

Palo Alto Networks Shifts Left with Prisma Cloud 3.0

By [Ankur Shah](#)

Nov 16, 2021 ⌚ 8 minutes 👁 32963 views

Cloud Infrastructure Entitlement Management

Cloud Native Security Platform

Cloud Network Security

Cloud Posture Security

Uncategorized

Bridgecrew

Cloud Infrastructure

Cloud Native Security Platform

IaC

Ignite '21

Prisma Cloud

Delivering the Industry's First Integrated Platform to Secure the Full Application Lifecycle

New innovations enable organizations to integrate security from code to runtime with a single solution.

If enterprises and governments can agree on anything, it may be that cybersecurity is the subject of intense global focus at the moment. An ongoing stream of high-profile attacks spanning ransomware, malware in the supply chain, data leaks and more, are pushing public and private entities to adopt more proactive strategies for securing cloud infrastructure.

Gartner recently stated that "By 2023, 70% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 40% in 2020." Moreover, Palo Alto Networks Unit 42 Cloud Threat Researchers found that between April and June 2020, **cloud security incidents increased** by an astounding 188%, and some industries saw increases of more than 400%.

The challenge in securing these cloud environments stems from the nature of the cloud itself. Workloads and resources in the cloud are broadly distributed and highly ephemeral. One new cloud account connects with workloads, applications and data, where each point presents potential attack vectors.

In order to secure cloud native applications and infrastructure, organizations need to adapt to be more agile and integrated. They need to be able to proactively address threats beginning in development, and provide continuous security along the application lifecycle all the way through to runtime environments. In order to achieve this agility, they need new tools that are purpose-built for cloud native environments, which can span the full software development lifecycle and provide critical security information at the right point and right time.

This requirement is exactly what **Prisma Cloud, our Cloud Native Security Platform**, was built to address. With Prisma Cloud, organizations can leverage a single solution to protect their environments and applications at runtime, while also integrating security across their development environments and tools.

Today we're excited to announce Prisma Cloud 3.0, providing customers five new innovations for securing cloud native applications:

- **Infrastructure as Code (IaC) Security:** Addressing cloud risk earlier to reduce the burden on both developers and security teams. With Prisma Cloud IaC Security, IaC scanning and code fixes are embedded directly into



Orca Security Ltd.
Exhibit 2135
Wiz v. Orca
IPR2024-01109, -01190, -01191
Ex. 2135-001

Today we're excited to announce Prisma Cloud 3.0, providing customers five new innovations for securing cloud native applications:

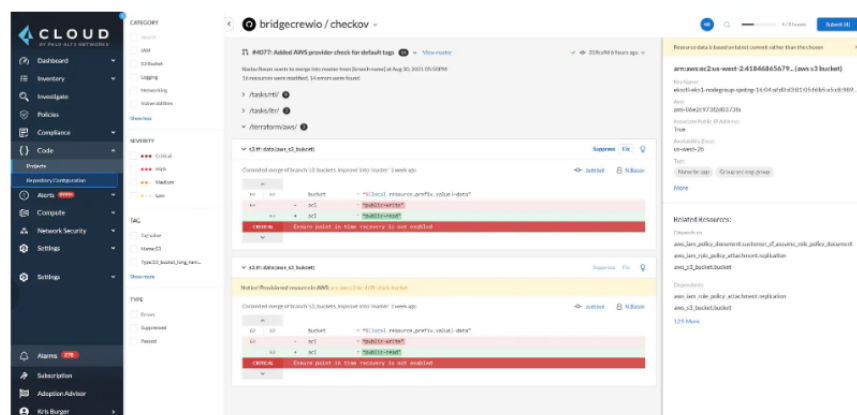
- **Infrastructure as Code (IaC) Security:** Addressing cloud risk earlier to reduce the burden on both developers and security teams. With Prisma Cloud IaC Security, IaC scanning and code fixes are embedded directly into developer tools across the development lifecycle.
- **Agentless Security for Flexible Cloud Workload Protection:** Providing visibility into an organization's cloud workload and application risks to complement existing agent-based protection.
- **Cloud Infrastructure Entitlement Management for Azure:** Net-effective permissions analysis and Azure Active Directory integration extend our existing IAM Security capabilities beyond AWS.
- **Pre-Defined Rules and Automated App Profiling for Identity-Based Microsegmentation:** Including pre-defined rules and automated policy creation to simplify and accelerate any microsegmentation adoption.
- **Adoption Advisor Dashboard:** Helping organizations operationalize Prisma Cloud with a dashboard that provides guidance on how to discover and unleash the power of the product as well as measure the implemented value.
- **Rapid Risk Discovery:** Reducing the time needed to identify and remediate misconfigurations from hours to minutes by detecting event-driven configuration changes as they occur, instead of solely relying on the more traditional polling architecture.



