Cloud-Native Application Protection Platform (CNAPP)

Introducing FortiCNAPP

FortiCNAPP helps quickly manage risk, rapidly detect and respond to active threats, boost developer productivity and increase security effectiveness.

Watch Now

Simplify and Strengthen Cloud Security

FortiCNAPP unifies fragmented tools into a single platform to simplify and strengthen cloud security. It empowers teams to maximize their impact on security with minimal time and effort by automatically connecting

risk insights with runtime threat data, ensuring they prioritize and address the most critical security risks and active threats.

Rapidly Detect and Mitigate Zero-Day Threats

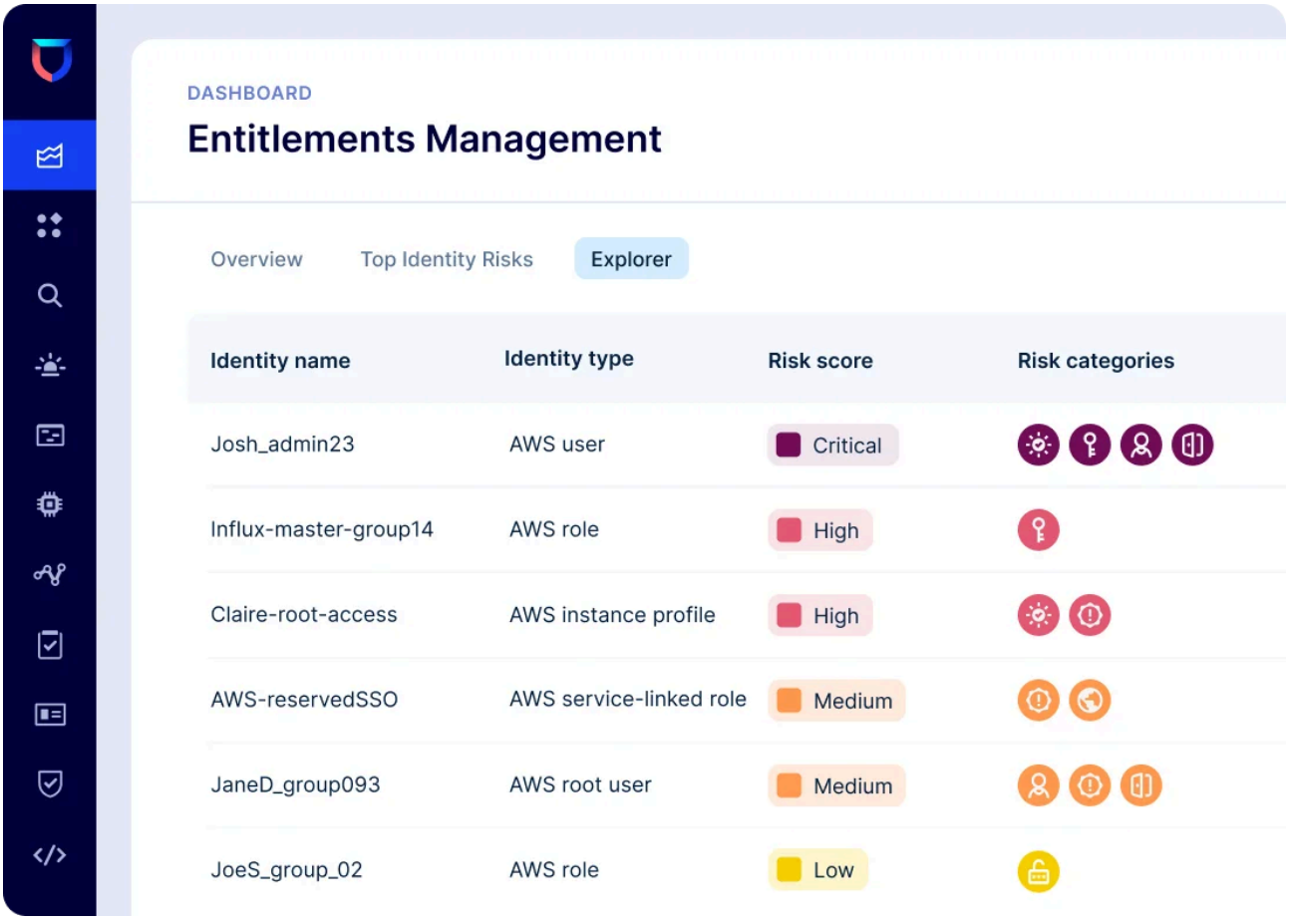
Continuously monitor workloads and detect unusual behavior without the need to write and maintain rules. Automatically discover early signs of compromised credential, ransomware, and cryptojacking attacks before their patterns are defined. Achieve faster identification of issues, quicker response times, and greater security efficacy with patented machine learning and integrations with the Fortinet Security Fabric and leading workflow tools.

