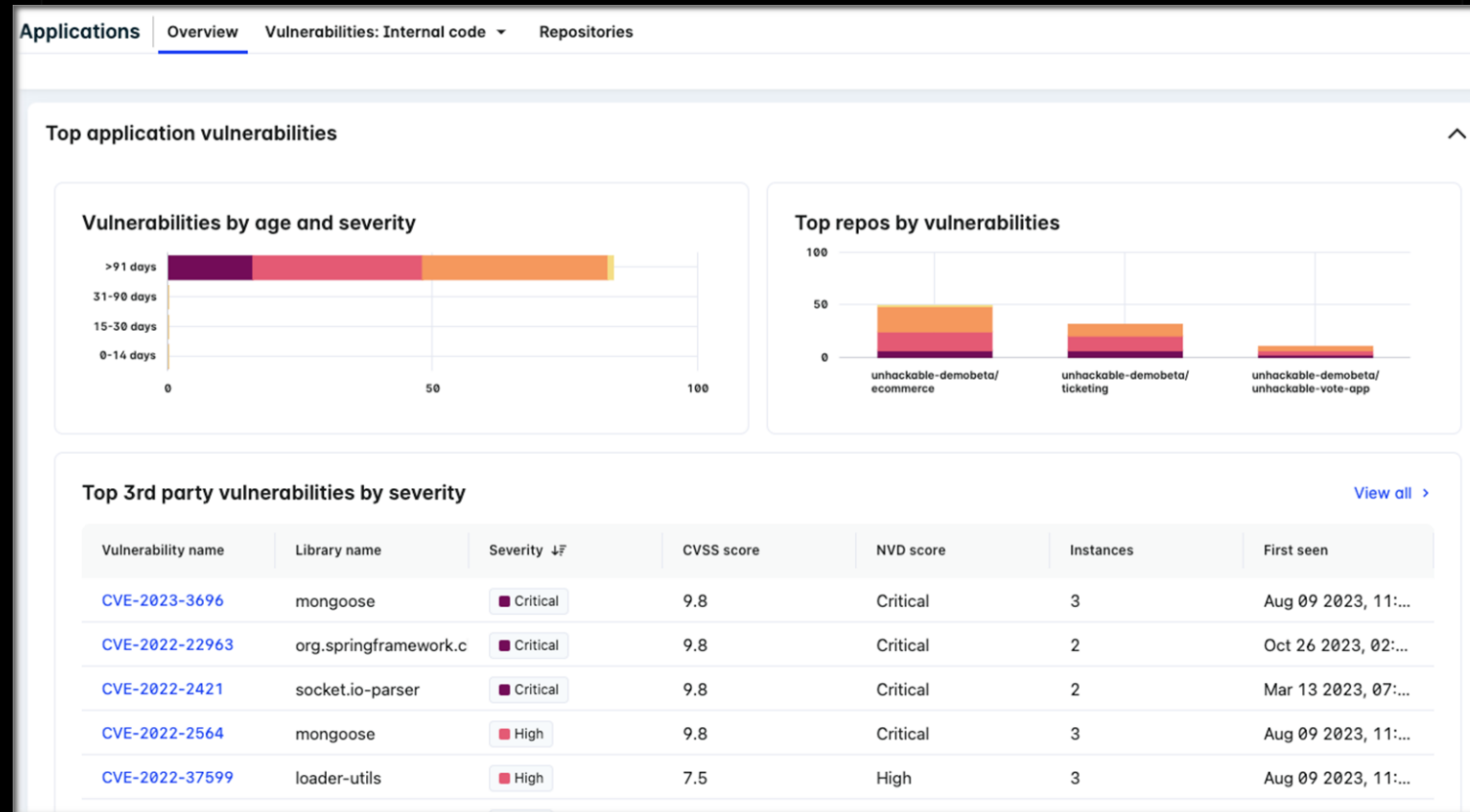




Shift Security Left to Reduce Risk and Remediation Costs

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

github-actions bot commented on Oct 8

Lacework Code Security found potential new issues in this PR.