Cloud Code Security: Shift Security Left to Reduce Misconfigurations

Modern development and DevOps teams rely on Infrastructure as Code (IaC) templates, such as AWS CloudFormation or HashiCorp Terraform, to quickly and repeatedly provision cloud infrastructure. **According to Gartner**, “By 2023, 60% of organizations will use infrastructure automation tools as part of their DevOps toolchains, improving application deployment efficiency by 25%.”

While IaC templates are rising in adoption, the Palo Alto Networks Unit 42 threat researchers found that nearly **50% of CloudFormation templates in use contain misconfigurations**. If a misconfigured IaC template is used dozens or hundreds of times, it could easily add hundreds or thousands of misconfigurations and alerts for security teams to address later in the process.



New code security module in Prisma Cloud



To address this concern, Palo Alto Networks acquired and has now integrated

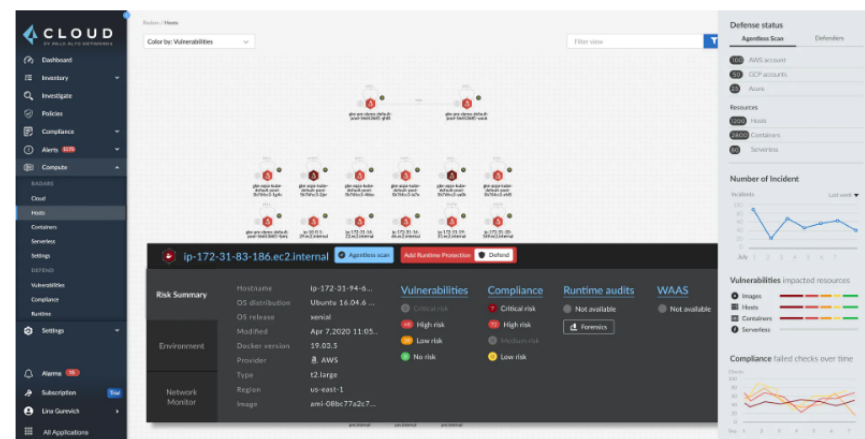
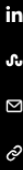
New code security module in Prisma Cloud

To address this concern, Palo Alto Networks acquired and has now integrated **Infrastructure as Code Security** leader Bridgecrew into Prisma Cloud. Until now, security and DevOps teams had to leverage multiple scanning solutions and dashboards across development and runtime security. Now, the Bridgecrew integration provides enterprises with a single solution for addressing IaC risks and integrating security into the development pipeline.

Agentless Security: The Industry's Only Solution with Agentless and Agent-Based Protection

Protecting cloud native applications requires a full stack approach to security, where foundational security requirements like vulnerability management and compliance are combined with runtime protection, network visibility and security for web applications and APIs.

Today, Prisma Cloud delivers full stack protection through our unified agent framework, **the Defender**. Every time a workload or application is deployed, the DevOps, cloud platform or security teams can deploy a Defender agent to protect those environments. In fact, Prisma Cloud has released **auto-deployment and auto-upgrade capabilities** to allow teams to more easily deploy and upgrade Defender for virtual machines across AWS, Google Cloud and Azure.



