SECURITY SUMMIT

Security Summit

Verona 28 ottobre 2026

Clusit

ASTREA

Sessione

Visibilità e controllo nell’era del cloud e della AI

Luca Bechelli | Membro del Comitato Direttivo Clusit
Alessandro Alagna | Sales Engineer Watchguard

Luca Bechelli



Membro del Comitato Direttivo

Partner @P4I – GRUPPO DIGITAL360

Alessandro Alagna

Sales Engineer Italy and Malta



"Bring Your Own AI"

78%

dei lavoratori della conoscenza utilizza strumenti personali di IA generativa sul posto di lavoro senza autorizzazione IT.

FONTE: MICROSOFT & LINKEDIN WORK TREND INDEX

Impatto economico e sicurezza

43%

Incidenza negli incidenti

Gli incidenti di sicurezza coinvolgono direttamente o indirettamente l'uso di Shadow AI.

+$670k

Costo Medio Addizionale

Costo aggiuntivo addebitato dalle aziende per ciascun data breach legato a Shadow AI non gestita.

Lo Stato della Governance Aziendale

63%

Aziende colpite da breach senza una governance IA definita.

40%

Organizzazioni totalmente prive di policy formali sull'IA.

+40%

Aziende con incidenti gravi entro il 2030 causa Shadow AI (previsione).

FONTE: GARTNER RESEARCH & IBM SECURITY

Efficacia dei Blocchi vs Alternative Managed

Aggiramento Blocchi

41%

Lavoratori che eludono i firewall per usare tool vietati.

Fornitura Enterprise AI

-89%

Crollo dello Shadow AI con alternative gestite e sicure.

FONTE: GARTNER RESEARCH & IBM SECURITY

Shadow IT e Shadow AI: due facce dello stesso fenomeno

Shadow IT

Servizi SaaS, cloud, dispositivi e workflow adottati senza supervisione formale.

Shadow AI

Strumenti GenAI, assistenti e automazioni utilizzati fuori dai processi approvati.

Punto comune

La richiesta di produttività corre più velocemente dei processi IT.

Il problema non è innovare, ma farlo senza visibilità e governance.

Perché la mancanza di visibilità conta

Dati

Prompt, allegati, codice e informazioni riservate possono uscire dai flussi governati.

Identità

Account personali e accessi non federati riducono tracciabilità e revoca.

Compliance

Retention, localizzazione e condizioni del fornitore possono non essere note.

Un dominio nei log non basta: servono identità, contesto e dati trattati.

Le quattro domande da collegare

Che cosa?

Applicazioni, domini, servizi AI, estensioni e API.

Chi e dove?

Utente, gruppo, dispositivo, sede o lavoro remoto.

Quali dati?

Upload, prompt, codice e contenuti sensibili.

Quale rischio?

Permessi, compliance e impatto operativo.

La visibilità utile collega evento, identità, dato e rischio.

Un approccio a più livelli

Persone

Policy chiare e formazione contestuale.

Identità e device

MFA, postura e privilegi minimi.

Rete e accesso

DNS, web filtering, SSE e firewall.

Dati e monitoraggio

Classificazione, DLP e correlazione.

Nessun singolo controllo copre ogni utente, luogo e applicazione.

Che cosa deve offrire una soluzione efficace

Clientless

Integrazione con i tenant cloud e SaaS supportati, senza agenti.

Oltre il tenant

Shadow AI e SaaS usati con account personale o senza email aziendale.

Visibilità completa

Ufficio, lavoro remoto e dispositivi gestiti: nessun punto cieco.

Dati e conformità

Condivisioni esposte, misconfigurazioni e compliance sui principali framework internazionali.

Senza visibilità fuori dal tenant, lo shadow AI resta invisibile.

Q&A

DOMANDA 1 | INTERVISTA

Quale prodotto aiuta nella detection e remediation di Shadow IT e Shadow AI?

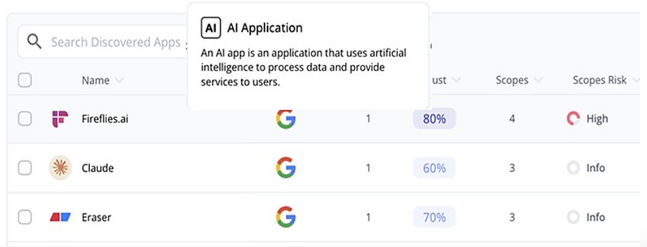
WatchGuard Cloud Detection and Response (CloudDR).

- Visibilità sugli ambienti cloud e SaaS supportati.
- Analisi delle evidenze raccolte dalle integrazioni configurate.
- Azioni di remediation in base alle funzionalità disponibili.

