VICSAMGROUP

VICSAM GROUP DIGITAL WEEK

45 anni di innovazione.
Una settimana per guardare avanti.

dal 20 al 24
Cassago
Ottobre
2025

www.vicsamgroup.it

Agenda

01. Centro di competenze

02. Un viaggio di mezzo secolo

03. La sicurezza digitale come servizio

04. Governa gli accessi e proteggi i tuoi dati

05. Real security for the real world

06. La parola all’esperto MotoGP Vibe

Un’azienda Gruppo, non un gruppo di aziende

VICSAM

LEFT

ducky NETWORK

Content is King

WORKCOM

NETYS

LARTNETWORK TELEFONIA & TELEMATICA

VICSAM

Business Unit

Retail Solutions

Software Solutions

Business Analysis & Consulting

ICT - Cloud & Security Services

Marketing HUB

Print Solutions

VICSAM

ICT - Cloud & Security Services

Centro di competenze

Intervento a cura di

Davide Guzzi

CBO | Chief Business Officer - Cloud & Security Services

VICSAM GROUP DIGITAL WEEK

VICSAM GROUP DIGITAL WEEK

Cassago
20-24
Ottobre
2025

OLTRE 20 PARTNER TECNOLOGICI

5 SALES SPECIALIST

35 TECNICI SISTEMISTI

NOC + LIGHT SOC E SOC AS A SERVICE

VICSAM GROUP

VICSAM GROUP DIGITAL WEEK

Cassago
20-24
Ottobre
2025

PARTECIPAZIONE OLTRE 30 EVENTI

18 CERTIFICAZIONI SALES SPECIALIST

22 CERTIFICAZIONI TECNICHE

NIS 2 E ISO 27001 COMPLIANCE

VICSAM GROUP

VICSAM GROUP DIGITAL WEEK

Cassago
20-24
Ottobre
2025

Un viaggio dal 1980 a oggi

Come la **trasformazione tecnologica** ha ridefinito il **presente** e le **sfide della cybersecurity**

1980
Tre soci davanti a un bar fondano l'azienda

1981
Arriva l'IBM PC: inizia l'era del personal computer.

1984 *
Apple lancia il Macintosh, con grafica e mouse.

1990
Windows 3.0 porta i PC nelle case di tutti.

1991
Nasce Linux: rivoluzione open source.

1993 - 1995
Internet commerciale e **W**orld **W**ide **W**eb aprono la strada alla rete globale.

2000
Millennium Bug: primo grande stress test dei sistemi informatici.

2002
Introduzione dell'euro: adeguamento massivo dei software.

2004
Nascono i social network: Facebook e LinkedIn cambiano la comunicazione.

2007
iPhone inaugura l'era degli smartphone.

2008 - 2010
Il cloud computing diventa mainstream.

2018
GDPR: nuova centralità dei dati personali.

2020
La **pandemia** accelera smart working e videoconferenze.

2022 - 2024
Cyberwar: il conflitto russo-ucraino + **NIS2**

2025 - Oggi e futuro
6 sedi Lombardia, Emilia, Veneto
Oltre 200 dipendenti
6 business unit

VICSAM GROUP

VICSAM GROUP DIGITAL WEEK

Cassago
20-24
Ottobre
2025

ICT – Cloud & Security Services Specialist

Alessandra Pagani

WatchGuard
hp
ZEBRA
Microsoft

Riccardo Esposito

REEVO Acronis
Cyber Guru

Marco Taddeo

/LIBRAESVA
hp
Cyber Guru
safetica
WatchGuard

Silvia Sironi

DraftSight
DASSAULT SYSTEMES
LART NETWORK TELEFONIA & TELEMATICA
SOLIDWORKS

VICSAM GROUP

VICSAM
ICT - Cloud & Security Services

La sicurezza digitale come servizio

Intervento a cura di

Claudio Paneari

Sales Solution Architect

REEVO

YAMAHA FACTORY RACING

2025 OFFICIAL SPONSOR

VICSAM GROUP DIGITAL WEEK

REEVO
Cloud & Cyber Security

REEVO
Cloud & Cyber Security

SIAMO UN **PROVIDER EUROPEO PER CLOUD, CYBERSECURITY E CLOUD NATIVE** CON L'OBIETTIVO DI **PROTEGGERE I DATI DELLE AZIENDE E DELLE ORGANIZZAZIONI NEL NOSTRO CAVEAU DIGITALE**, CON L'INTENTO DI **ACCELERARE LA TRASFORMAZIONE DIGITALE** E RENDERE LE **PERFORMANCE, LA SECURITY, E LA RESILIENZA IL NOSTRO MARCHIO DISTINTIVO**.

REEVO
Cloud & Cyber Security

COSA FACCIAMO

CLOUD

TI CONSENTIAMO DI AFFRONTARE LA TUA TRASFORMAZIONE DIGITALE IN TUTTA TRANQUILLITÀ GRAZIE A UN PORTAFOGLIO DI SERVIZI CLOUD CHE COPRE TUTTE LE ESIGENZE IN MATERIA DI INFRASTRUTTURA, PROTEZIONE DEI DATI, SICUREZZA E CONTINUITÀ OPERATIVA.

CYBERSECURITY

METTIAMO LA PROTEZIONE DEI DATI AL CENTRO DELLA NOSTRA MISSIONE E ABBIAMO DECISO DI FORNIRE SOLUZIONI E SERVIZI DI CYBERSICUREZZA DI PRIM'ORDINE, CONSENTENDO ALLE ORGANIZZAZIONI DI ADOTTARE IL NOSTRO APPROCCIO DI SICUREZZA FIN DALLA PROGETTAZIONE.

CLOUD NATIVE

LE NOSTRE SOLUZIONI SI BASANO SU UNA FILOSOFIA DI SICUREZZA BY DESIGN PER RISOLVERE LE PROBLEMATICHE RELATIVE ALLA SOVRANITÀ DEI DATI E ALLA CONFORMITÀ NORMATIVA.

FORNIAMO UN'ALTERNATIVA EUROPEA SICURA E CONFORME AGLI STANDARD GLOBALI DEGLI HYPERSCALER.

CERTIFICAZIONI, ACCREDITAMENTI, QUALIFICAZIONI

GESTIONE E QUALITÀ
ISO 9001

GESTIONE AMBIENTALE
ISO 14001

IT SERVICE MANAGEMENT
ISO 20000

GESTIONE DEI DATI E DELLE INFORMAZIONI SICUREZZA
ISO 27001

GESTIONE DELLA SICUREZZA PER I CLOUD PROVIDER
ISO 27017

GESTIONE DEI DATI PERSONALI IN CLOUD
ISO 27018

PRIVACY INFORMATION MANAGEMENT
ISO 27701

INFORMATION SECURITY INCIDENT MANAGEMENT
ISO 27035

GESTIONE DELLA BUSINESS CONTINUITY
ISO 22301

SISTEMI DI CONTROLLO PER EROGAZIONI DI SERVIZI IT
ISAE 3402 TYPE II

IDENTIFICAZIONE E CLASSIFICAZIONE DEL RISCHIO
SSAE 18 TYPE II

GARANZIA DI CONTINUITA' DEL DATA CENTER
RATING 4 E/O ANSI TIA 942

QUALIFICAZIONE DEI SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE
ACN QI2 QC2

GARANZIA DELLA QUALITÀ DEI SERVIZI CYBER SECURITY
CYBER SECURITY MADE IN EUROPE

CLOUD SECURITY ALLIANCE
CSA STAR L2

CODICE DI CONDOTTA SULL'UTILIZZO DI STRUMENTI PER LA PROTEZIONE DEI DATI
CISPE

RESPONSABILITÀ AMMINISTRATIVA DI IMPRESA
MODELLO 231

GESTIONE PER LA PARITÀ DI GENERE
PDR UNI 125:2022

REEJO
Cloud & Cyber Security

YAMAHA FACTORY RACING

OFFICIAL
SPONSOR 25/26

REEVO
Cloud & Cyber Security

COSA INTERESSA ALLE AZIENDE?