[See it now: How to detect threats]

Prioritize What Matters Most

Quickly visualize complex relationships between entities, risks, and threats to gain deeper insight into potential attack paths. Understand the risk of lateral movement and privilege escalation by attackers. Instantly assess the exploitability and impact of critical vulnerabilities and misconfigurations. Boost operational efficiency and maximize the impact on security by effectively prioritizing the issues that matter most.

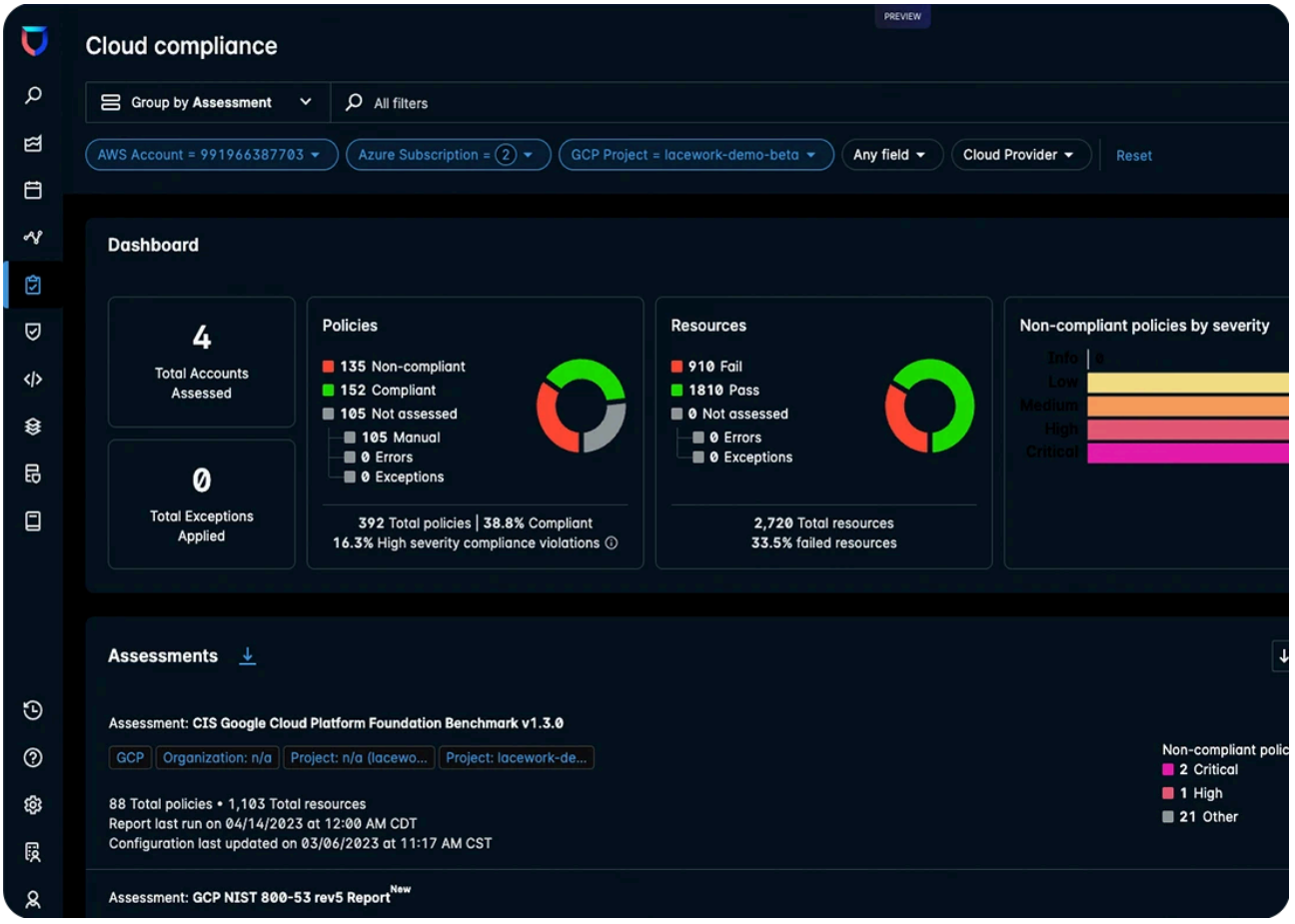
[See it now: How to prioritize risks]