▼ sca found potential 3 new issues

- [CVE-2021-45046](#) (ECommerce/pom.xml: org.apache.logging.log4j:log4j-core@2.15.0) ❌(critical)
 - ▼ More details
 - Package: org.apache.logging.log4j:log4j-core@2.15.0 (direct)
 - Vulnerability [CVE-2021-45046](#) (severity: critical, fixed in 2.16.0)
 - SmartFix: 2.17.1 (Minimal version with no known vulnerabilities)
 - Link: [CVE-2021-45046](#)
 - Sample path: [ECommerce@0.0.1-SNAPSHOT](#) -> org.apache.logging.log4j:log4j-core@2.15.0
 - ▼ Explanation: Why is this SmartFix recommended?

```
Sorted Version Graph for package pkg:maven/org.apache.logging.log4j/log4j-core@2.15.0
2.15.0 is vulnerable:
  critical  CVE-2021-45046      FixVersion= 2.16.0
  high     CVE-2021-45105      FixVersion= 2.17.0
  medium   CVE-2021-44832      FixVersion= 2.17.1
2.16.0 is vulnerable:
  high     CVE-2021-45105      FixVersion= 2.17.0
  medium   CVE-2021-44832      FixVersion= 2.17.1
2.17.0 is vulnerable:
  medium   CVE-2021-44832      FixVersion= 2.17.1
2.17.1 is not vulnerable
```