RICAVI –
COSTI =

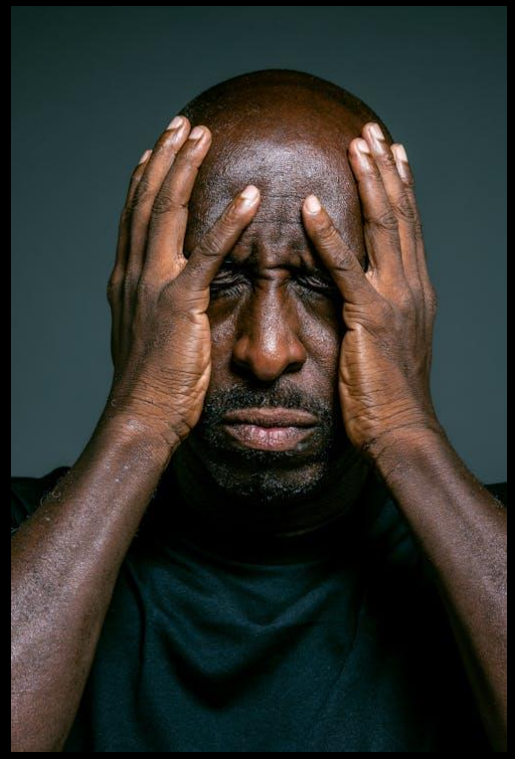
_____

MARGINE

REEVO
Cloud & Cyber Security

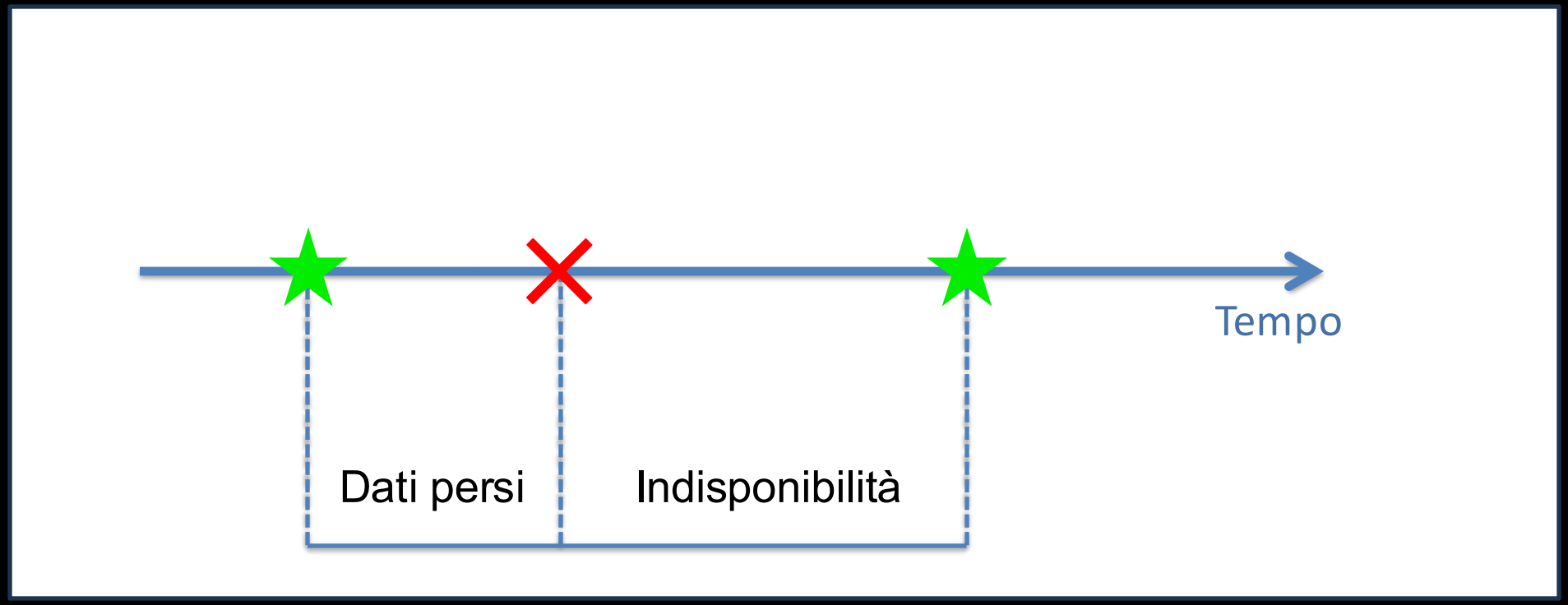
COSA PUÒ INTERROMPERE IL FUNZIONAMENTO IT?

- Disastri naturali (terremoti, alluvioni, ecc)
- Guasti
- Problemi software
  - aggiornamenti
  - corruzione dati, ecc
- Cancellazione dati (colposa o dolosa)
- Attacchi informatici (ransomware, DDos, ecc)



REEVO
Cloud & Cyber Security

ANATOMIA DI UN DISASTRO



REEVO
Cloud & Cyber Security

I DANNI

- Improduttività: struttura pagata per niente
- Indisponibilità: no valore aggiunto
- Ripristino sistemi: riscostruire infrastruttura
- Perdita integrità: ricostruire dati persi
- Perdita riservatezza: dati in mano esterna
- Perdita immagine: credibilità

REEVO
Cloud & Cyber Security

IL CONTESTO

- Attacchi sono all'ordine del giorno
  - campagne di phishing
  - credenziali trafugate
  - vulnerabilità non sanate

- Spesso «down» costa più dell'incidente in sé

- Gli attacchi informatici fanno parte del lavoro come:
  - cedolini
  - commercialista
  - fatture

REEVO
Cloud & Cyber Security

SECURITY AS A SERVICE

- Abbonamento a
  - competenze
  - strumenti
  - processi
  - eventualmente (H24)

- Responsabilità tua: asset e decisioni
- Responsabilità fornitore: monitoraggio, processi, contenimento
- Non è «magia», non sostituisce best practice di igiene informatica

REEVO
Cloud & Cyber Security

SICUREZZA PREVENTIVA

- Valutazioni cicliche/continue
  - analisi superficie di attacco esterna
  - analisi superficie di attacco interna
  - cyber risk assessment

- Implementare azioni di correttive

- Obiettivo: ridurre la superficie di attacco, non essere attrattivi

REEVO
Cloud & Cyber Security

SICUREZZA REATTIVA

- Monitoraggio di ciò che succede nella rete, in «tempo reale»
- Prelevamento di allarmi e informazioni: correlazione
- Pulizia del «rumore di fondo», allarmi qualificati
- Obiettivo:
  - bloccare sul nascere gli attacchi, contenimento
  - reagire in minuti/ore, non giorni

REEVO
Cloud & Cyber Security

LE 5 DOMANDE PER VALUTARE UN FORNITORE

- Che visibilità mi date (console/dashboard, report, ecc)?
- Quali sono i tempi garantiti (SLA, contenimento)?
- Copertura H24?
- Chi fa cosa in un incidente (processi e responsabilità)?
- Quali sono i costi (chiari e fissati)?

REEVO
Cloud & Cyber Security

LA SICUREZZA A CASA...

- Cancello all'ingresso del palazzo
- Portone all'ingresso della scala
- Porta di casa blindata
- Allarme collegato alla centrale
- Pronto intervento o pattuglia

...E NEL MONDO CYBER

- Firewall
- EDR, Cyber Risk Assessment, 2FA
- Penetration Test, Attack Surface Management
- Security Operation Center
- Incident Response

REEVO
Cloud & Cyber Security

TAKEAWAY – IL SUCCO DEL DISCORSO

- La cyber security è un TUO problema, non del fornitore
- Dal fornitore compri tempo e competenza
- Sicurezza preventiva riduce la probabilità dell'attacco
- Sicurezza reattiva e contenimento riducono l'impatto
- Sfida: scegliere il fornitore giusto

VICSAM
ICT - Cloud & Security Services

Governa gli accessi e proteggi i tuoi dati

netwrix

Intervento a cura di

Sergio Gulli

Sales Manager Italy e Malta

VICSAM GROUP DIGITAL WEEK

La sicurezza non è una destinazione, è un viaggio

Come puoi essere sicuro che la tua azienda domani sarà più sicura di quanto non lo sia oggi?

Lo stato della Sicurezza dei Dati

Proliferazione e diffusione incontrollata dei dati

La proliferazione incontrollata dei dati si riferisce alla diffusione incontrollata di dati nella rete, nei dispositivi e nelle applicazioni di un'organizzazione.

