CORTEX® XDR™ | paloalto® NETWORKS

Addressing Cloud Security Challenges with Palo Alto Networks

The Acceleration to the Cloud

Cloud computing is pervasive: according to IDC, by 2022, over 90% of enterprises worldwide will rely on a mix of on-premises or dedicated private clouds, multiple public clouds, and legacy platforms to meet infrastructure needs.[1]

As pervasive as cloud computing has become, it is increasingly a primary target for cyberattacks. Moving to the cloud can help simplify and improve certain aspects of security—for example, at the infrastructure layer.

However, cloud deployments also present new challenges in security that many organizations are either not accustomed to handling or have not yet learned how to address efficiently. When attempting to address cloud security, many organizations find that their on-premises methodologies do not translate directly or easily to the cloud.

1. "IDC Expects 2021 to Be the Year of Multi-Cloud as Global COVID-19 Pandemic Reaffirms Critical Need for Business Agility," IDC, 30 March 2021, https://www.idc.com/getdoc.jsp?containerId=prMETA46165020.

The Many Roles in Cloud Security

Cloud security encompasses a wide range of activities, from configuration management (ensuring cloud assets are set up correctly from a security perspective) to deep investigations and response (dealing with a threat that has been detected anywhere in the enterprise environment and finding malicious activities associated with that threat).

Depending on the organization, these activities are owned by many different roles and team functions associated with cloud security, including:

- Cloud infrastructure engineers and architects
- Security architects and engineers
- DevOps and DevSecOps teams
- Governance, risk, and compliance (GRC) teams
- SOC managers
- Security analysts, incident responders, and threat hunters
- CISOs

Again, depending on how cloud initiatives are run and organized, each of these teams may have different requirements relative to their area of ownership. And depending on the initiative, some of these teams' scope of ownership may vary to be broad or narrow.

Table 1: Cloud Security Roles and Responsibilities

Team/Role	Key Responsibilities
Cloud infrastructure engineers and architects	Design cloud environments; deployment and overall ownership of cloud and container platforms
Security architects and engineers	Coverage across both cloud and SOC teams; implement security for public cloud environments and new cloud native architectures (e.g., cloud VMs, containers, Kubernetes, and serverless)
DevOps and DevSecOps teams	Manage cloud infrastructure deployments; design cloud native architectures at scale
GRC teams	Monitor and communicate risks to the business
SOC managers	Ensure security operations are keeping up with the business; dwell times are low
Security analysts, incident responders, and threat hunters	Monitor, detect, investigate, and respond to threats spanning cloud and on-premises
CISOs	Security of overall cloud journey and investments

Cloud Security Challenges

Cloud security challenges are as diverse as the teams responsible for solving those challenges. In general, there are requirements specific to cloud native environments and those specific to hybrid cloud/multicloud environments.

Cloud security teams largely embrace the DevOps mindset of "move as fast as possible." They are responsible for protecting cloud native applications directly in conjunction with build-to-run processes. Their challenge is to ensure that those applications do not fall victim to various threats and security issues during and after the continuous and rapid iterations of the build-to-run cycle, including:

- **Vulnerabilities in applications**: Application code, if not scanned with the right tools, can introduce known CVEs to critical environments that an attacker can exploit. This can be especially challenging to address across many various environments and the application lifecycle.
- **Insecure configurations**: The wrong configurations, both to the applications themselves or the infrastructure they are running on, can add to risk. For example, a misconfigured storage bucket, insecure network configuration, or application running as root adds to overall risk for an enterprise.
- **Lack of runtime protection**: Running applications can be vulnerable to attacks without the proper visibility and protection covering file system activity, network communications, process activity, and system call activity. Without the right security solution in place, organizations are left exposed without the ability to both prevent threats or capture forensic activity for further incident analysis.

- **Visibility and control over network communications**: Microservices and application workloads communicate with one another and with the outside world. Security and infrastructure teams need to understand application dependencies, reduce their cloud network threat surface, and contain any cyberattack.
- **Over-permissioned entitlements across public clouds**: As organizations onboard large numbers of developers, DevOps engineers, platform engineers, and other key stakeholders, they want to ensure each user has the proper cloud entitlements. Yet, manual configurations for each user, inability to audit cloud permissions automatically, and lack of right-sized permissions are continued challenges across single and multicloud environments.

Security operations teams are responsible for keeping up with the pace of cloud application development and production rollouts and ensuring that the cloud environment is accounted for within their workflows for threat detection, investigation, and response. Their challenge is to see across both on-premises and cloud environments simultaneously—and not just have visibility, but be able to get the most out of that visibility without applying new methodology or translating on-premises methodology to the cloud. Their core challenges are:

- **Detecting threats that span the entire organization**: Threat detection mechanisms do not easily provide the ability to collect, process, and analyze cloud data along with on-premises environments and assets.
- **Simplifying incident response in cloud environments**: Security operations teams too often need to context switch between on-premises activity and cloud activity since they are often accessed via different tools, or use separate or unrelated workflows to triage alerts, perform ad hoc analysis, or investigate deeper into a threat—either for scoping or to conduct forensic analysis.
- **Correlate threat activities across multiple data sources**: For operations teams that maintain data collection on-premises, they cannot realistically send cloud data to their central logging platforms to run cross-data analysis. For cloud-hosted data logging, getting deep context from cloud, endpoint, network, and user data into a single location can be expensive and/or technically challenging (or not feasible), and the analytics used to detect threats is not processing those data sources with the depth of integration needed to properly contextualize an incident.
- **Gaining threat-oriented context spanning cloud and on-premises**: Incident response teams need the full range of threat context that comes from threat alerts, incidents, assets, threat intelligence, and all third-party data sources—from both cloud and on-premises—at their fingertips, so they can run complete investigations that result in actionable findings.
- **Compounded alert fatigue from disparate cloud alerts**: Monitoring and triage teams are unable to easily incorporate suspicious cloud activity into their broader and already noisy alert queue, resulting in poorly verified escalations, lack of or shallow understanding of causality, inability to easily build a timeline of events, and general increase in fragmentation of processes overall.

