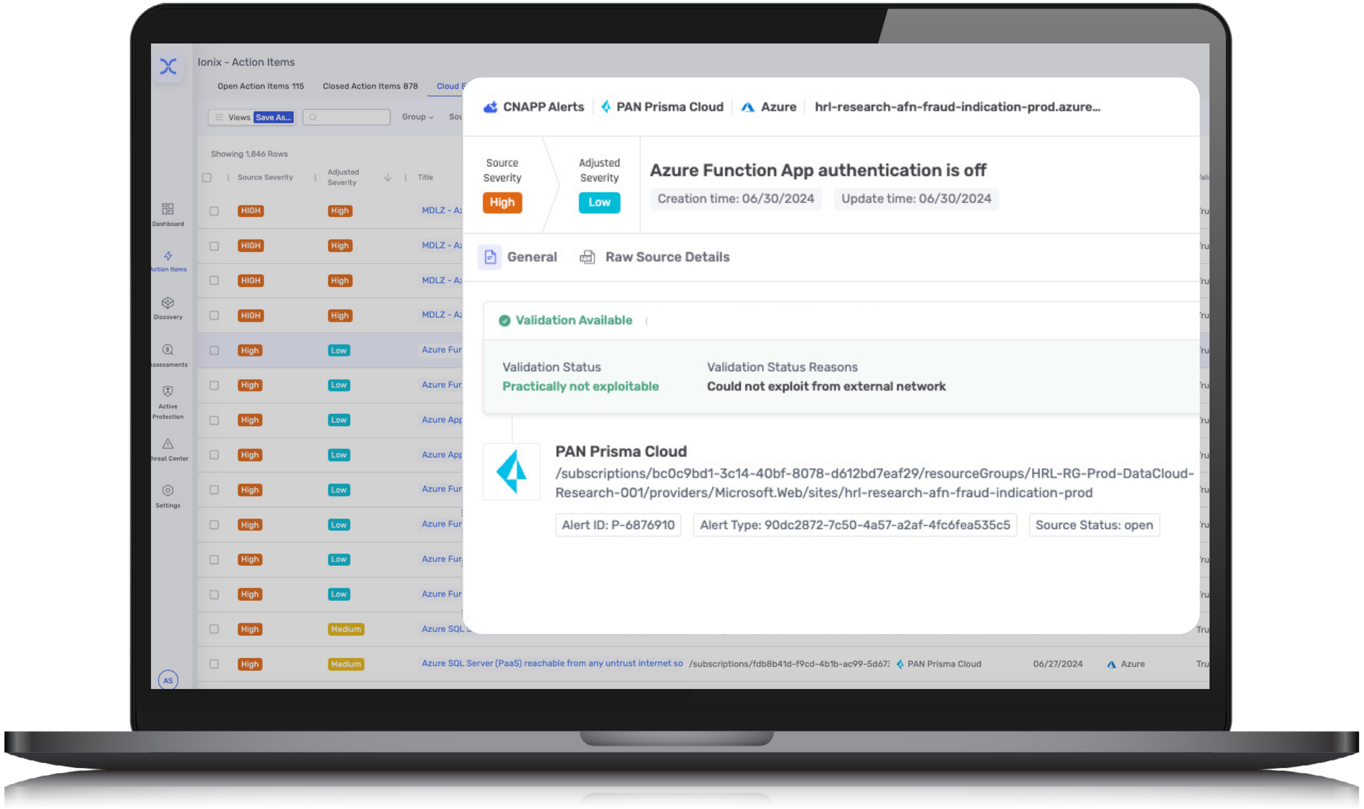
IONIX

FEATURE OVERVIEW

CLOUD EXPOSURE VALIDATOR

Validate and prioritize cloud security findings (vulnerabilities and misconfigurations) based on real-world exposure, enabling your team to focus on actual threats rather than theoretical risks.