Prisma Cloud Radar with Agentless scanning results

As cloud adoption continues to accelerate, we want to work with our customers to help their security teams address visibility and security concerns for their cloud workloads by providing them with added flexibility. Customers are looking for quick visibility into their security posture without having to deploy agents.

Agentless scanning is an additional, complementary solution in Prisma Cloud that simplifies our approach to visibility across compute assets, in addition to our agent-based protection. Agentless security primarily focuses on vulnerability management and compliance scenarios, where runtime protection, including preventative capabilities, is better provided by the live Defender agents on the hosts.

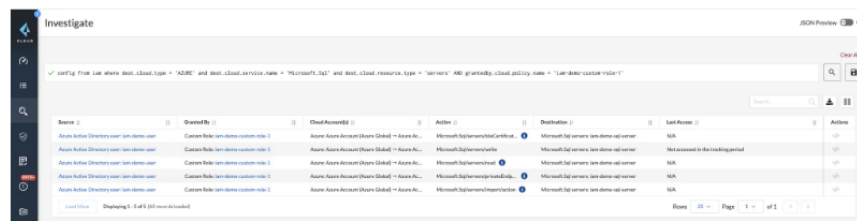
Agentless scanning works off cloud provider APIs and disk snapshots, and can be initiated easily while onboarding cloud accounts, providing a non-intrusive way to understand security posture. This extends coverage to both active and dormant virtual machines in the public cloud. At launch, Prisma Cloud will support virtual machines on AWS with plans to extend to other stacks and clouds.



Agentless scanning works off cloud provider APIs and disk snapshots, and can be initiated easily while onboarding cloud accounts, providing a non-intrusive way to understand security posture. This extends coverage to both active and dormant virtual machines in the public cloud. At launch, Prisma Cloud will support virtual machines on AWS with plans to extend to other stacks and clouds.

Cloud Infrastructure Entitlement Management: New Support for Microsoft Azure Environments and Azure Active Directory Integration

As organizations increasingly adopt Infrastructure-as-a-Service (IaaS) models for cloud development, the number of entities that are granted access to critical infrastructure necessarily grows as well. However, organizations must ensure these entitlements are tightly controlled. **Gartner recently reported** that "the vast majority of granted entitlements in IaaS are unnecessary. More than 95% of accounts in IaaS use, on average, less than 3% of the entitlements they are granted, which greatly increases the attack surface for account compromises."



Source	Granted By	Cloud Account	Action	Destination	Last Access	Action
Azure Active Directory user - sam.davis@contoso.com	Custom Role - sam.davis@contoso.com	Azure Active Directory (Global) - Azure AD	Microsoft.Sql/permissions/grant	Microsoft.Sql servers - sam.davis@contoso.com	N/A	Not accessed in the monitoring period
Azure Active Directory user - sam.davis@contoso.com	Custom Role - sam.davis@contoso.com	Azure Active Directory (Global) - Azure AD	Microsoft.Sql/permissions/grant	Microsoft.Sql servers - sam.davis@contoso.com	N/A	Not accessed in the monitoring period
Azure Active Directory user - sam.davis@contoso.com	Custom Role - sam.davis@contoso.com	Azure Active Directory (Global) - Azure AD	Microsoft.Sql/permissions/grant	Microsoft.Sql servers - sam.davis@contoso.com	N/A	Not accessed in the monitoring period
Azure Active Directory user - sam.davis@contoso.com	Custom Role - sam.davis@contoso.com	Azure Active Directory (Global) - Azure AD	Microsoft.Sql/permissions/grant	Microsoft.Sql servers - sam.davis@contoso.com	N/A	Not accessed in the monitoring period

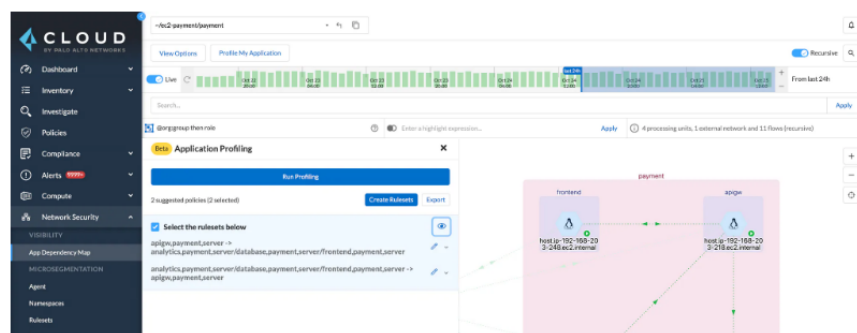
Investigating Azure identity incidents in Prisma Cloud