Understand Which Cloud Identities Pose the Greatest Risk

Gain comprehensive and continuous visibility into all users, resources, groups, and roles across multiple cloud service providers. Automatically determine each identity's net-effective permissions and identify those with excessive privileges. Quickly prioritize the most at-risk identities with personalized risk scores based on multiple factors. Streamline permission right-sizing and accelerate least-privilege access with automated remediation guidance.

[See it now: How CIEM works]



Simplify and Accelerate Cloud Compliance

Automatically map cloud assets, configurations, and activity to compliance frameworks including PCI DSS, HIPAA, SOC 2, and ISO 27001. FortiCNAPP continuously assesses posture across AWS, Azure, and GCP, identifies misconfigurations, and prioritizes remediation efforts to reduce audit fatigue. With real-time policy checks, detailed reporting, and integration with the Fortinet Security Fabric, you can streamline audits, minimize risk, and confidently prove compliance at any scale.

[See it now: How to achieve continuous compliance]

Features and Benefits

With FortiCNAPP, cloud and security operations teams benefit from reduced complexity, greater visibility, and enhanced security effectiveness – all through a single unified, AI-driven platform.

Gain unmatched visibility

Achieve proactive, stronger, and more efficient security by understanding how everything is interconnected from code to cloud

Unify cloud security

Simplify and strengthen security with a unified platform that reduces detection, investigation, and response times

Detect Zero-Day Threats

Quickly discover active threats like compromised credentials, ransomware, and cryptojacking before their attack patterns are defined

Enhance anomaly detection

Detect unusual behavior and reduce alert noise without the need to write or maintain endless, complex rule sets

Prioritize risk

Maximize security outcomes with minimal time and effort by gaining insights into the exploitability and impact of each risk and threat

Stay compliant

Ease and streamline continuous cloud compliance and keep pace with changing regulatory requirements and industry best practices

Kubernetes (K8s) Security

Reduce the risk of misconfigured Kubernetes services and continuously monitor Kubernetes environments for abnormal and risky behavior

Code Security

Shift security left by finding and fixing open-source vulnerabilities, first-party code weakness, and misconfigured Infrastructure-as-Code

Case Studies & Awards

Careem

Industry-Leading Delivery App, Careem, Boosts DevSecOps Efficiency with Fortinet Cloud Security

Coveo

How Coveo Gained Cloud Visibility and Reduced Risk with FortiCNAPP

[AOK Systems GmbH]

AOK Systems GmbH Efficiently Secures Sensitive Healthcare Data with FortiCNAPP

2025 SC Award – Best Cloud Workload Protection Solution

FortiCNAPP has earned the 2025 SC Award for Best Cloud Workload Protection Solution, a prestigious honor recognizing excellence in securing cloud-native workloads. This award offers third-party validation that Lacework FortiCNAPP is an effective, top-tier CNAPP.

[Read the Article]

Cloud Service Providers

Microsoft Azure

Gain nonstop protection and control checks with comprehensive, continuous, and end-to-end Azure security.

Google Cloud

Streamline continuous compliance, manage vulnerabilities, and detect threats in Google Cloud with more automation.