CVE fix version

2.16.0 - high CVE

FortiCNAPP fix

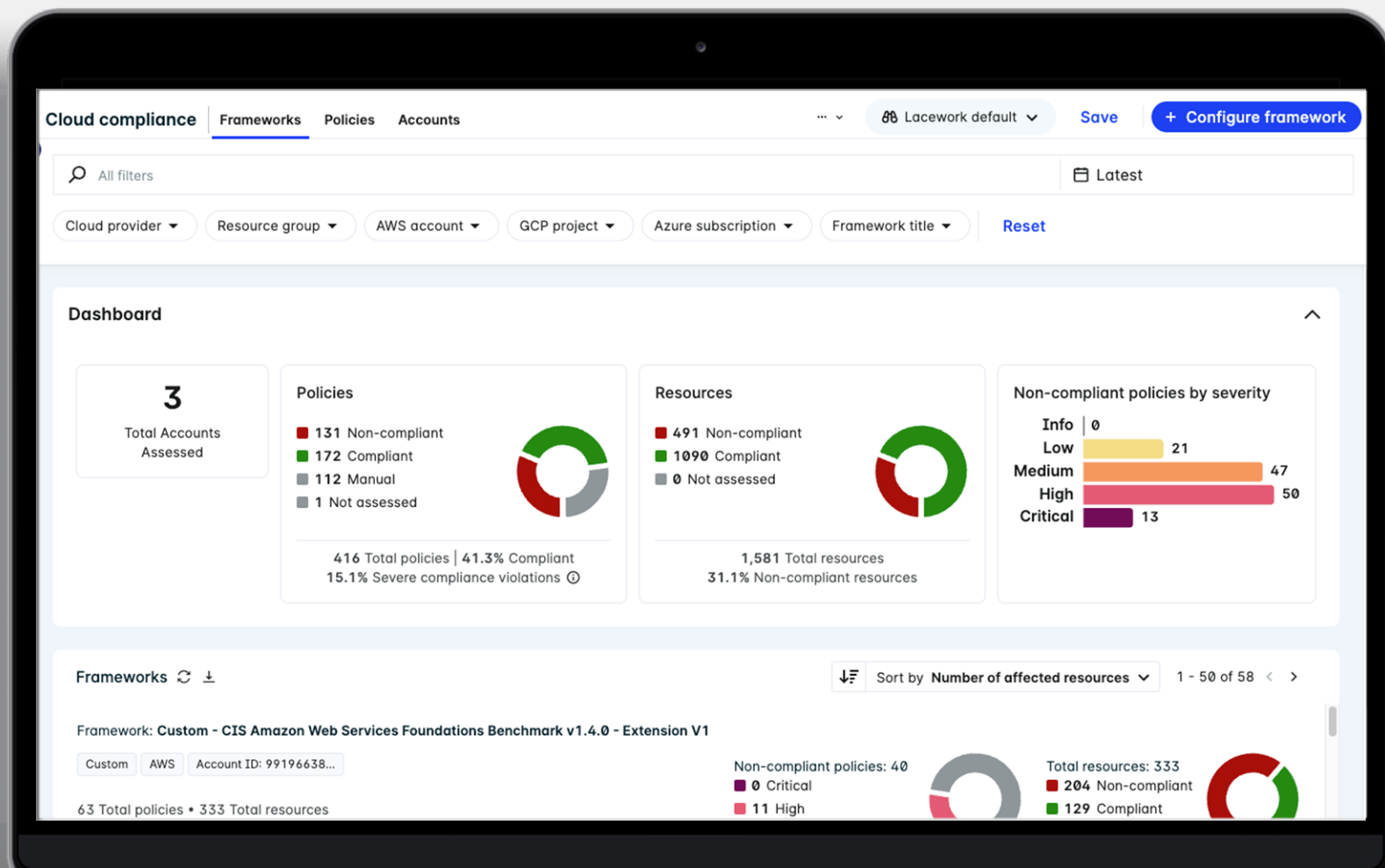




Gain Visibility of Cloud & K8s Configuration Risk

Security Posture Management CSPM and KSPM

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

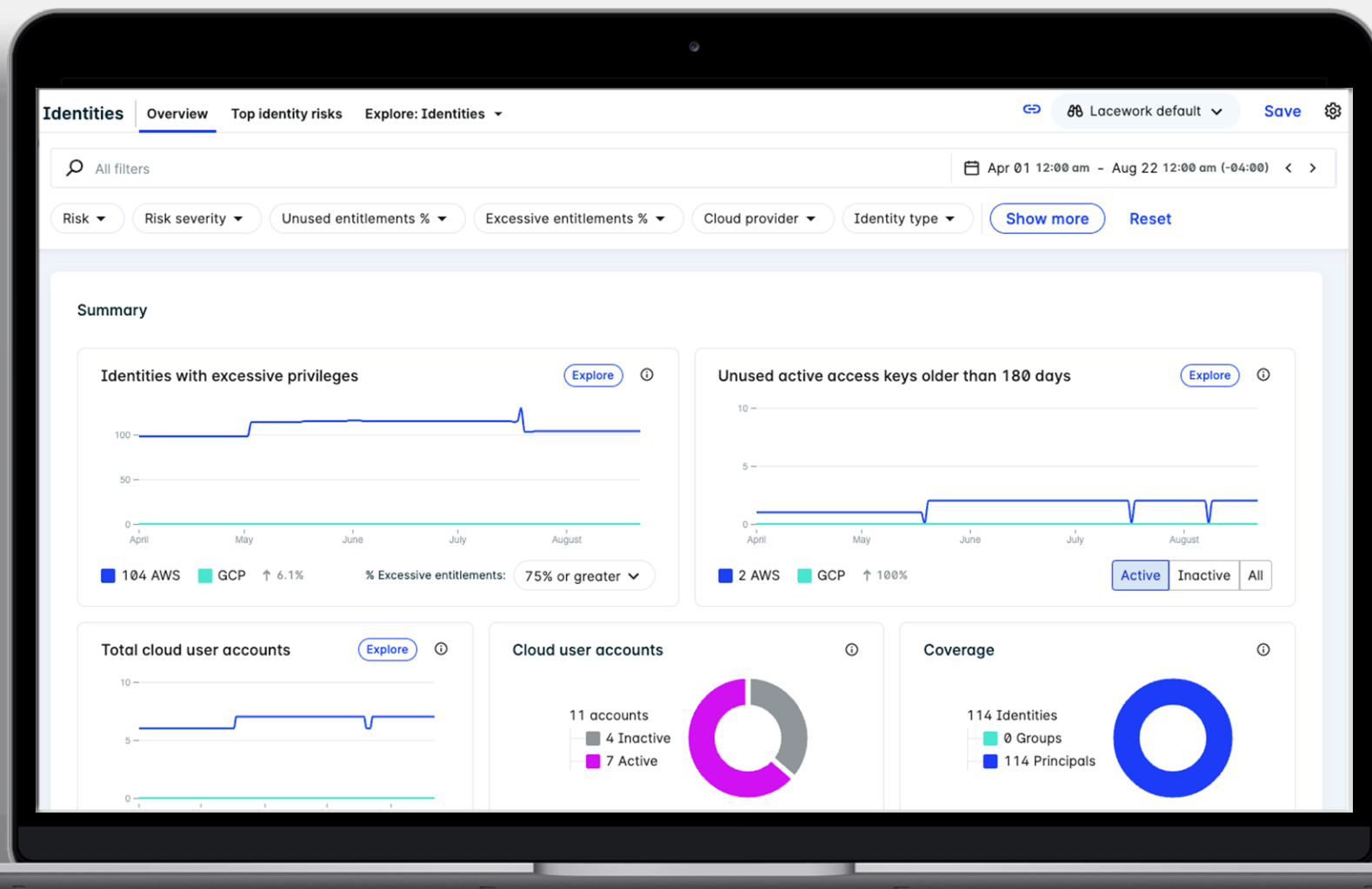




Reduce Identity Risk and Achieve Least Privilege Access

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

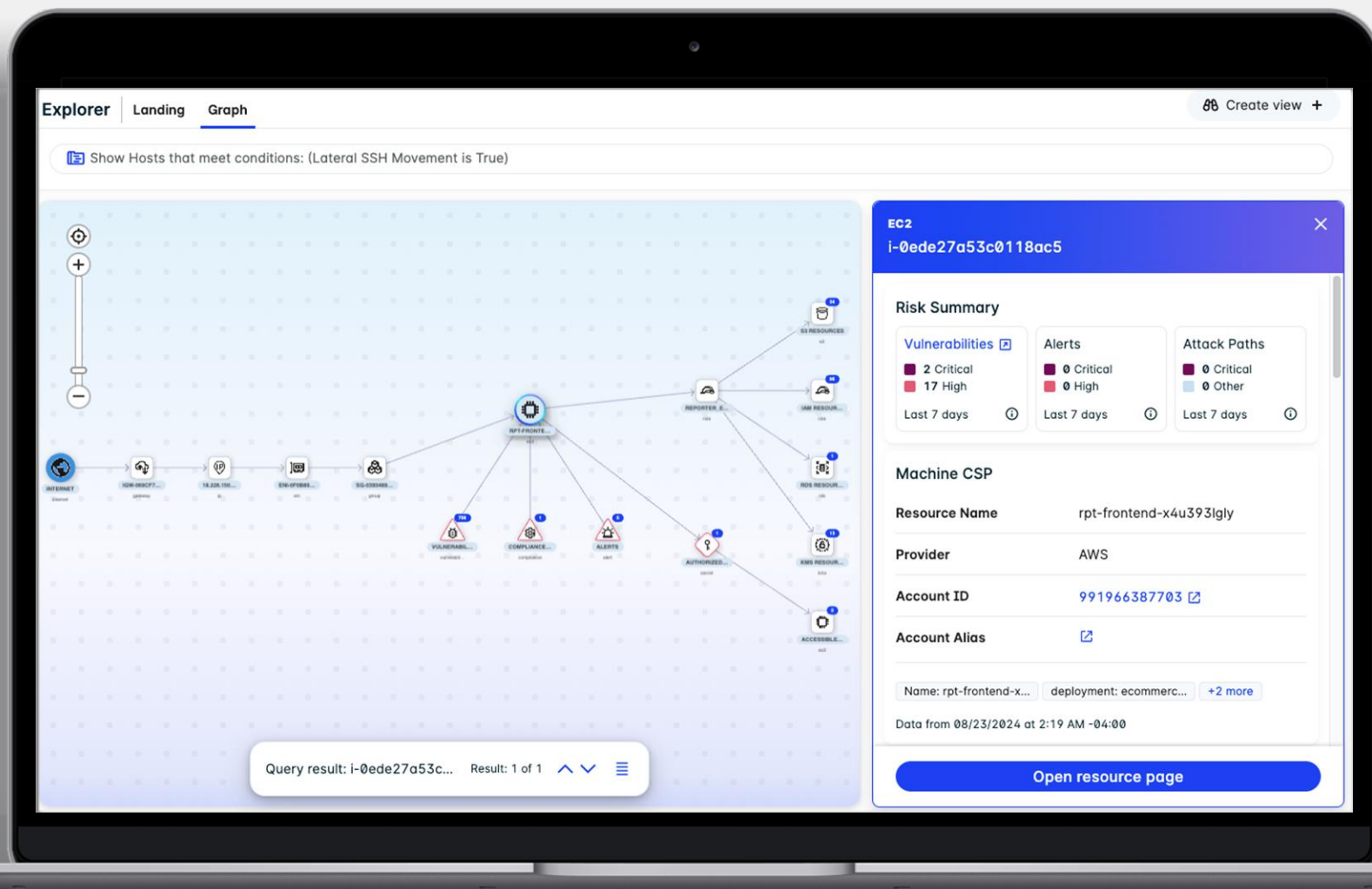




Prioritize Risks That Matter Most

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

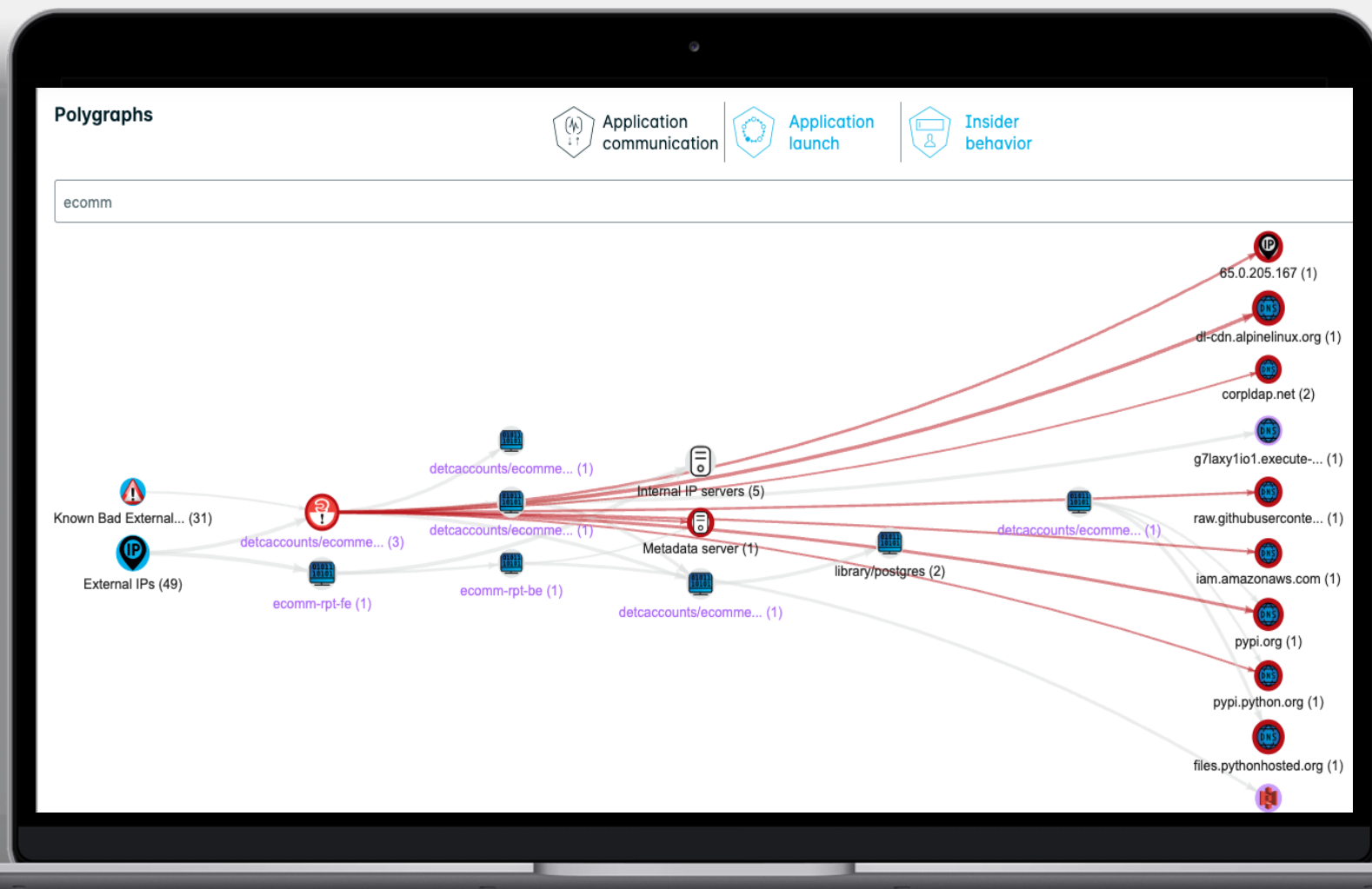




Identify Anomalies and Malicious Activity

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

Potentially compromised AWS keys ID: 82366
Alert modified: 07/22/2024 at 6:21 PM -04:00 ⓘ