To help our customers better address these growing risks, Prisma Cloud now extends **Cloud Infrastructure Entitlement Management (CIEM)** to Microsoft Azure. These capabilities include:

- **Net effective permissions analysis for Microsoft Azure:** Seamlessly analyze and gain visibility for accounts, resources and workloads managed by Azure.
- **Azure AD integration:** Ingest single sign-on (SSO) data from Azure AD to calculate net-effective user permissions, no matter which CSP or service the user is accessing.

Identity-Based Microsegmentation: Pre-Defined Rules and Automated App Profiling

Security teams want to **secure their applications with Zero Trust principles** and enforce least-privilege network access. But, determining which apps should be allowed to communicate is an enduring task that's not suited for manual security work.



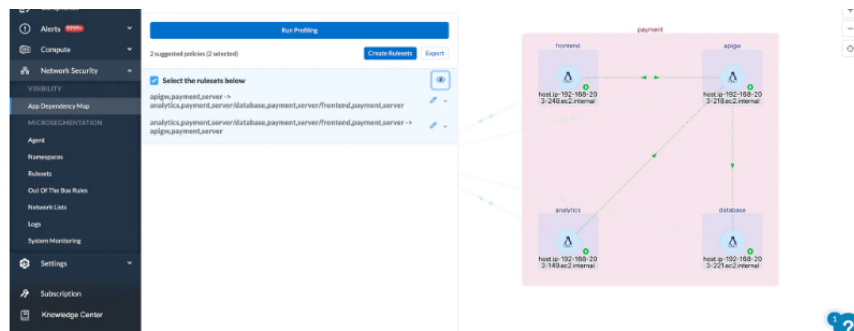
in

+

✉

🔗





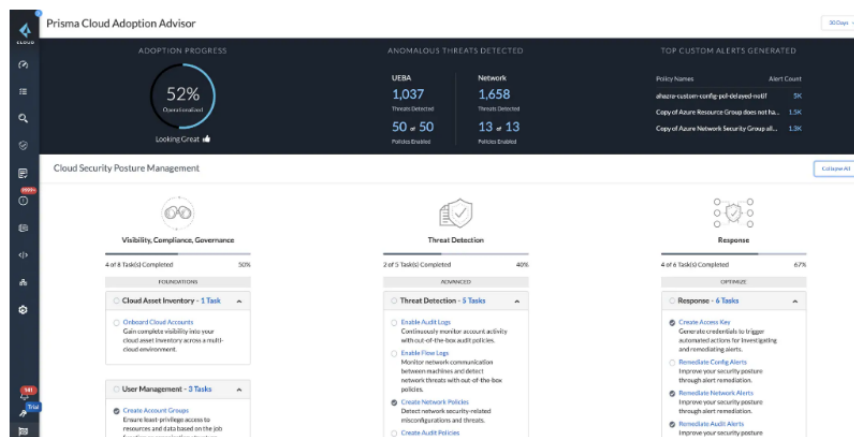
AppDependency Mapping in Prisma Cloud

Prisma Cloud **Identity-Based Microsegmentation** now offers out-of-the-box rules and application profiling, helping security teams simplify and accelerate their Zero Trust adoption. These new rules are validated, predefined microsegmentation rules that can help secure common applications in just minutes.

Application profiling is a simple workflow that automatically generates the optimal, least-privilege microsegmentation rules for any cloud native application, with just a single click. These new capabilities help security teams accelerate their Zero Trust adoption, simplify policy creation and minimize human error.

