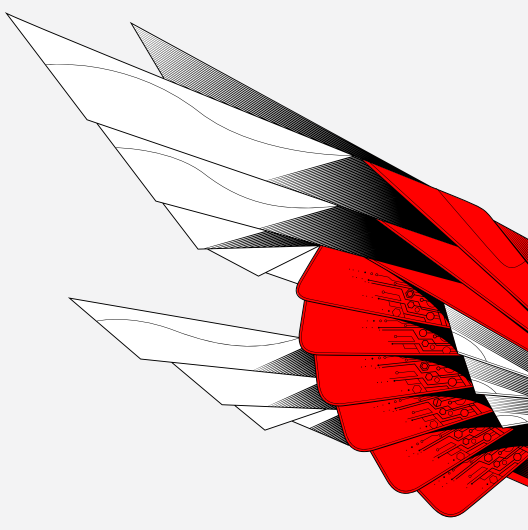
# BLEIBEN SIE NEUEN WORKLOAD-BEDROHUNGEN EINEN SCHRITT VORAUS



- 92 % DER UNTERNEHMEN HOSTEN IHRE UMGEBUNGEN DERZEIT IN DER CLOUD
- DATENVERLUSTE, FEHLENDE TRANSPARENZ, IDENTITÄTSBETRUG UND NICHT AUTORISIERTE ZUGRIFFE WAREN 2021 DIE GRÖSSTEN CLOUD-BEDROHUNGEN
- SICHERHEITSTEAMS KÖNNEN NUR AUF 3–5 % DER SICHERHEITSEREIGNISSE REAGIEREN, DIE TÄGLICH REGISTRIERT WERDEN

## SCHÜTZEN SIE IHRE CLOUD-UMGEBUNG MIT EINER MEHRSCHICHTIGEN SICHERHEITSSTRATEGIE VON CROWDSTRIKE UND AWS

Mehrschichtiger Schutz ist ein Architekturkonzept, das auf einer militärischen Strategie basiert, bei der Angreifer mehrere Verteidigungslinien überwinden müssen. Beim Schutz von Cloud-Workloads bedeutet „mehrschichtig“, dass mehrere Schutzmechanismen – Transparenz, Prävention und Behebung – Ihre wertvollen Daten und Informationen sowie Ihr Wissen schützen.

Die führenden CrowdStrike-Lösungen zum Schutz von Endgeräten und Workloads sowie der CrowdStrike-Bedrohungsnachrichtendienst integrieren sich direkt mit den AWS-Services. Dadurch erhalten Sie eine effektive, mehrschichtige Lösung, mit der Sie Bedrohungen immer einen Schritt voraus bleiben.

### TRANSPARENZ ERMÖGLICHT KLARHEIT

Mehrschichtiger Schutz beginnt mit Transparenz, denn Sie können nur das schützen, was Sie auch sehen. Gemeinsam bieten CrowdStrike und AWS Einblicke darin, welche Daten, Anwendungen und Assets verwendet werden, damit Sie auf Angriffe reagieren können. Mit CrowdStrike-Lösungen können Sie sich die Konfigurationen aller Komponenten ansehen, den bei Workloads ein- und ausgehenden Netzwerkdatenverkehr aggregieren und API-Aufrufe prüfen. Außerdem können Sie die Laufzeit einsehen.

### PRÄVENTION ERMÖGLICHT MASSNAHMEN

Sobald Sie eingehende Bedrohungen sehen, können Sie Gegenmaßnahmen ergreifen. Durch den mehrschichtigen Ansatz von CrowdStrike und AWS können Sie Präventionsmaßnahmen ergreifen, indem Sie mithilfe von Aggregation und Korrelation ungewöhnliches Verhalten in Ihren Workloads erkennen. CrowdStrike Falcon Discover und die Falcon-Sensoren liefern Erkennungs- und Audit-Informationen mit Laufzeit-Transparenz aus mehreren AWS-Quellen und generieren Warnmeldungen, damit Sie handeln können.

### BEHEBUNG ERMÖGLICHT REAKTION

Ergreifen Sie gezielt Maßnahmen. Ihr Sicherheitsteam wird entlastet, da das CrowdStrike Falcon Integration Gateway und die Falcon-API besonders riskante Ereignisse an AWS Security Hub senden, um Behebungs-Workflows auszulösen und sogar die konkrete Domäne oder IP-Adresse zu blockieren, die als schädlich eingestuft wurde.

## HOLEN SIE SICH DIE KOSTENLOSE TESTVERSION IM AWS MARKETPLACE

Gehen Sie den ersten Schritt, um Bedrohungen einen Schritt voraus zu bleiben. Überzeugen Sie sich selbst, wie zuverlässig Sie mit dem mehrschichtigen Ansatz von CrowdStrike und AWS Bedrohungen beheben und beseitigen können.

**KOSTENLOSE TESTPHASE STARTEN**