Stream.Security

Closing the Cloud Security Gap with Stream Security & EDR

Traditional Endpoint Detection and Response (EDR) solutions are designed to detect and respond to threats at the workload level, monitoring processes, file integrity, and behavioral anomalies. However, EDR lacks visibility into the cloud layer, where modern attacks frequently originate. Stream Security bridges this gap by delivering real-time cloud visibility, correlating workload activity with cloud-layer events to uncover the entire attack storyline. Together, Stream Security and EDR solutions provide end-to-end threat detection and response, ensuring that security teams can fully understand and neutralize cloud-native attacks.

Let's walk through real-life attack scenarios that demonstrate where EDR misses context, and how Stream Security fills the gap.

Gartner
COOL VENDOR 2024

Attack Scenario: Cloud-to-Workload Exploitation

Step 1: Initial Access (Cloud Layer)

- An attacker exploits a publicly exposed cloud resource (e.g., misconfigured S3 bucket, open API endpoint) to gain a foothold.
- Stream Security detects unusual access patterns, highlighting misconfigurations and excessive permissions that increase the risk of exploitation.

Step 2: Privilege Escalation & Lateral Movement (Cloud Layer)

- The attacker compromises an overprivileged identity, assuming new roles and escalating privileges within the cloud environment.
- Stream Security monitors API calls and role assumptions in real-time, detecting suspicious activity before it reaches workloads.

Step 3: Workload Exploitation (EDR Coverage)

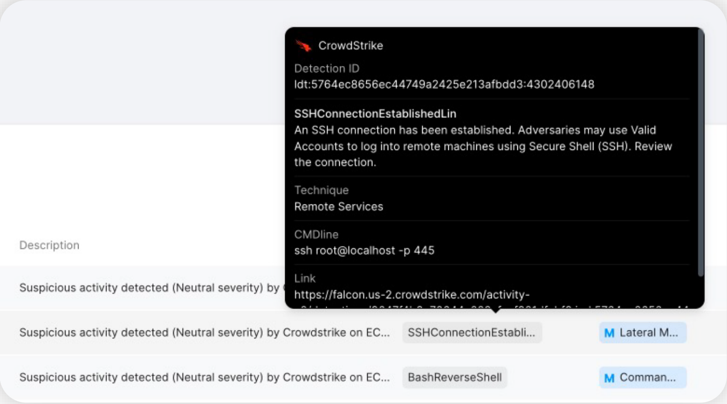
- Using the compromised identity, the attacker moves laterally to launch malware or exploit vulnerabilities in a virtual machine or container.
- EDR detects runtime anomalies, such as unauthorized processes, suspicious network activity, or file modifications.

Step 4: Data Exfiltration & Persistence (Cloud & Workload)

- The attacker attempts to exfiltrate sensitive data via cloud storage or maintain access by deploying persistence mechanisms.
- Stream Security tracks cloud-layer persistence (e.g., IAM backdoors, modified configurations), while EDR identifies persistence within workloads (e.g., scheduled tasks, rootkits).

Step 5: Evading Detection (Cloud & Workload)

- The attacker tries to clear logs or disable monitoring tools at both the cloud and workload levels.
- Stream detects cloud log tampering, while EDR alerts on attempts to disable security agents.



CrowdStrike

Detection ID
ldt:5764ec8656ec44749a2425e213afbdd3:4302406148

SSHConnectionEstablishedLin
An SSH connection has been established. Adversaries may use Valid Accounts to log into remote machines using Secure Shell (SSH). Review the connection.

Technique
Remote Services

CMDline
ssh root@localhost -p 445

Link
https://falcon.us-2.crowdstrike.com/activity-

Description		
Suspicious activity detected (Neutral severity) by		
Suspicious activity detected (Neutral severity) by Crowdstrike on EC...	SSHConnectionEstabli...	M Lateral M...
Suspicious activity detected (Neutral severity) by Crowdstrike on EC...	BashReverseShell	M Comman...