Adoption Advisor: New Dashboard Improves Cloud Security Operationalization

Security teams want to ensure the highest **return on investment** and highest levels of efficiency possible with their existing security tools. This can be a challenge as cloud environments change quickly. Installing, activating and operationalizing security tools is time consuming without pre-built guidance.



Adoption advisor dashboard in Prisma Cloud

The adoption advisor dashboard is a single location where users can see all of the capabilities they have activated in Prisma Cloud. The dashboard provides detailed guidance for leveraging unused platform capabilities, as well as real-time measurements of activated capabilities.

The initial release of the adoption advisor covers **Cloud Security Posture Management** (CSPM) capabilities, with plans to quickly expand to other areas of the platform.

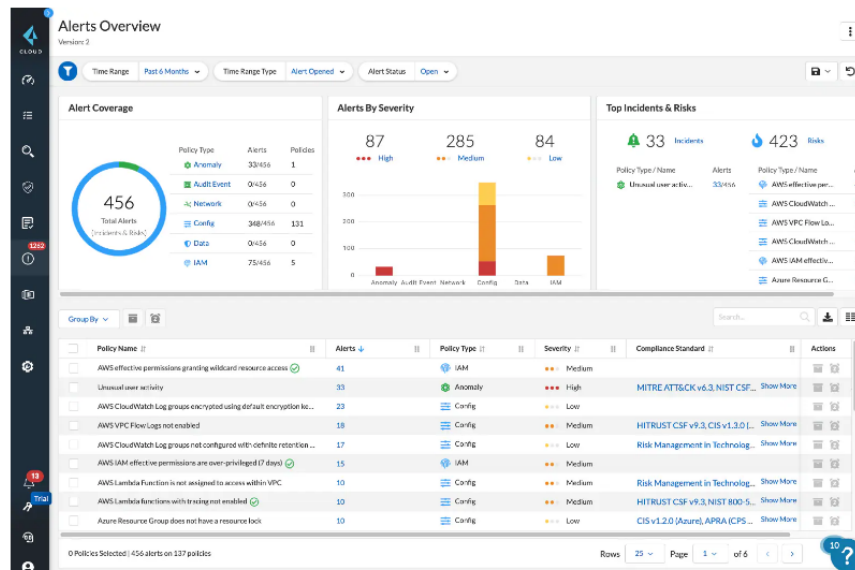
Rapid Risk Discovery: Identify and Remediate Insecure Cloud Resources, Faster



Management (CSPM) capabilities, with plans to quickly expand to other areas of the platform.

Rapid Risk Discovery: Identify and Remediate Insecure Cloud Resources, Faster

Security teams need to **identify misconfigurations** and vulnerabilities as quickly as possible to prevent incidents and ensure compliance in their cloud environments.



Alerts dashboard in Prisma Cloud

We've introduced improvements to the Prisma Cloud architecture that reduce alert times. Customers can address issues faster and save costs from excessive API calls and cloud audit log investigation. This ensures teams can reduce their time-to-remediation for any misconfiguration or threat.

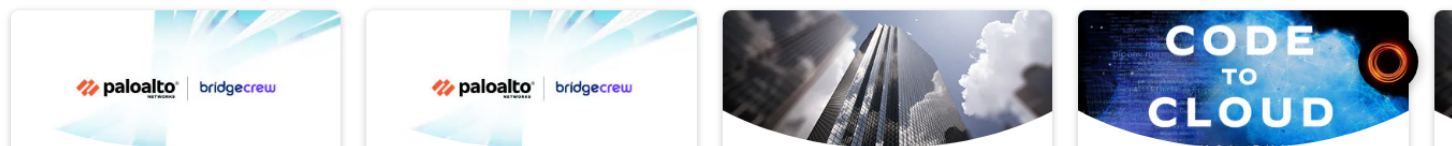
See Prisma Cloud 3.0 for Yourself

These enhancements will be on display along with many other powerful capabilities at our annual Palo Alto Networks user conference, **Ignite**, taking place virtually this week.

Current customers can also reach out to their account representative for more information, or if you're not a current customer, please reach out to **request a free trial** or **register for one of our preview demo sessions**.