Event activity window: 07/20/2024 at 1:28 AM -04:00 to 07/22/2024 at 5:00 PM -04:00 ⓘ

High AWS Composite Cloud Activity Internet Exposure: Unknown SEC-15867 Reconnaissance Active Scanning Vulnerability Scanning Resource Development +25 more

Details Exposure Investigation Events Related Alerts Remediation Integrations Timeline

Why
Alert Description
AWS credentials may have been compromised. The following entities are suspected. Users:
AssumedRole/991966387703:EKSNodeGroupRole ; Principal Ids:
AROA6N5ON3X3SUEYQ65Y6:i-046f6cf7b6e1cd734 ; Instance Ids: i-046f6cf7b6e1cd734 .

Supporting Facts ⓘ

- **Anomalous Activity (AWS)**
For user(s) AssumedRole/991966387703:EKSNodeGroupRole , one or more APIs are new including DescribeElasticGpus, DescribeHosts, GetSessionToken.
For user(s) AssumedRole/991966387703:EKSNodeGroupRole and this environment, one or more IPs are new including 87.249.139.165 ⓘ.
- **Third Party Qualified Findings**
Associated Amazon GuardDuty detections had the following ids:
arn:aws:guardduty:us-east-2:991966387703:detector/2ac8672e4fe1ed91df4c41d0a675bac6/finding/8ec86e1abe57a235dde84e399cfac
arn:aws:guardduty:us-east-2:991966387703:detector/2ac8672e4fe1ed91df4c41d0a675bac6/finding/6cc867525bd69b8a4336861e1098
arn:aws:guardduty:us-east-2:991966387703:detector/2ac8672e4fe1ed91df4c41d0a675bac6/finding/3cc86e0c0ef72f25528f6b9df21ca6
Associated Amazon GuardDuty detections had the following descriptions:
An EC2 instance has an unprotected port which is being probed by a known malicious host.

Lacework AI Assist^{beta} ... ? ×

Why is this alert important 👍 👎

This alert is important because it indicates that AWS credentials may have been compromised, which could allow unauthorized access to your AWS environment. Here are a few key reasons why this is a critical security concern:

1. **Unauthorized access:** Compromised credentials can be used by attackers to gain unauthorized access to your AWS resources, potentially leading to data breaches, data manipulation, or service disruptions.
2. **Sensitive API usage:** The alert mentions that new and sensitive APIs were used by the suspected users, such as DescribeElasticGpus, DescribeHosts, and GetSessionToken. These APIs could be used for discovery and further exploitation of your AWS infrastructure.
3. **Privilege escalation:** The alert indicates that privilege

Why is this alert important **Submit**



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