Aumento e inasprimento delle normative

Gestire il rischio e soddisfare i requisiti normativi è un compito complesso, esacerbato dai rischi emergenti.

Prevalenza di attacchi ransomware

Ogni giorno si verificano 1,7 milioni di attacchi ransomware, il che significa 19 attacchi ransomware ogni secondo.

Attackers using AI

Ransomware as a service

Insider threats

Attacker using AI

- Deep Fakes
- Phishing
- Smishing / Vishing
- Brute-forcing

People & Identities

- Standing privileges
- Shadow access
- Weak passwords
- Low Visibility
- Over-Privileged Accounts

Data at risk

I rischi dell'AI

Gli strumenti di AI generativa offrono enormi vantaggi in termini di produttività, ma comportano **rischi significativi**:

1. **Fuga di dati sensibili:**
   - ChatGPT e Copilot possono **memorizzare e rigenerare** dati inseriti dagli utenti, inclusi documenti riservati, codice proprietario o informazioni personali.
   - Secondo uno studio di Netskope, il **46% delle violazioni** di policy GenAI coinvolge codice sorgente proprietario condiviso con modelli pubblici.

2. **Hallucination e risposte errate:**
   - I modelli generativi possono creare contenuti **inesatti o fuorvianti**, con impatti legali e reputazionali. Circa il **17% dei contenuti generati** in ambito business contiene errori.

3. **Shadow AI e uso non autorizzato:**
   - Dipendenti possono usare strumenti AI **non approvati**, esponendo l'azienda a rischi di compliance e data leakage. Il 48% degli utenti ha caricato dati sensibili in strumenti AI pubblici.

4. **Attacchi di prompt injection**
   - Attori malevoli possono manipolare i modelli per far emergere dati di addestramento o contenuti riservati.

Secondo l'indagine Technology & Work (2025):

il 48% dei dipendenti ha ammesso di caricare dati aziendali sensibili in strumenti pubblici di intelligenza artificiale.

Come vengono sfruttati dai criminali

Un attaccante potrebbe usare un'altra IA, magari un modello di linguaggio come **ChatGPT**, per automatizzare la ricerca. L'attaccante potrebbe:

Chiedere a ChatGPT di generare una serie di **query di ricerca avanzate** (dorking) per motori di ricerca come Google o Bing, mirate a trovare stringhe di testo specifiche che indicano la presenza di dati sensibili (es: `"API key" github.com`, `"password" site:pastebin.com`)

Usare l'IA per analizzare rapidamente i risultati di ricerca, scartando i falsi positivi e identificando i file che contengono dati potenzialmente “utili” o non.

Sfruttare un'altra IA per analizzare il codice trovato, evidenziando le parti che sembrano essere chiavi API valide o credenziali.

Questo processo, che manualmente richiederebbe ore, può essere completato in pochi minuti con l'ausilio dell'intelligenza artificiale. L'esempio dimostra non solo la vulnerabilità, ma anche come l'IA possa essere utilizzata per **amplificare le minacce esistenti**.

“Non è sempre un hacker con una felpa con cappuccio,
a volte è solo il famoso ‘’Utonto’’ che fa clic sul link sbagliato
...di nuovo!!!”

Come difendersi?

- **Politiche aziendali chiare:** Stabilire linee guida precise sull'utilizzo degli strumenti AI, vietando l'inserimento di dati sensibili.
- **Formazione del personale:** Educare i dipendenti sui rischi e sull'importanza di non "inquinare" i modelli AI con informazioni riservate.
- **Utilizzo di versioni locali o private:** Laddove possibile, optare per modelli AI gestiti internamente all'azienda, che non condividono dati con l'esterno.
- **Verifica e monitoraggio:** Implementare sistemi che scansionano e rilevano la presenza di dati sensibili in archivi pubblici.

COSA MANCA?

Quali sono i vostri processi di sicurezza?

ATTACK SURFACES		MITIGATE		REMEDIATE		
		IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
	DATA	Quali sono i dati sensibili?	Chi deve avere accesso a dati sensibili?	Chi accede a dati sensibili?	Devo segnalare una violazione dei dati?	Quali dati devo essere recuperati?
	IDENTITY	Quali account sono a rischio e perché?	Come eliminare i privilegi permanenti?	Ci sono attività improprie da parte degli utenti?	Come rispondere più velocemente a una minaccia?	Come annullare le modifiche AD improprie?
	INFRASTRUCTURE	Cosa ci rende vulnerabili alle minacce?	Come evitare modifiche ingiustificate?	Quali modifiche alla configurazione non sono state approvate?	Come si è verificato un incidente?	Come si sarebbe potuto fermare un incidente?

Quali sono le risposte?

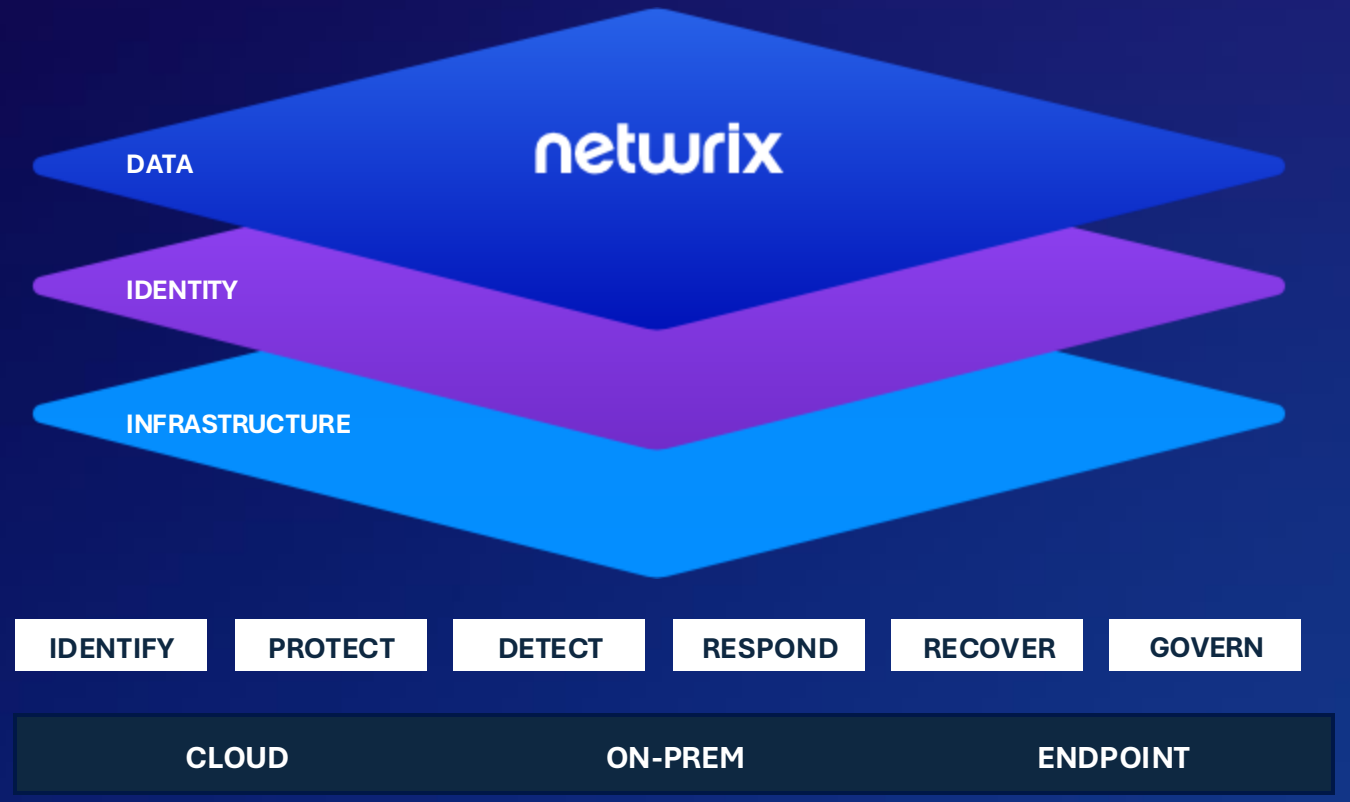
ATTACK SURFACES	MITIGATE		REMEDIATE		
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DATA	Trovare e classificare i dati sensibili	Gestire l'accesso ai dati sensibili	Controllare e verificare l'accesso ai dati sensibili	Facilitare la segnalazione di una violazione dei dati	Velocizza il recupero dei dati
IDENTITY	Scoprire gli account a rischio	Proteggere gli accessi privilegiati e gestire le identità	Trovare un'attività utente impropria	Automatizza la risposta alle minacce correlate all'identità	Annullare modifiche ad AD improprie
INFRASTRUCTURE	Contrassegnare le vulnerabilità nelle risorse IT	Prevenire modifiche rischiose alla configurazione	Contrassegnare le modifiche impreviste alla configurazione	Abilita l'analisi forense degli incidenti	Migliora la gestione degli incidenti e le indagini

Quali sono le tecnologie?