In general, requirements for security, user experience, investigative methodology, and response workflows will differ significantly between cloud native security teams and more traditionally oriented SOC teams.

This is largely because cloud security teams will more closely mirror the process of the build-to-run cycle of cloud application development and deployment, which first requires:

- Depth and breadth in the foundational aspects of cloud security
- Coverage for the largest range of cloud activity possible
- Extremely deep insight into the cloud environment

Whereas SOC teams usually have their existing processes in place already and are focused on:

- Unifying their enterprise-wide view to gain critical investigative context and the right telemetry needed for threat detection and analytics
- Ensuring that cloud context is deeply integrated into the bigger picture of threat activity across the entire organization

Comprehensive Cloud Security with Palo Alto Networks

Today, most organizations will use a combination of legacy SOC tools, such as SIEM plus a CSPM or CWPP solution, to address specific aspects of these challenges. The main issue with this approach is that it fails to natively stitch together endpoint, network, cloud, and identity data to contextualize cloud threats across the broader hybrid environment.

Another approach is to look at evaluating EDR or XDR marketed as a cloud security tool to try and solve the entire end-to-end problem. The main challenge with this approach is that EDR/XDR is a SOC-optimized tool and does not meet the unique security, usability, and speed requirements of cloud security teams.

Palo Alto Networks provides a unique cloud security solution that meets the depth, coverage, and operational requirements of both cloud security and traditional SOC teams.

Prisma® Cloud provides full lifecycle vulnerability management, compliance monitoring, and runtime protection, enabling cloud security teams to prioritize and resolve the risks of applications running in the cloud. Prisma Cloud also ensures secure configurations of cloud resources and environments, identifies over-permissioned entitlements in public clouds, and combines network visibility and microsegmentation to deliver comprehensive cloud network security.

Cortex® XDR™ provides cloud capabilities for SOC teams focused on enterprise-wide threat monitoring. Cortex XDR's cloud capabilities are what SOC teams need to extend detection, monitoring, and investigation into cloud environments. XDR integrates cloud host data, traffic logs, audit logs, Prisma Cloud data, and third-party cloud security data with non-cloud endpoint, network, and identity data sources for SOC teams to increase their coverage to span on-premises and multicloud environments.

Table 2: Prisma Cloud and XDR's Cloud Capabilities

Feature	Prisma Cloud	Cloud Capabilities in XDR
Runtime security	Application control and allow listing automatically profile host and application behaviors to alert on or prevent malicious processes and network behavior; file integrity monitoring; data feeds provide vulnerability, suspicious IP lists, anti-malware, and advanced threat protection data; OWASP top 10 protection; DOS prevention; bot protection; and virtual patching	Linux host EDR provides behavioral threat protection, brute force protection, kernel integrity monitoring, local analysis of file/dll/macro, privilege escalation protection, shellcode protection, and shared object hijacking protection
Analytic techniques	Analytics for cloud applications, hosts, Kubernetes, and serverless to identify the source (provenance) of the threat (e.g., vuln, image, setting, who changed), with network and user behavior analytics to detect anomalous activities	Cross-data analytics that covers endpoint, network, identity, and cloud for automated correlation, stitching for detection and response to identify all evidence and malicious activities associated with the incident
Incident management	Designed for cloud and DevSecOps teams to identify threats and provide forensics for vulnerabilities, configurations, permissions, and suspicious activities of applications and resources, and provide the history of actions against those resources	Designed for the SOC analyst that investigates the impact of the threat by gathering evidence and additional context via automated and ad hoc correlations that uncover all other malicious activity related to the alert
Threat detection	Prisma Cloud ML-based detectors automatically capture data across network flow logs, audit logs, and cloud resources in public clouds, host, and applications in public clouds and on-prem	XDR ML-based detectors where the results are automatically correlated across endpoint, network, and identity data sources
Automated incident building with alert grouping, causality, and timeline	Alerts show misconfiguration and threat context from correlating config data with user behavior and network traffic; visual investigation of cloud data exfil, cloud account compromise, cloud policy violations, and noncompliance to industry benchmarks	Focused on stitching alerts, context, and threat data in an automated fashion to provide an end-to-end incident story for incident responders who need to see the scope of all related threat activity enterprise-wide, across the on-premises and multicloud environment

Together, Prisma Cloud and XDR's cloud capabilities offer the most comprehensive cloud security solution today, enabling full cloud security from build to run to security operations.

Visit our website to learn more about Prisma Cloud and Cortex XDR, or check out the following resources:

- Prisma Cloud Tech Brief
- Prisma Cloud product documentation
- Cortex XDR product documentation
- Next Has Arrived: The Launch of Third-Generation XDR

paloalto® NETWORKS | Cybersecurity Partner of Choice

3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087