RELATED BLOGS





ANNOUNCEMENT, CLOUD POSTURE SECURITY, CLOUD WORKLOAD PROTECTION PLATFORM, DEVSECOPS, PRODUCTS AND SERVICES

Prisma Cloud and Bridgecrew: Doubling Down on Developer-Led Security



ANNOUNCEMENT, DEVSECOPS, PRODUCTS AND SERVICES

Prisma Cloud Shifts Left With Proposed Acquisition of Bridgecrew



MUST-READ ARTICLES, NEWS AND EVENTS

New Cloud Location Innovates and Strengthens Presence in Indonesia



CLOUD COMPUTING, DEVSECOPS, EVENTS

Build Security Expertise from Code to Cloud at our Upcoming Global Practitioner Summit





Get the latest news, invites to events, and threat alerts

Enter your email now to subscribe!

Sign up →

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).

Products and Services				Company	Popular Links
Network Security Platform	Cloud Security	AI-Driven Security Operations Platform	Threat Intel and Incident Response Services	About Us	Blog
CLOUD DELIVERED SECURITY SERVICES	Cortex Cloud	Cortex XDR	Proactive Assessments	Careers	Communities
Advanced Threat Prevention	Prisma Cloud	Cortex XSOAR	Incident Response	Contact Us	Content Library
DNS Security		Cortex Xpanse	Transform Your Security Strategy	Corporate Responsibility	Cyberpedia
Data Loss Prevention		Cortex XSIAM	Discover Threat Intelligence	Customers	Event Center
IoT Security		External Attack Surface Protection		Investor Relations	Manage Email Preferences
Next-Generation Firewalls		Security Automation		Location	Products A-Z
Hardware Firewalls		Threat Prevention, Detection & Response		Newsroom	Product Certifications
Strata Cloud Manager					Report a Vulnerability
SECURE ACCESS SERVICE EDGE					Sitemap
Prisma Access					Tech Docs
Prisma SD-WAN					Unit 42
Autonomous Digital Experience Management					Do Not Sell or Share My Personal Information
Cloud Access Security Broker					

Document title: Palo Alto Networks Shifts Left with Prisma Cloud 3.0
Capture URL: <https://www.paloaltonetworks.com/blog/2021/11/shift-left-with-prisma-cloud-3-0/>
Capture timestamp (UTC): Wed, 19 Mar 2025 18:23:35 GMT

Ex. 2135-007

Page 7 of 8

Bridgecrew:
Doubling Down on
Developer-Led
Security

Bridgecrew

Presence in
Indonesia

Upcoming Global
Practitioner Summit



Get the latest news, invites to events, and threat alerts

Enter your email now to subscribe!

Sign up →

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).



Products and Services

Network Security Platform

Cloud Security

AI-Driven Security Operations Platform

Threat Intel and Incident Response Services

Company

Popular Links

CLOUD DELIVERED SECURITY SERVICES

Cortex Cloud

Cortex XDR

Proactive Assessments

About Us

Blog

Careers

Communities

Contact Us

Content Library

Advanced Threat Prevention

Prisma Cloud

Cortex XSOAR

Incident Response

Corporate Responsibility

Cyberpedia

DNS Security

Cortex Xpanse

Transform Your Security Strategy

Customers

Event Center

Data Loss Prevention

Cortex XSIAM

Discover Threat Intelligence

Investor Relations

Manage Email Preferences

IoT Security

External Attack Surface Protection

Location

Products A-Z

Next-Generation Firewalls

Security Automation

Newsroom

Product Certifications

Hardware Firewalls

Threat Prevention, Detection & Response

Report a Vulnerability

Strata Cloud Manager

Sitemap

SECURE ACCESS SERVICE EDGE

Tech Docs

Prisma Access

Unit 42

Prisma SD-WAN

Do Not Sell or Share My Personal Information

Autonomous Digital Experience Management

Cloud Access Security Broker

Zero Trust Network Access



Privacy Trust Center Terms of Use Documents
Copyright © 2025 Palo Alto Networks. All Rights Reserved