ATTACK SURFACES	MITIGATE		REMEDIATE		
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DATA	Data Discovery e Data Classification DLP **DSPM**	Audit e Access Review DLP **DSPM**	Audit e Data Classification DLP **DSPM**	Audit e Data Classification DLP **DSPM**	Audit e Backup
IDENTITY	IAM e IGA	PAM	Behavior Anomaly Detection	ITDR	AD Recovery
INFRASTRUCTURE	VA e PENTEST	FIM	Configuration Management e hardening	Threat Detection	ITDR

Il nostro approccio

- Soluzioni end-to-end
- Colmare le lacune
- Creare connessioni



Le nostre Tecnologie

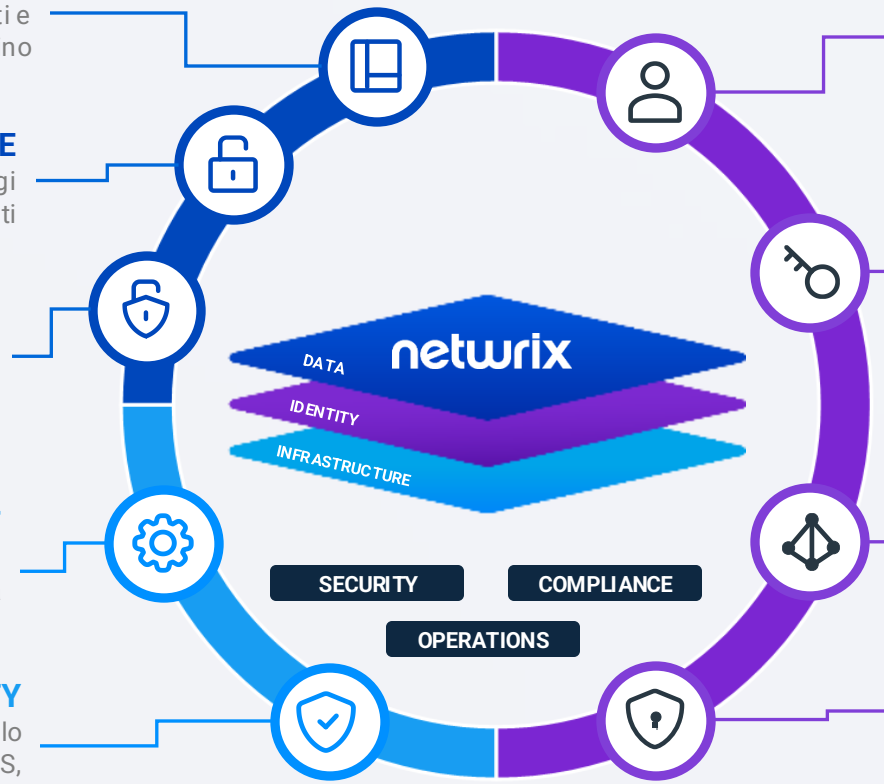
DATA DISCOVERY & CLASSIFICATION
Individua e classifica i dati sensibili non strutturati e strutturati ovunque si trovino

DATA ACCESS GOVERNANCE
Allinea i diritti di accesso ai dati con i principi dei privilegi minimi per i dati strutturati e non strutturati

DATA LOSS PREVENTION
Scopri, monitora e proteggi i dati sensibili da fughe di notizie involontarie e dannose su tutti gli endpoint Windows, Mac e Linux

SECURITY CONFIGURATION MANAGEMENT
Mitigare i rischi operativi e di sicurezza attraverso l'identificazione proattiva delle deviazioni della configurazione

ENDPOINT MANAGEMENT & SECURITY
Configura, distribuisci e controlla facilmente le policy e lo spostamento dei dati da/verso gli endpoint utente multi-OS, applicando al contempo i privilegi minimi



IDENTITY GOVERNANCE & ADMINISTRATION
Provisioning, deprovisioning e gestione dei diritti acquisiti in modo accurato e tempestivo

PRIVILEGED ACCESS MANAGEMENT
Raggiungi l'obiettivo Zero Standing Privilege con un approccio effimero, just-in-time e just-enough privilege

ACTIVE DIRECTORY SECURITY / ITDR
Assicurati che AD sia pulito, compreso, configurato correttamente, monitorato attentamente e controllato rigorosamente

PASSWORD MANAGEMENT & SECURITY
Garantisci password complesse, univoche e non compromesse, con accessi semplificati e condivisione sicura