How Stream.Security & EDR Work Together

Unifying the Attack Storyline

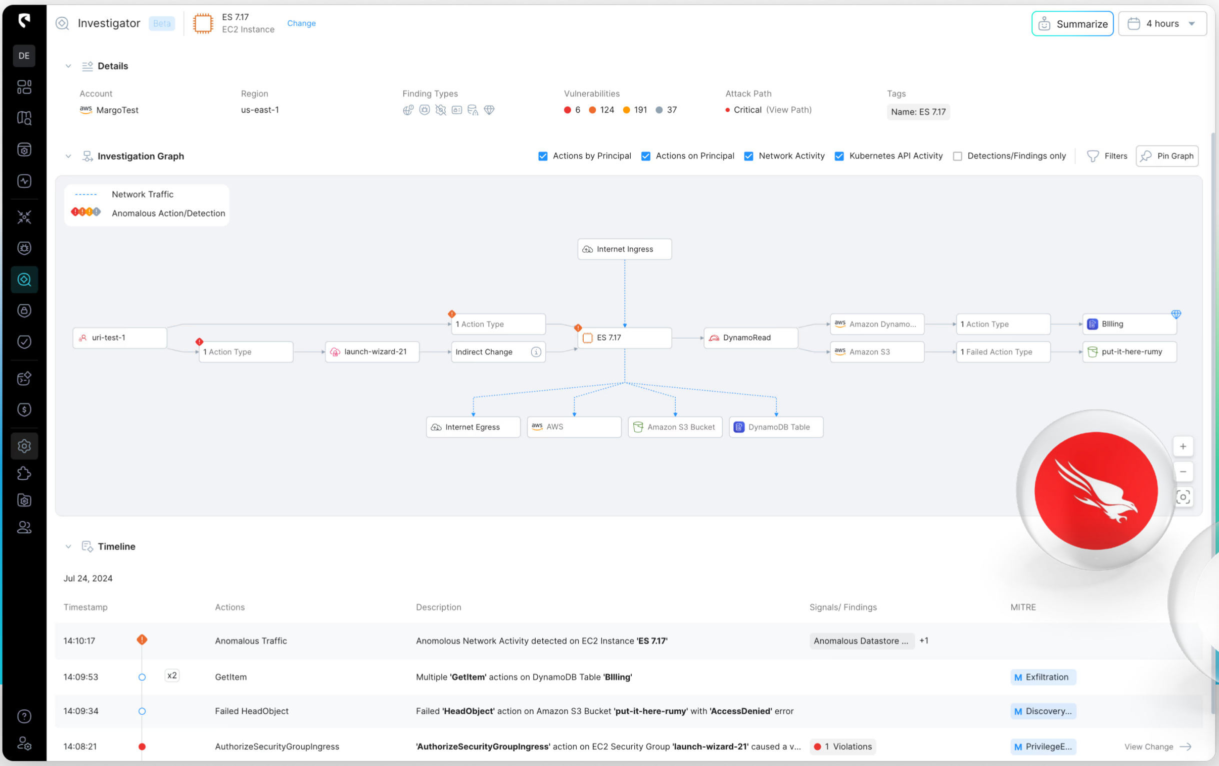
Stream Security correlates cloud-layer events (misconfigurations, identity misuse, API activity) with EDR-detected workload activity, presenting a full attack narrative instead of isolated alerts.

Expanding Response Alternatives

With complete context, Stream provides multiple validated response options, ensuring that actions eliminate the threat while minimizing business disruption.

Reducing Investigation Time

By automating cloud-workload correlation, Stream removes manual analysis, allowing security teams to respond faster and more effectively.



Investigator Beta | ES 7.17 EC2 Instance Change | Summarize | 4 hours

Details

Account	Region	Finding Types	Vulnerabilities	Attack Path	Tags
aws MargoTest	us-east-1		● 6 ● 124 ● 191 ● 37	● Critical (View Path)	Name: ES 7.17

Investigation Graph

☑ Actions by Principal ☑ Actions on Principal ☑ Network Activity ☑ Kubernetes API Activity ☐ Detections/Findings only | Filters | Pin Graph

Timeline

Jul 24, 2024

Timestamp		Actions	Description	Signals/ Findings	MITRE	
14:10:17		Anomalous Traffic	Anomolous Network Activity detected on EC2 Instance **'ES 7.17'**	Anomalous Datastore ... +1		
14:09:53	x2	GetItem	Multiple **'GetItem'** actions on DynamoDB Table **'BIlling'**		M Exfiltration	
14:09:34		Failed HeadObject	Failed **'HeadObject'** action on Amazon S3 Bucket **'put-it-here-rumy'** with **'AccessDenied'** error		M Discovery...	
14:08:21		AuthorizeSecurityGroupIngress	**'AuthorizeSecurityGroupIngress'** action on EC2 Security Group **'launch-wizard-21'** caused a v...	● 1 Violations	M PrivilegeE...	View Change →

Better Together:
Real-Time Cloud Security & Workload Protection

By combining Stream Security's real-time cloud modeling with EDR's workload protection, organizations gain a comprehensive security approach that eliminates blind spots and enables precise, impact-driven response strategies. This ensures that:

- Attacks are neutralized before reaching critical workloads.
- Security teams receive actionable, high-fidelity alerts instead of isolated noise.
- Business continuity is preserved, preventing unnecessary disruptions.

Stream Security & EDR:
The Complete Solution for Cloud-Native Threats