BROCHURE ILLUSTRATIVA DELLA SOLUZIONE

Sophos ITDR

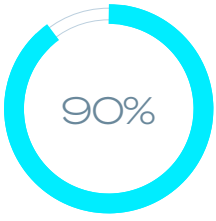
Neutralizza le minacce identity-based prima che possano causare danni alla tua azienda

Sophos Identity Threat Detection and Response (ITDR) blocca gli attacchi che sfruttano l'identità, monitorando continuamente il tuo ambiente alla ricerca di errori di configurazione e rischi di identità, fornendo allo stesso tempo dati di intelligence sulle credenziali compromesse, raccolti dal dark web.

Minacce all'identità: un problema di sicurezza sempre più diffuso

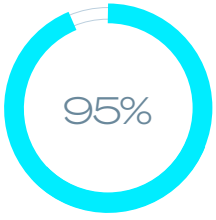
I sistemi di accesso e controllo basati sugli utenti si trovano in prima linea nel moderno panorama informatico e di cybersecurity, il passaggio al cloud e allo smart working non ha fatto altro che incrementare la complessità del monitoraggio e della protezione della superficie di attacco dell'identità. I cybercriminali sfruttano le identità compromesse, le vulnerabilità nelle infrastrutture e gli errori di configurazione per ottenere accesso non autorizzato a dati e sistemi sensibili. Di conseguenza, è sempre più importante intercettare gli utilizzi impropri dell'identità e bloccare gli attacchi basati sull'identità per garantire l'efficacia delle Security Operations.

I dati parlano chiaro

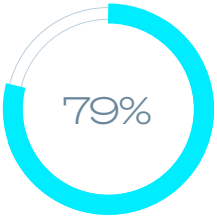


Percentuale di organizzazioni che l'anno scorso hanno subito almeno una violazione dell'identità[1].

Costo medio di una violazione dei dati[2].



Percentuale di ambienti Microsoft Entra ID con errori di configurazione critici[3].



Percentuale di violazione dei dati che riguardano l'identità[4].

La soluzione Sophos ITDR

Sophos ITDR previene gli attacchi basati sull'identità, monitorando continuamente il tuo ambiente per individuare eventuali rischi ed errori di configurazione dell'identità (un problema che riguarda il 95% delle organizzazioni), fornendo allo stesso tempo dati di intelligence sulle credenziali compromesse, raccolti nel dark web. Scopri i tuoi rischi di identità in pochissimi minuti (rispetto a vari giorni richiesti da altre soluzioni obsolete) e monitora l'evoluzione della tua superficie di attacco dell'identità nel tempo.

Vantaggi

- **Ottieni visibilità** con una visuale centralizzata dell'identità nei tuoi sistemi.
- **Scopri rapidamente** i rischi e gli errori di configurazione dell'identità, con consigli pratici su come agire.
- **Analizza continuamente** i sistemi per individuare eventuali cambiamenti nel profilo di identità.
- **Cerca nel dark web** per intercettare eventuali credenziali compromesse.
- **Rileva potenziali attività dannose** svolte da utenti interni o da posizioni e IP sconosciuti.
- **Rispondi alle minacce all'identità** con tempestività e precisione.
- **Si integra con Sophos MDR** per offrire opzioni di indagine e risposta alle minacce all'identità con l'intervento di esperti.

Riduci la tua superficie di attacco dell'identità

Sophos ITDR analizza continuamente il tuo ambiente Microsoft Entra ID per identificare all'istante errori di configurazione e lacune di sicurezza basate sull'identità, assegnando maggiore priorità ai problemi che richiedono un intervento immediato. I cybercriminali si servono di queste vulnerabilità per causare danni, ottenere privilegi più elevati e sferrare attacchi. Risolvi rapidamente i rischi, incluse le lacune nelle policy di accesso condizionale, le applicazioni rischiose, nonché gli account orfani e quelli con privilegi eccessivi.

Riduci il rischio di fuga e furto di credenziali

Secondo i dati di intelligence della Counter Threat Unit (CTU) di Sophos X-Ops, il numero di credenziali rubate che sono in vendita in uno dei principali marketplace sul dark web è raddoppiato negli ultimi 12 mesi. Sophos ITDR rileva e risponde alle minacce all'identità che riescono a eludere i tradizionali controlli di sicurezza basati sull'identità, proteggendo i sistemi dal 100% delle tecniche "Credential Access" (Accesso con credenziali) di MITRE ATT&CK[5]. La soluzione identifica i comportamenti rischiosi degli utenti, come i pattern di accesso insoliti, e mette in evidenza i casi in cui vengono utilizzate credenziali rubate o compromesse per accedere ai tuoi sistemi.

Ecco cosa offre Sophos ITDR

Catalogo delle identità
Ottieni visibilità con una vista centralizzata delle identità nei tuoi sistemi.

Valutazione continua del profilo di identità
Analizza continuamente il tuo ambiente Microsoft Entra ID per individuare errori di configurazione e lacune di sicurezza.

Monitoraggio delle credenziali compromesse sul dark web
Cerca credenziali compromesse sul dark web e nei database delle violazioni.