Portfolio

DATA DISCOVERY & CLASSIFICATION

- Data Classification
- Access Analyzer

DATA ACCESS GOVERNANCE

- Auditor
- Access Analyzer
- 1Secure

DATA LOSS PREVENTION

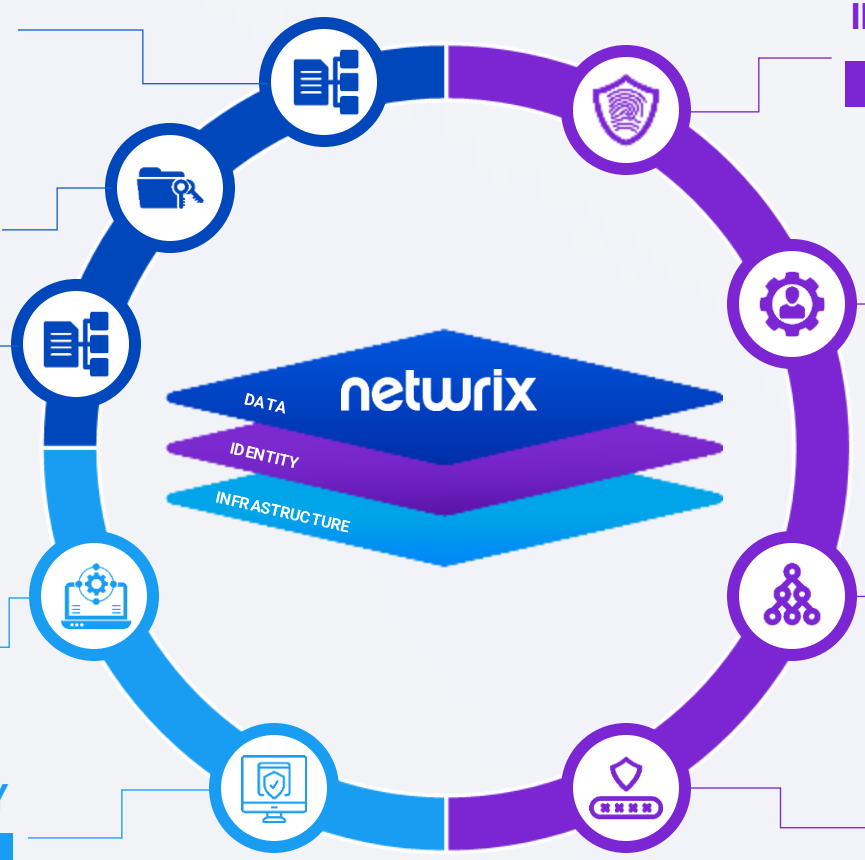
- Endpoint Protector

SECURITY CONFIGURATION MANAGEMENT

- Change Tracker
- Platform Governance

ENDPOINT MANAGEMENT & SECURITY

- Endpoint Protector
- Endpoint Policy Manager



IDENTITY GOVERNANCE & ADMINISTRATION

- Identity Manager
- Directory Manager

PRIVILEGED ACCESS MANAGEMENT

- Privilege Secure
- Endpoint Policy Manager

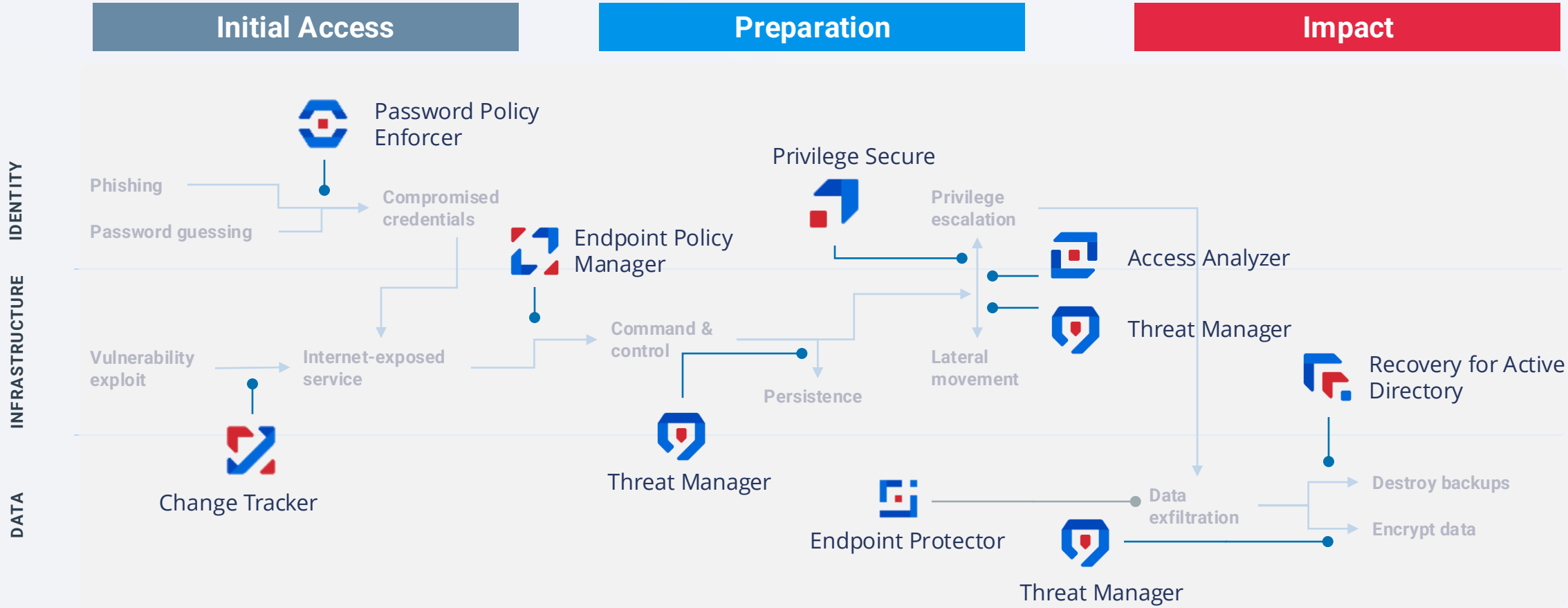
ACTIVE DIRECTORY SECURITY / ITDR

- Privilege Secure
- Endpoint Policy Manager
- Recovery for AD
- Auditor
- Access Analyzer
- Threat Manager
- Threat Prevention
- Directory Manager
- PingCastle

PASSWORD MANAGEMENT & SECURITY

- Password Policy Enforcer
- Threat Prevention
- Directory Manager
- Password Secure

Come avviene una violazione e Netwrix Mapping



Netwrix Solutions To Accelerate Your Success

Identity Management

Proteggere e governare in modo efficace le identità digitali, gestendo i loro accessi e le loro autorizzazioni e garantendo controlli di accesso appropriati e conformità alle normative.

Privileged Access Management

Ridurre il rischio di compromissione,: proteggere, controllare, gestire e monitorare l'uso degli account privilegiati. Eliminarli e gestire l'accesso utilizzando un approccio just-in-time e con privilegi appena sufficienti.

Data Security Posture Management

DSPM – protezione dei dati sensibili da accessi non autorizzati, violazioni, perdite e usi impropri fornendo visibilità su dove risiedono i dati sensibili, chi vi ha accesso e come sono stati utilizzati.

Identity Threat Detection & Response

Proteggere, rafforzare e difendere in modo completo la propria infrastruttura di identità, (AD ed Entra ID), eliminando i punti ciechi, rilevando minacce sofisticate in tempo reale, impedendo agli aggressori di sfruttare le identità e garantendo un ripristino rapido per ridurre al minimo le interruzioni dell'attività.

Endpoint Management

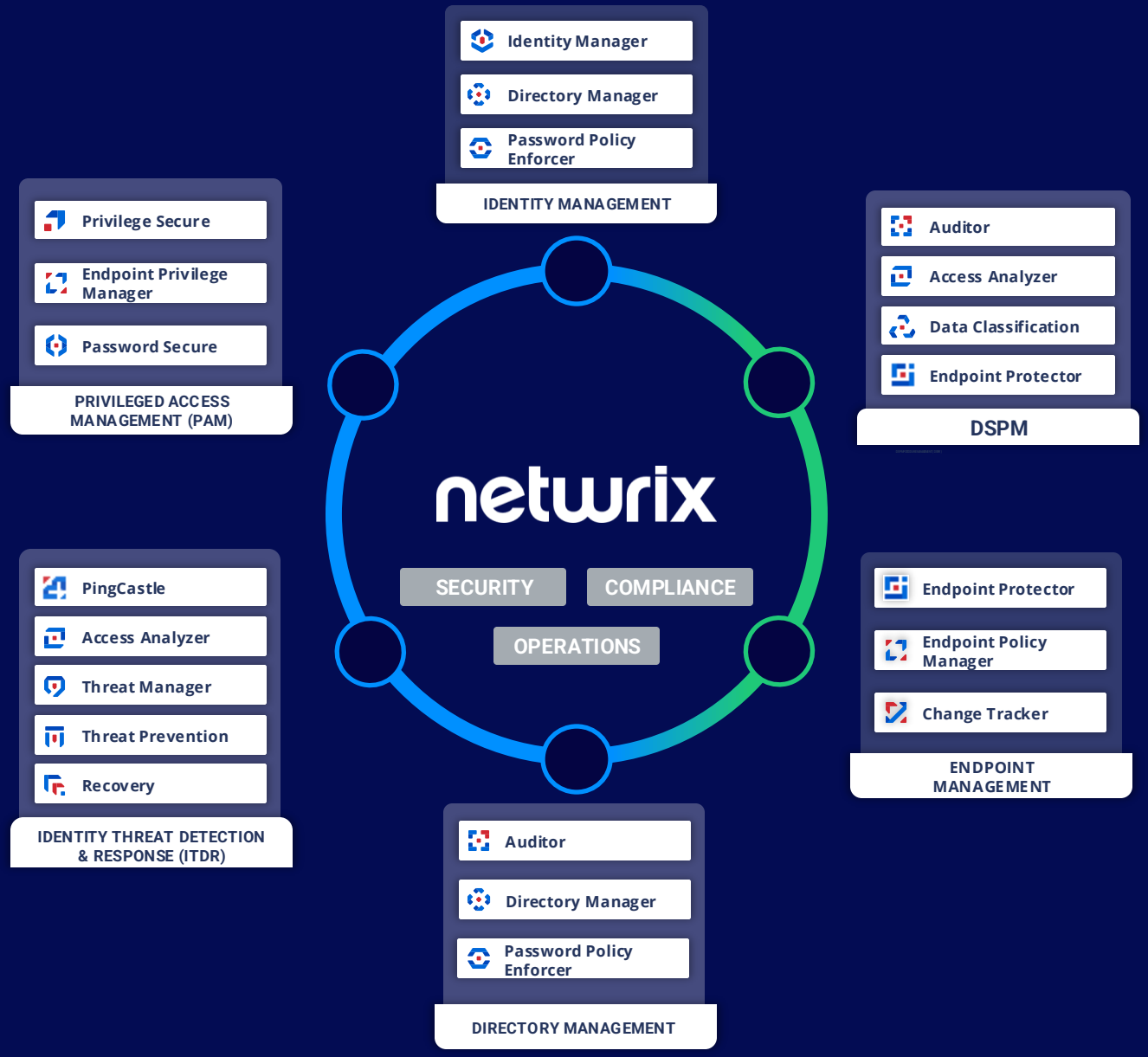
La gestione degli endpoint consente di proteggere e gestire i propri dispositivi endpoint, salvaguardando i dati e ottimizzando le prestazioni dei dispositivi e degli utenti.