- **Gain instant visibility** into true CSPM alert risk levels and their potential business impact
- **Drive security decisions** based on validated exposure data rather than theoretical CVE scores
- **Unify security operations** by removing communication barriers between teams



Showing 1,846 Rows

□	Source Severity	Adjusted Severity	Title					
□	HIGH	High	MDLZ - Az					Tru
□	HIGH	High	MDLZ - Az					Tru
□	HIGH	High	MDLZ - Az					Tru
□	HIGH	High	MDLZ - Az					Tru
□	High	Low	Azure Fur					Tru
□	High	Low	Azure Fur					Tru
□	High	Low	Azure App					Tru
□	High	Low	Azure App					Tru
□	High	Low	Azure Fur					Tru
□	High	Low	Azure Fur					Tru
□	High	Low	Azure Fur					Tru
□	High	Low	Azure Fur					Tru
□	High	Medium	Azure SQL S					Tru
□	High	Medium	Azure SQL Server (PaaS) reachable from any untrust internet so	/subscriptions/fdb8b41d-f9cd-4b1b-ac99-5d67:	PAN Prisma Cloud	06/27/2024	Azure	Tru

CNAPP Alerts | PAN Prisma Cloud | Azure | hrl-research-afn-fraud-indication-prod.azure...

Source Severity: High
Adjusted Severity: Low

Azure Function App authentication is off

Creation time: 06/30/2024
Update time: 06/30/2024

General | Raw Source Details

Validation Available

Validation Status: Practically not exploitable

Validation Status Reasons: Could not exploit from external network

PAN Prisma Cloud

/subscriptions/bc0c9bd1-3c14-40bf-8078-d612bd7eaf29/resourceGroups/HRL-RG-Prod-DataCloud-Research-001/providers/Microsoft.Web/sites/hrl-research-afn-fraud-indication-prod

Alert ID: P-6876910
Alert Type: 90dc2872-7c50-4a57-a2af-4fc6fea535c5
Source Status: open

THE VULNERABILITY MANAGEMENT CHALLENGE

As of October 2024, the National Vulnerability Database (NVD), a government repository of standards-based vulnerability management data, has recorded over 31,000 vulnerabilities, with approximately 18,469 still awaiting analysis, suggesting this number is likely to increase. This significant rise in reported vulnerabilities can be attributed to several factors, including the widespread use of open-source software and the move to cloud computing in most enterprises. The adoption of cloud technologies has led to increasingly complex modern software systems, creating more opportunities for vulnerabilities to emerge.

NEW TOOLS TO SOLVE OLD PROBLEMS

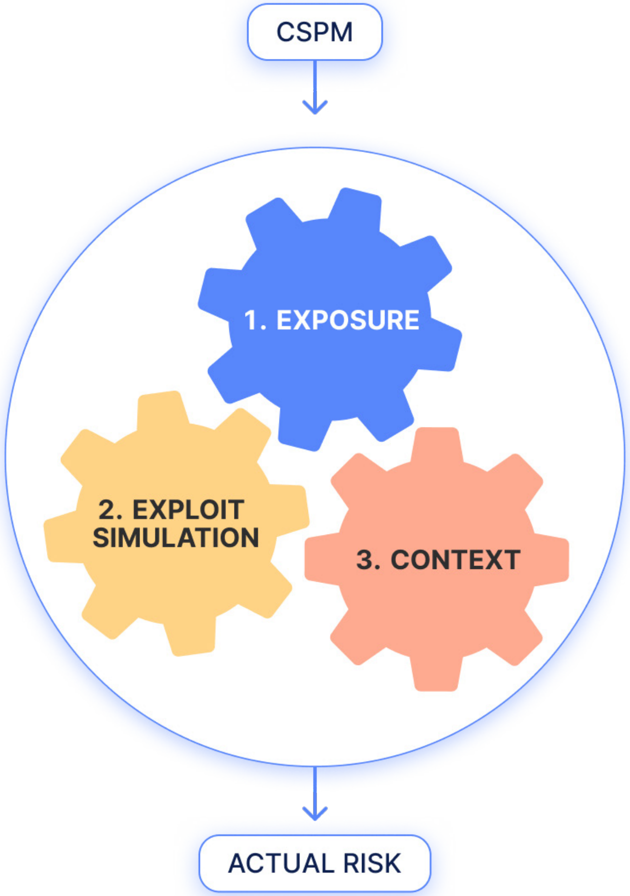
Cloud Security Posture Management (CSPM) has emerged as the primary tool for monitoring and managing risks in cloud deployments. These solutions are designed to assess cloud environments, identify vulnerabilities and cloud misconfigurations, and prioritize risks based on various parameters that differ among vendors. CSPM provides context to help users better understand the specific risks posed by security findings within their unique cloud environments, offering insights relying on generic severity scores like CVSS and EPSS with internal factors for prioritization, such as identity. However, despite the sophistication of these tools, the sheer volume and rapid increase of vulnerabilities in cloud environments presents a significant challenge. Security teams find themselves overwhelmed with alerts, as even the most advanced CSPM solutions struggle to keep pace with the exponential growth of findings.