WatchGuard Cloud Detection and Response

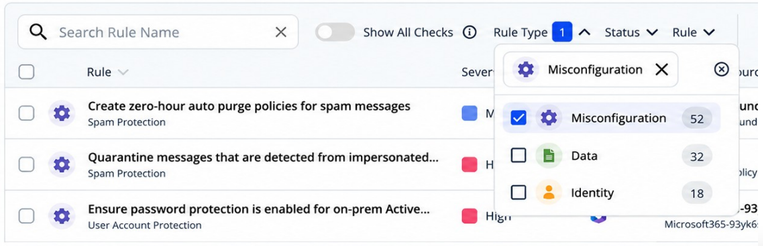
Shadow IT Protection

Eliminate unknown exposure and regain control



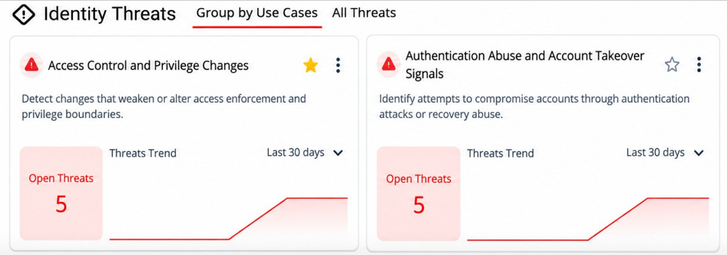
Misconfiguration Management

Close the most common attack paths before they're exploited



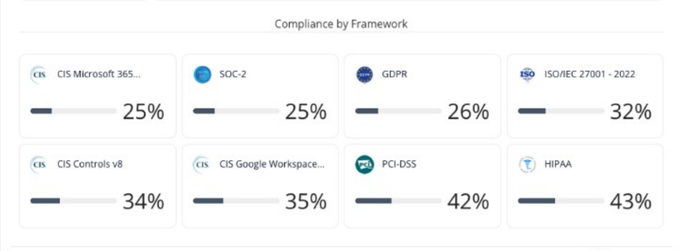
Identity Threat Detection & Response

Stop identity-based attacks in real time



Continuous Compliance Readiness

Assess posture. Find the gaps. Remediate risk. Prove improvement.



One Platform. Agentless. Designed for MSP Scale.

DOMANDA 2 | INTERVISTA

In che modo CloudDR acquisisce le informazioni?

Attraverso le evidenze rese disponibili dal tenant integrato.

- CloudDR si integra con i servizi cloud supportati.
- Utilizza il contesto disponibile su applicazioni, identità, autorizzazioni e attività.
- La copertura dipende dai dati esposti dalla specifica integrazione.

What CloudDR Reveals

1 Misconfigurations

Continuously monitor and fix the Cloud configuration



2 Identity Threats

Discover, monitor and manage every Cloud account



3 Shadow Apps

Discover, monitor and manage Shadow apps



4 Shared Data

Discover and remove file sharing violations

Public Shares | External Shares | Unused Shares | Sensitive Files

5 Compliance

Audit compliance… over 40 frameworks



- User Account Protection
- Access Control
- Privacy Control
- Data Leakage Prevention
- System Integrity
- Gen AI Security
- Malware Protection
- Phishing Protection
- Spam Protection

Copyright © 2026 WatchGuard Technologies, Inc. All Rights Reserved.

DOMANDA 3 | INTERVISTA

Cosa succede se il dipendente utilizza credenziali personali?

CloudDR viene affiancato da FireCloud per coprire il punto cieco fuori dal tenant.

- L’attività con account personale può non comparire nel tenant aziendale.
- FireCloud aggiunge visibilità sull’accesso web dal dispositivo gestito.
- Le due fonti offrono una vista complementare: tenant cloud e navigazione web.

Discover and Enforce Shadow SaaS and AI Governance

CloudDR

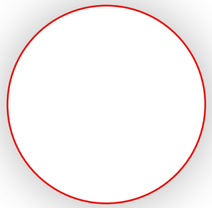
Deep SaaS Risk Context



Understand + Act

FireCloud

Remote User Visibility



Discover + Control

Firebox

Network Visibility + Control



See + Enforce

Governed AI + SaaS

One Operational Outcome

- Discover what's being used
- Understand who, what, and why
- Prioritize meaningful risk
- Approve, revoke, restrict, or remediate
- Prove improvement over time

Unknown → Governed

CloudDR Adds Depth. FireCloud and Firebox Expand Visibility and Control Across Remote Users and Networks.

Copyright © 2026 WatchGuard Technologies, Inc. All Rights Reserved.

Contatti:

Venite a trovarci al nostro Stand!