Directory Management

Le directory di identità sono sicure quando sono pulite, comprese, monitorate attivamente, configurate correttamente e strettamente controllate.

netwrix

Netwrix Solutions To Accelerate Your Success



netwrix

Chi ben comincia è a metà dell’opera

E ricordatevi anche dell’altra metà dell’opera

netwrix

Identità
sono il vettore di attacco #1

Non è possibile
proteggere i dati
senza proteggere l'identità.

Zero Standing Privilege

Il nuovo approccio alla gestione degli accessi privilegiati

Ridurre la superficie di attacco rimuovendo i privilegi permanenti

- Rimuovere i privilegi permanenti per ridurre i rischi
- Concedere l'accesso giusto agli utenti giusti
- Protezione dei diritti di amministratore locale
- Ridurre al minimo la superficie di attacco ripulendo gli oggetti con accesso privilegiato
- Proteggere gli account di servizio e quelli integrati
- Avanzare verso la **ZERO TRUST**

netwrix

Non puoi proteggere ciò che non sai di avere

Prima di capire il come dovresti capire il cosa proteggere

Data Security Posture Management DSPM

Definizione

Secondo Gartner, la Data Security Posture Management (DSPM) è un insieme di strumenti e pratiche che forniscono visibilità sulla posizione dei dati sensibili, su chi ha accesso a essi e su come vengono utilizzati, oltre a valutare la postura di sicurezza del sistema o dell'applicazione in cui sono archiviati.

Goal

Data Security Posture Management : proteggere i dati sensibili da accessi non autorizzati, violazioni, perdite e usi impropri fornendo visibilità su dove risiedono i dati sensibili, chi vi ha accesso e come sono stati utilizzati.

netwrix

DSPM Data Security Posture Management

I Problemi

ACCESSO ECCESSIVO

DIRITTI AMMINISTRATIVI E DI ACCESSO COMPLESSI

RISCHI SCONOSCIUTI

REQUISITI DI COMPLIANCE

SANS

"In those 12 incidents, only 14 percent of the information that was targeted and stolen by an adversary was needed by the owner of the compromised account."

netwrix

Data Security Posture Management – How?

01
DISCOVER

Discover dati sensibili, regolamentati e mission-critical.

02
ASSESS

Identifica, assegna priorità e **risolvi** i rischi e le lacune di sicurezza prima di una violazione.

03
PROTECT

Controlla l'accesso alle informazioni sensibili, previeni la perdita di dati e mantienile sempre al sicuro.

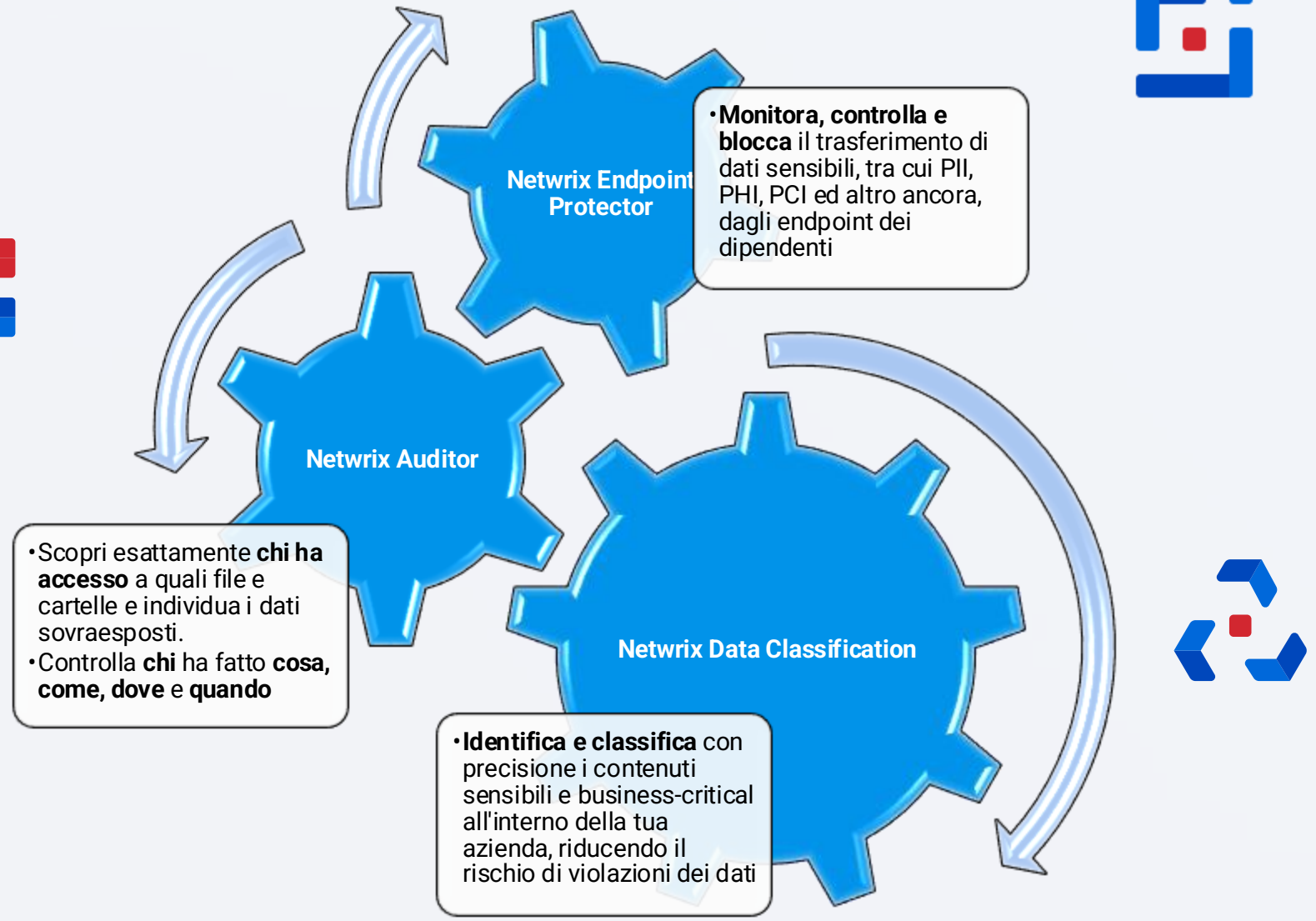
04
DETECT

Rileva comportamenti sospetti per accelerare le indagini e la risposta

05
INVESTIGATE

Analizza gli incidenti di sicurezza e **implementa** le lezioni apprese per rafforzare i dati.