A NEW APPROACH

A new methodology is required that can effectively reduce the noise and allow security teams to focus on issues that represent real danger and exposure, taking into consideration the perspective and techniques of potential attackers. Rather than simply chasing vulnerabilities based on generic metrics, this approach prioritizes threats ***based on their practical exploitability and potential impact in the context of the specific environment and attacker behavior.***

IONIX CLOUD EXPOSURE VALIDATOR: A THREE STEP APPROACH TO VALIDATION

IONIX integrates with CNAPP (Cloud Native Application Protection Platform) systems and reviews the findings of leading vendors such as Wiz and Palo Alto Prisma Cloud. The IONIX Cloud Exposure Validator then enriches the findings with our proprietary external exposure validation, taking exploitability and asset context into account, and then validates risk to determine if attackers can exploit vulnerabilities from outside the organization.



EXPOSURE

CAN A SPECIFIC ASSET BE REACHED FROM OUTSIDE THE ORGANIZATION?

As part of the integration, IONIX Cloud Exposure Validator correlates the cloud workload from the CSPM with the Fully Qualified Domain Name (FQDN) it represents in the IONIX platform. This allows IONIX to determine whether specific CSPM findings are exposed to potential attacks and therefore represent a real danger, or if they are not exposed and can be addressed later.

EXPLOIT SIMULATION

CAN A SPECIFIC ASSET BE EXPLOITED?

IONIX Cloud Exposure Validator simulates a non-intrusive, risk-free CVE exploit based on the CSPM findings to validate if CVEs can be exploited by attackers from outside the organization and therefore pose a real threat.

A CSPM finding initially classified as high or medium may be escalated to critical if it is exposed and has validated, exploitable vulnerabilities. Such findings should be treated urgently.

This reclassification ensures that security teams prioritize addressing vulnerabilities and misconfigurations that represent real-world risks, focusing resources on the most pressing issues first.

CONTEXT

WHAT IS THE TRUE RISK IN CONTEXT OF A GIVEN ASSET?

IONIX Cloud Exposure Validator can further refine security assessment by placing CSPM findings in contextual perspective thereby evaluating true risk. Context can be applied in a number of ways, for example:

- A finding might be escalated from non-critical to critical if the cloud workload has an exploitable vulnerability that is externally accessible and shows significant blast radius damage potential.
- A finding might be de-escalated from critical to non-critical if the cloud workload has a vulnerability or misconfiguration that can't be exploited from the outside.