Analisi dei comportamenti degli utenti
Monitora le attività anomale associate al furto di credenziali o alle minacce interne.

Rilevamento avanzato delle minacce all'identità
Identifica fin dalle prime fasi della catena di attacco le attività sospette che indicano l'uso di tecniche cybercriminali specifiche.

Azioni di risposta alle minacce
Rispondi con rapidità e precisione: obbliga gli utenti a reimpostare la password, isola gli account che mostrano comportamenti sospetti e molto di più.

"Sophos ITDR ha migliorato significativamente la visibilità sui nostri rischi di identità. La visuale centralizzata nella nostra piattaforma XDR ci permette di inoltrare i rischi e gli errori di configurazione dell'identità evidenziati da Sophos ITDR a tutti i nostri programmi di sicurezza, migliorando così il profilo di cybersecurity dell'azienda e riducendo il rischio".

– Information Security Director, servizi finanziari

"Sophos ITDR individua i rischi in ambiti di Azure e dell'ecosistema Microsoft che in passato erano fonte di grande preoccupazione, come le lacune nelle policy di accesso condizionale e le applicazioni non sicure o dotate di privilegi eccessivi".

– Senior Information Security Officer

Integrazione con Sophos MDR

Sophos ITDR è completamente integrato in Sophos MDR, il servizio di Managed Detection and Response più attendibile a livello globale. Questa potente combinazione permette agli esperti di sicurezza di Sophos di monitorare, svolgere indagini e rispondere per conto tuo alle minacce basate sull'identità:

- Sophos ITDR crea automaticamente casi di MDR per i rilevamenti di minacce all'identità e per i risultati ad alto livello di rischio.
- Gli analisti di sicurezza di Sophos MDR indagano sui casi ed eseguono azioni di risposta per neutralizzare le minacce.

Esempio: credenziali trapelate sul dark web

- Sophos ITDR identifica le credenziali di un utente che sono in vendita in un popolare marketplace del dark web.
- Gli analisti di Sophos MDR sono in grado di bloccare l'account dell'utente e obbligarlo a reimpostare la password.

Esempio: furto di credenziali in uso

- Sophos ITDR identifica gli accessi sospetti da paesi, dispositivi e indirizzi IP mai riscontrati prima.
- Gli analisti di Sophos MDR sono in grado di bloccare l'account dell'utente compromesso e di terminare tutte le sessioni attive.

Insieme è meglio: Sophos ITDR + Microsoft Entra ID

Microsoft Entra ID è fondamentalmente uno strumento di gestione delle identità e degli accessi (Identity and Access Management, IAM) che offre gestione delle identità e dei gruppi, controllo dell'accesso basato sui ruoli (Role-Based Access Control, RBAC), gestione degli accessi privilegiati (Privileged Access Management, PAM) e policy di accesso condizionale. Fornito come console unificata per il rilevamento e la neutralizzazione delle minacce e dei rischi di identità, Sophos ITDR va oltre le funzionalità IAM di base, includendo anche opzioni di igiene dell'identità, monitoraggio del dark web, rilevamento avanzato delle minacce e molto di più. **La combinazione di Entra ID e Sophos ITDR garantisce il sistema di protezione dell'identità più completo per la tua azienda.**

Licenze semplici

Sophos ITDR è facile da distribuire, da usare e da acquistare. Le licenze semplici, basate su sottoscrizioni che tengono conto del numero di utenti e server presenti nella tua organizzazione, garantiscono prezzi prevedibili. Puoi scegliere di aggiungere Sophos ITDR alla soluzione Sophos XDR o al servizio Sophos MDR, a seconda delle tue esigenze.

- **Add-on per il servizio Sophos Managed Detection and Response (MDR):** gli esperti di sicurezza di Sophos monitorano, svolgono indagini e rispondono per conto tuo alle minacce basate sull'identità.
- **Add-on per il prodotto Sophos Extended Detection and Response (XDR):** il tuo team interno utilizza gli strumenti Sophos di rilevamento, indagine e risposta basati sull'IA in combinazione con Sophos ITDR.

Gartner

Uno dei vendor "Customers' Choice" 2025 di Gartner® Peer Insights™ per i servizi di Extended Detection and Response (XDR).

Tra i Leader nei G2 Overall Grid® Reports per Extended Detection and Response (XDR) e Managed Detection and Response (MDR).

MITRE | ATT&CK® Evaluations

Ottimo Performer nelle valutazioni MITRE ATT&CK® per i Servizi gestiti e i Prodotti Enterprise.

FROST & SULLIVAN

Tra i Leader nel Frost Radar™ 2025 di Frost & Sullivan, categoria Managed Detection and Response.

Per scoprire di più, visita
sophos.it/ITDR

1 - Studio Identity Defined Security Alliance (IDSA) 2024.
2 - IBM, Cost of a Data Breach 2024.
3 - Ricerche svolte dal team Sophos Incident Response.
4 - Identity Defined Security Alliance.
5 - In base ai sistemi di rilevamento disponibili, mappati al framework MITRE ATT&CK.

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

2025-09-15 BR-IT (MP)

SOPHOS