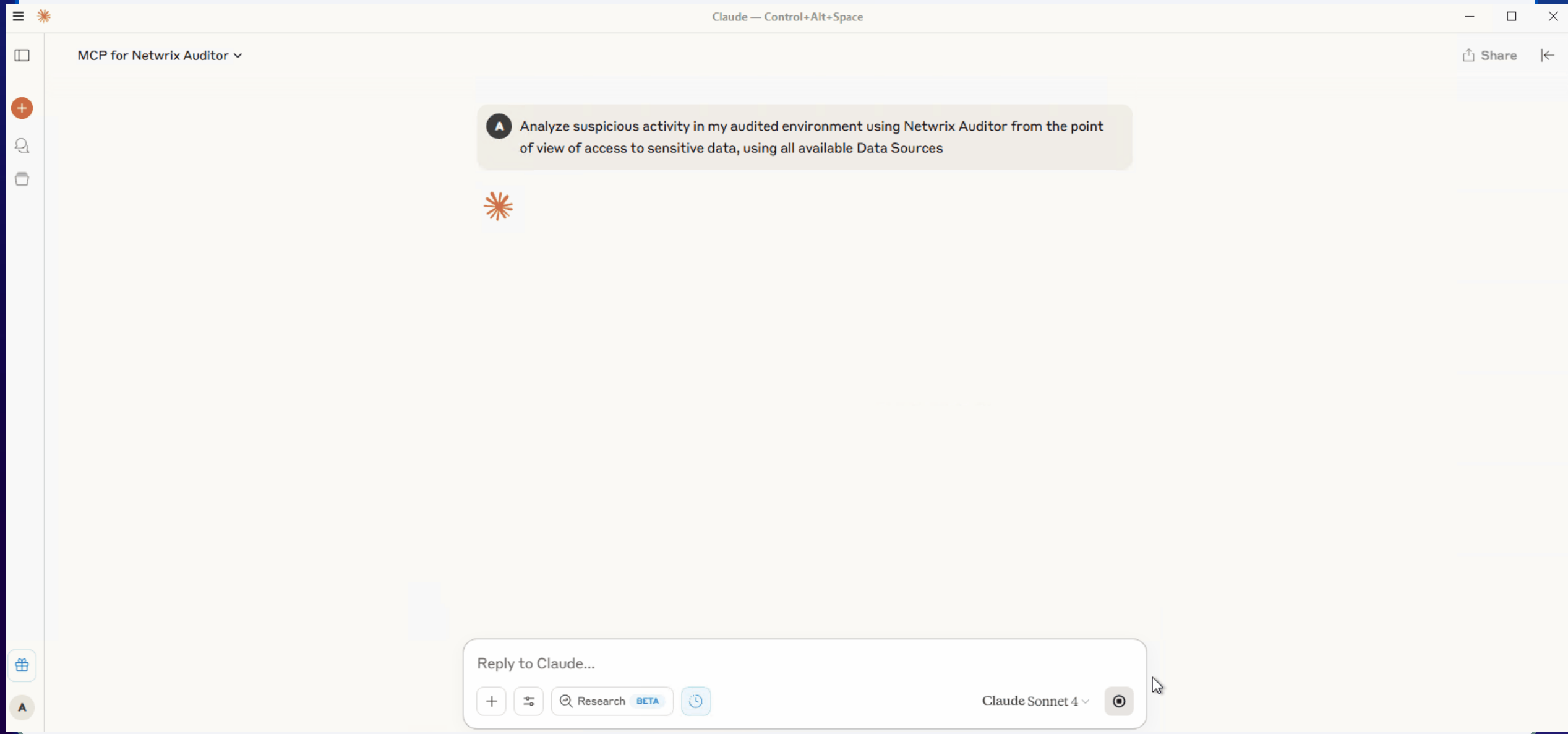
Netwrix da DLP a DSPM



MCP Server Netwrix

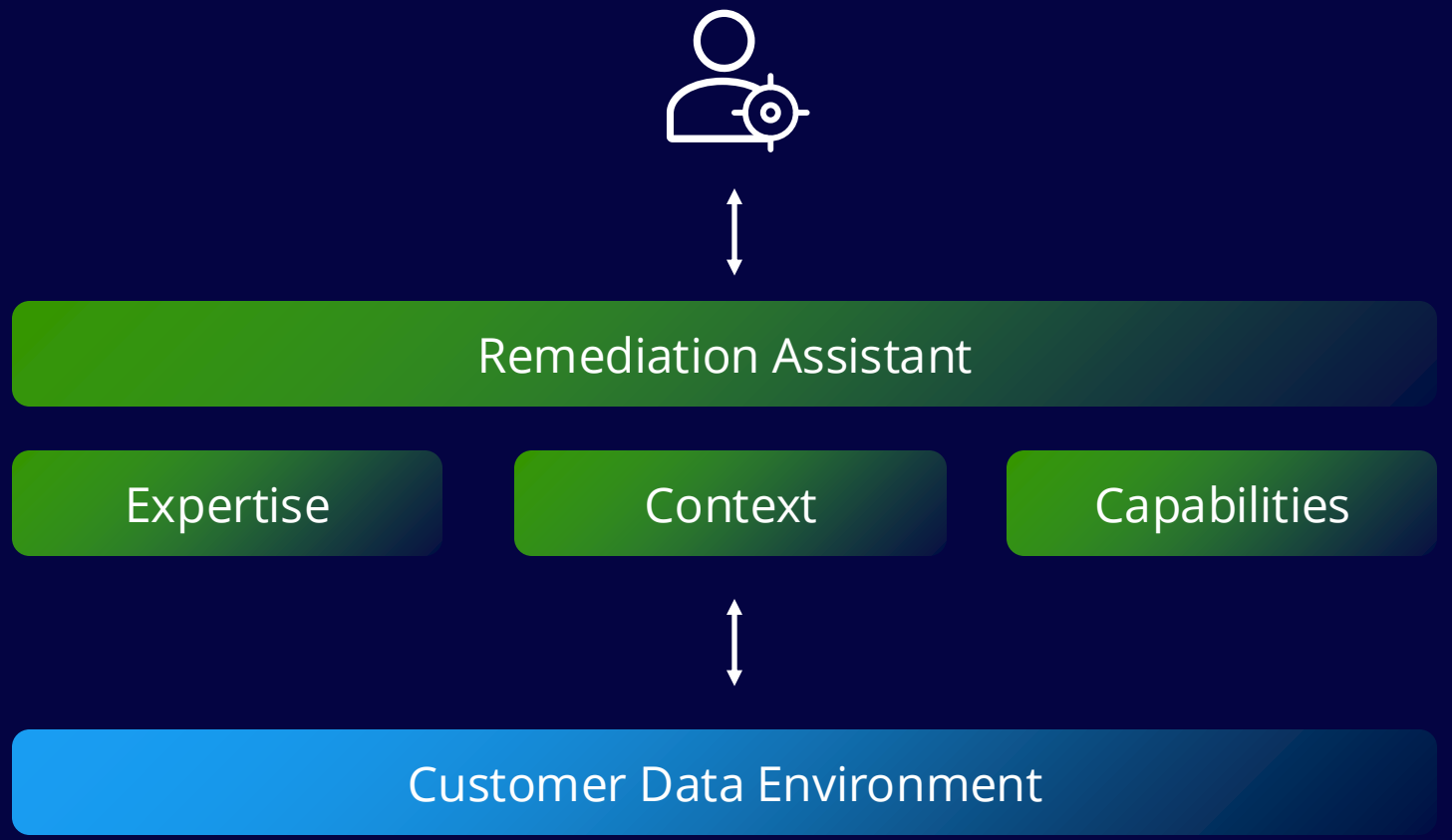
L’ AI come strumento di analisi e difesa

netwrix


Claude — Control+Alt+Space
MCP for Netwrix Auditor
Share
Analyze suspicious activity in my audited environment using Netwrix Auditor from the point of view of access to sensitive data, using all available Data Sources
Reply to Claude...
Research
BETA
Claude Sonnet 4

Integrazione del server MCP tra i prodotti

Dai priorità alle azioni correttive con Netwrix AI



- Summarize risks
- Understand impact
- Generate remediation steps for admins

1Secure DSPM **NEW**

1Secure powered by PingCastle **NEW**

NETWRIX 1SECURE

Home | Reports | Configuration

Help | Brett Bodenburg, Netwrix

Home → Chris Overton → Risk Assessment

Risk Assessment

Chris Overton | Trend since: Last month | Risk Profile Preview: Default Profile | Subscribe | Export

High	Medium	Low	Since last month	Since last month
10	0	21	3 risk(s) rising	2 risk(s) falling

All risks | All categories | All MITRE tactics | All MITRE techniques | All severities | All trends | All types | Filter by keyword

Risk metric / Severity / Trend

Administrative Accounts Susceptible to Kerberoasting — Powered by PingCastle

High | No change: 2 / 1.2k (0.17%) user(s) | Identity | Initial Access | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Valid Accounts | Steal or Forge Kerberos Tickets | OS Credential Dumping

Dangerous Default Permissions

High | Detected: Nov 07, 2024 | Identity | Privilege Escalation | Abuse Elevation Control Mechanism

Domain Controller SMB v1 Vulnerability — Powered by PingCastle

High | No change: 1 / 1 (100%) computer(s) | Infrastructure | Collection | Credential Access | Adversary in the Middle

Global Administrators

High | Rising: 16 / 24 (66.67%) → 17 / 25 (68%) user(s) | Identity | Persistence | Account Manipulation | Privilege Escalation

MS Graph Powershell Service Principal Assignment Not Enforced

High | Detected: Nov 07, 2024 | Identity | Persistence | Account Manipulation | Privilege Escalation

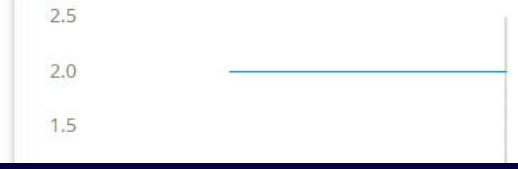
Administrative Accounts Susceptible to Kerberoasting