BRIDGING THE GAP BETWEEN CSPM AND SECURITY CONTROLS

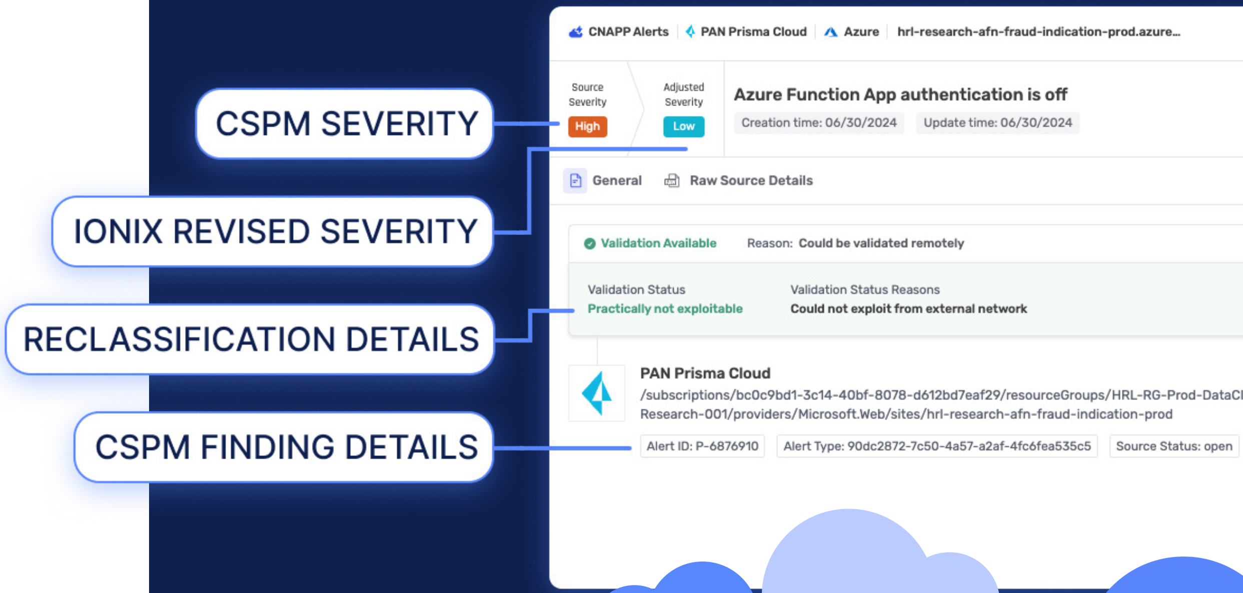
Current CSPMs face significant challenges in accurately identifying and validating implemented security controls across cloud environments. While detecting basic cloud misconfigurations, CSPMs often fail to comprehend deployed security layers, creating a critical recognition gap.

For instance, CSPMs typically flag any internet-facing resource as high-risk, unable to recognize when that resource is protected by enterprise-grade security controls like next-generation firewalls or WAFs. This limitation leads to a flood of false positives where CSPMs raise alerts about "exposed" resources that are well-protected by multiple security layers. This disconnect between CSPM findings and actual security posture forces security teams to manually validate each alert, consuming valuable time that could be better spent addressing genuine security gaps.

IONIX: MOVING FROM VULNERABILITY TO EXPLOITABILITY

The IONIX Cloud Exposure Validator marks an evolution in vulnerability management. By shifting the focus from mere vulnerability identification to a more nuanced understanding of exploitability, it addresses the core challenges faced by vulnerability teams today. This tool empowers security practitioners to move beyond the overwhelming noise of countless alerts, providing a clear understanding of what truly matters.

As cyber threats evolve, an approach that focuses on validated exploitability in context is crucial for staying ahead of attackers and maintaining a robust defense.



hrl-research-afn-fraud-indication-prod.azure...

Source Severity: High

Adjusted Severity: Low

Azure Function App authentication is off

Creation time: 06/30/2024 | Update time: 06/30/2024

Validation Available | Reason: Could be validated remotely

Validation Status: Practically not exploitable

Validation Status Reasons: Could not exploit from external network

PAN Prisma Cloud

/subscriptions/bc0c9bd1-3c14-40bf-8078-d612bd7eaf29/resourceGroups/HRL-RG-Prod-DataCl
Research-001/providers/Microsoft.Web/sites/hrl-research-afn-fraud-indication-prod

Alert ID: P-6876910 | Alert Type: 90dc2872-7c50-4a57-a2af-4fc6fea535c5 | Source Status: open

THE TRANSITION FROM VULNERABILITY TO EXPLOITABILITY IS NOT JUST ABOUT EFFICIENCY; IT'S ABOUT EFFECTIVENESS. IT ALLOWS VULNERABILITY TEAMS TO:

1. Prioritize threats based on their actual potential for exploitation
2. Allocate resources more strategically to address the most critical risks
3. Gain a more accurate picture of their organization's true security posture

GET STARTED TODAY

Contact our team to get a free scan.

Get a free scan | Learn more at ionix.io

Feature Overview: Cloud Exposure Validator

IONIX