Stream.Security

# Traditional Security Tools Fail in the Cloud. CDR is Closing that Gap.

As cloud environments grow more complex, traditional security tools struggle to keep up. Cloud Detection and Response (CDR) redefines how security teams manage cloud threats by bringing real-time clarity, intelligence, and precision to every stage of the incident response lifecycle.

THE CLOUD SECURITY GAP

## *First to respond. Last to know.*

Today's SOC teams face growing complexity:

- Alerts flood in with no clear context
- Missing data forces teams to escalate incidents
- Investigations focus on symptoms, not full attacks
- Legacy tools can't handle cloud-native environments

Traditional tools weren't designed for today's cloud, where infrastructure is dynamic and ephemeral.

## What's Missing from the Traditional Approach to Security?

SOC teams don't need more alerts, they need context. In the cloud, that context crosses infrastructure layers to accommodate complexity.

But most security teams are working with fragments:

```
⚠ { "AnomalousProcess", "host": "10.1.5.23" }
⚠ { "event": "AssumeRole", "pod": "nginx-pro...
⚠ { "ExploitAttempt", "cve": "CVE-2024-2...
```

***Without knowing who did what, why it happened, and what it enabled, analysts are left in the dark.***

## TRADITIONAL SECURITY STACK VS. CLOUD REALITIES

Today's security tooling isn't helping analysts understand the cloud. This brings them into a paradox: alerts are either left unaddressed or are escalated immediately to expert teams. Automatically, the first layers of an organization's defense are at a disadvantage compared to threat actors.

| Traditional Tools | Cloud-Native Environments |
|---|---|
| Static snapshots | Constant, real-time changes |
| Defined log sources | Distributed data from APIs, services, and infrastructure |
| Alerts without impact | Attack progression with a cross-layer ripple effect |
| Reactive triage | Vulnerable to rapid extensive breaches |
| Collection, not clarity | Dynamic and complex |

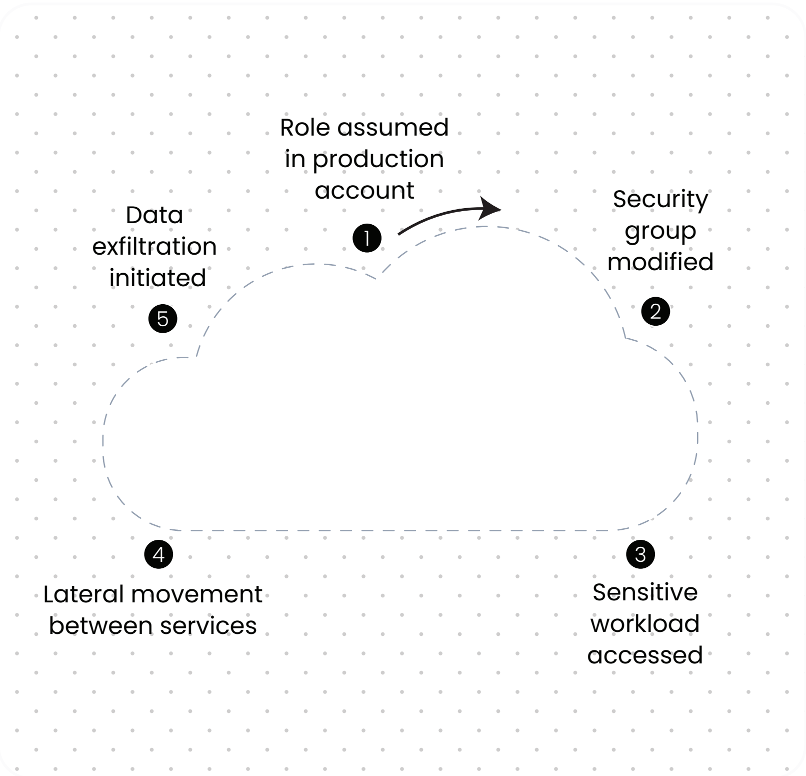
## Enter Cloud Detection and Response (CDR)

CDR gives SecOps teams the full picture before, during, and after an attack unfolds:

- Live attack storylines, not just events
- Cross-layer visibility that provides context to enrich alerts
- Exploitability modeling to prioritize risks based on attack paths and organization requirements
- Dynamic context that updates as the environment changes with cloud modeling

Real-World Example:

## Connecting the Dots



1 Role assumed in production account

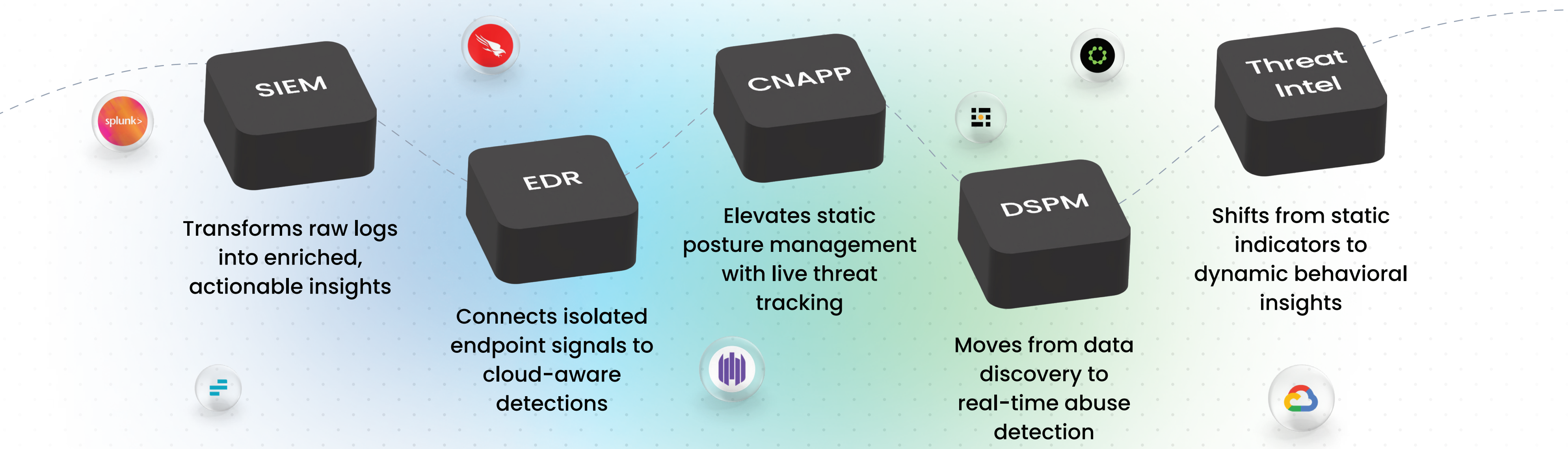
2 Security group modified

3 Sensitive workload accessed

4 Lateral movement between services

5 Data exfiltration initiated

## Not a Tool Replacement, But a Real-Time Clarity & Context Layer



SIEM: Transforms raw logs into enriched, actionable insights

EDR: Connects isolated endpoint signals to cloud-aware detections

CNAPP: Elevates static posture management with live threat tracking

DSPM: Moves from data discovery to real-time abuse detection

Threat Intel: Shifts from static indicators to dynamic behavioral insights

**CDR acts as the connective tissue that makes every tool smarter in the cloud.**

## Ready to Operate at Cloud Speed?

Stream.Security's Cloud Detection and Response platform delivers what SecOps teams need most:

- Instant clarity
- Reduced triage time
- Precision and speed in threat resolution

See how modern security teams are taking the lead.
Visit stream.security to learn more.

Stream.Security