Resources

Resource Type

eBooks

Data Sheets

Overview

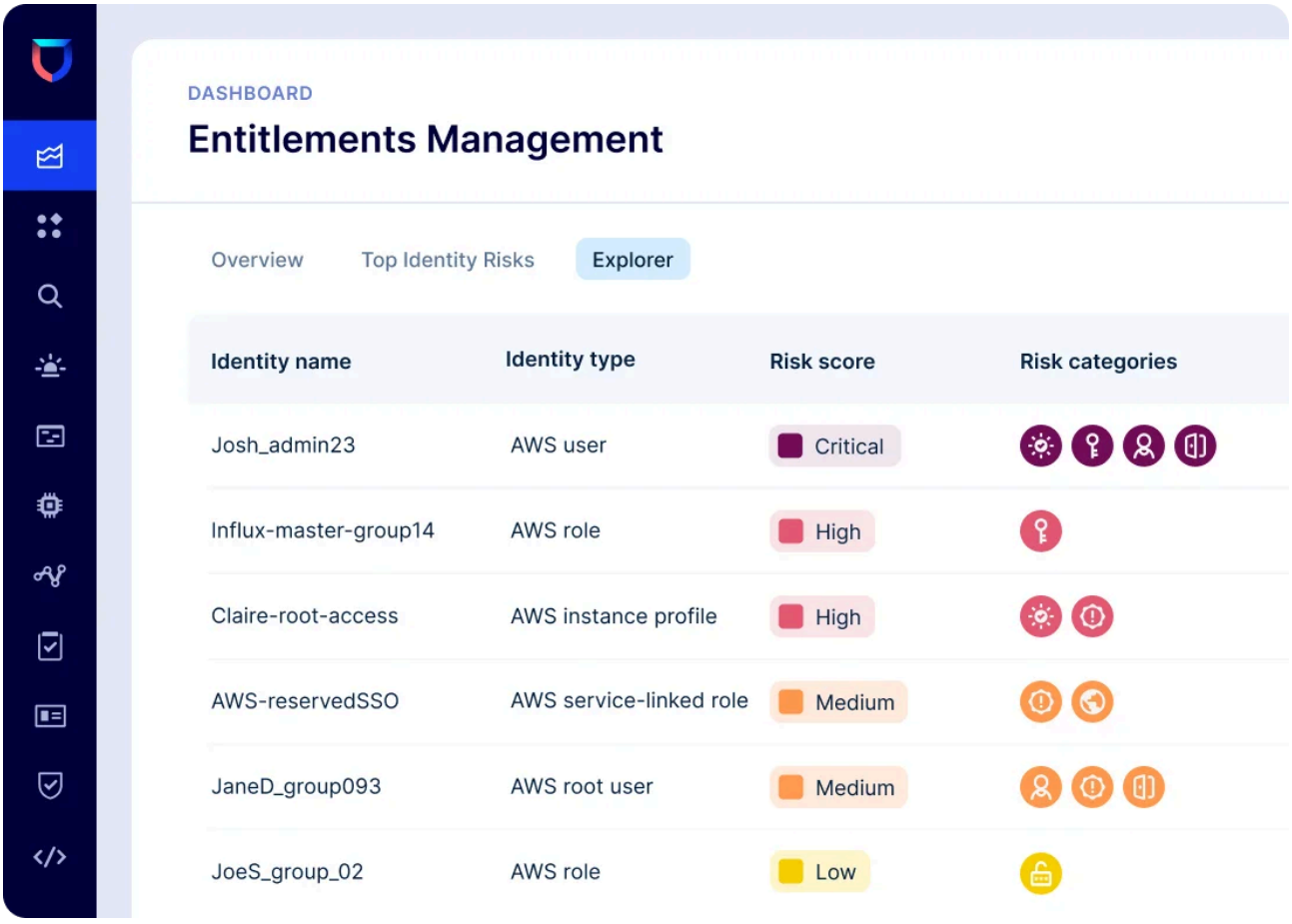
Solution Briefs

Schedule a FortiCNAPP Demo

Cloud security is fundamentally a data problem. If your current rules-driven cloud security solution can’t scale, then discover how you can automate security and compliance across AWS, Azure, Google Cloud, and private clouds with FortiCNAPP.

Watch our demo and see how we can help you:

- Investigate threats 80% faster
- Consolidate your security tools
- Eliminate false positives by 95%
- Reduce critical security alerts to about 1.4 per day



Source: https://www.lacework.com/blog/detecting-ai-resource-hijacking-with-composite-alerts