View

Identity | Initial Access | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Valid Accounts | Valid Accounts | Valid Accounts | Valid Accounts | Steal or Forge Kerberos Tickets | OS Credential Dumping

Severity: High
Previous: 2 / 1.2k (0.17%) user(s)
Current: 2 / 1.2k (0.17%) user(s)
Trend: 0 since last month

RISK HISTORY



netwrix

Netwrix Auditor

Identifica i rischi IT, rileva le attività sospette e indaga sugli incidenti di sicurezza

Riduci al minimo il rischio di violazioni dei dati

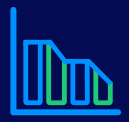
Raggiungi e dimostra la compliance

Aumenta la produttività dei tuoi team IT

netwrix

AUDITOR PRODUCT FEATURES

Change, Access, and Configuration Reporting



Risk Assessment

Alert in tempo reale sui modelli di minaccia

Verifiche dell'accesso degli utenti

Individuazione di comportamenti anomali

Rilevamento e classificazione dei dati sensibili (richiede NDC)

Report di compliance pronti all'uso

Ricerca simile a Google

netwrix

Netwrix Data Classification

Identifica e classifica i tuoi dati sensibili e business-critical e concentra le tue attività di sicurezza dei dati su tali dati

Identifica e blocca le informazioni sensibili

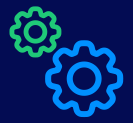
Sbarazzati dei dati non necessari per ridurre la superficie di attacco

Soddisfa i requisiti di privacy e conformità

netwrix

DATA CLASSIFICATION PRODUCT FEATURES

Classificazione dei dati ad alta fedeltà



Regole di classificazione predefinite

Motore di ricerca DSAR

Correzione automatizzata dei rischi

Etichettatura accurata dei dati

Rilevamento dati ROT

Ricerca accurata dei dati

Classificazione personalizzabile

netwrix

Netwrix Endpoint Protector

Blocca la perdita di dati sull'endpoint con la protezione continua su Windows, Linux e macOS e applica la crittografia per salvaguardare i dati in transito.

- Facilità d'uso grazie al supporto multi-OS
- Protezione continua in tempo reale, anche offline
- Controllo granulare dei dispositivi approvato dall'amministratore

netwrix

ENDPOINT PROTECTOR PRODUCT FEATURES

Point and Click Policy Creation

Cross-platform, lightweight agent

Extensible API Framework

Granular Print Controls

Granular Device Controls

Encryption of Sensitive Data Leaving Endpoint

Efficient Sensitive Data Scanning

MPIP Integration

netwrix

Netwrix 1Secure

Proteggiti dai rischi di identità e accesso ai dati

Accelera il rilevamento e la risposta agli incidenti

Valuta e mitiga i rischi con informazioni utili

Ottimizza il tuo investimento con la distribuzione SaaS istantanea

netwrix

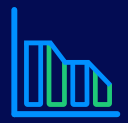
1SECURE PRODUCT FEATURES

Alerts on Critical Changes

Advanced Search and Filtering

Risk Assessment

Human-Readable Reports



Actionable Dashboards

Exportable Risk Reports

Secure Solution

Easy Ecosystem Integrations

netwrix

Netwrix PingCastle

Identificare e correggere i rischi nell'AD ibrido migliorando la postura di sicurezza

Identifica rapidamente i rischi
Ottieni una visione completa dei rischi in AD ed Entra ID. Sfrutta le mappature MITRE, ATT&CK™ e ANSSI con il punteggio di rischio per concentrare gli sforzi di sicurezza in modo efficace.

Colma le lacune di sicurezza
Riduci la superficie di attacco di Active Directory implementando strategie di correzione mirate. Segui i nostri consigli passo dopo passo, affrontando prima le vulnerabilità ad alto rischio per rafforzare il tuo livello di sicurezza dell'identità.

Monitora e migliora
Esegui Netwrix PingCastle su base pianificata su più domini per rilevare nuovi rischi e trust. Tieni traccia dei progressi e dei miglioramenti del punteggio di sicurezza per garantire una protezione AD continua.

netwrix

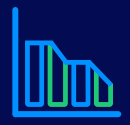
NETWRIX PINGCASTLE

AD Health Check Report

Risk Assessment

Risk Remediation Guidance

AD Security Maturity Level Evaluation



Historical Data and Trend Analysis

AD Map

netwrix

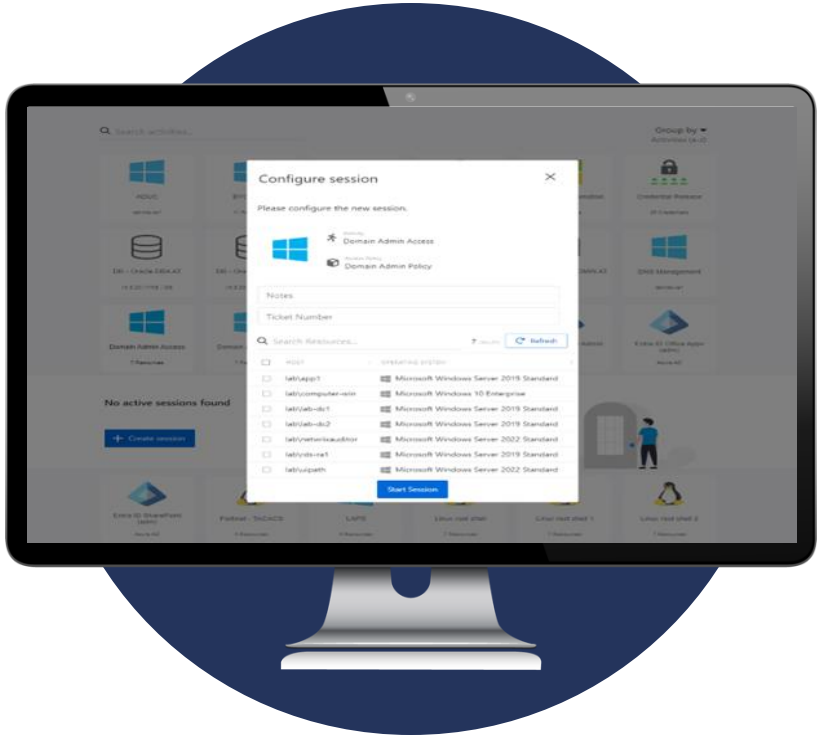
Netwrix Privilege Secure

Riduci i rischi con l'accesso privilegiato just-in-time

Riduci i rischi per la sicurezza eliminando gli account con privilegi permanenti. Con l'accesso just-in-time, gli utenti hanno solo l'accesso minimo necessario quando necessario.

Rafforza la protezione dei sistemi sensibili, dei dati e delle identità degli utenti con visibilità e controlli completi su tutte le attività privilegiate.

Semplifica la gestione della sicurezza dei privilegi attraverso l'amministrazione centralizzata e i flussi di lavoro integrati che migliorano sia la produttività che la supervisione.



netwrix

PRIVILEGE SECURE PRODUCT FEATURES

Remove Standing Privilege

Session Recording

Implement Zero-Standing-Privilege

Discover Blind Spots in Minutes

Protect Windows Endpoints

Role-based Access Management

Visibility of Attack Surface

Access Certification

netwrix

Netwrix ti aiuta a rispettare le norme

Government

FedRAMP
Federal Risk & Authorization Management Program

FISMA
Federal Information Security Management Act

CMMC
Cybersecurity Maturity Model Certification

CJIS
Criminal Justice Information Services

Critical Infrastructure

NERC CIP
North American Electric Reliability Corporation Critical Infrastructure Protection

NIS2
Directive on Security of Network and Information Systems

CESC2M2
Electricity Subsector Cybersecurity Capability Maturity Model

Finance

GLBA
Financial Services Gramm-Leach-Bliley Act

PCI DSS
Payment Card Industry Data Security Standard

SOX
Sarbanes–Oxley Act

FINRA
Financial Industry Regulatory Authority Guidelines

Education

FERPA
Family Educational Rights and Privacy Act

Privacy

GDPR
General Data Protection Regulation

CCPA
California Consumer Privacy Act

Healthcare

HIPAA
Health Insurance Portability and Accountability Act

HITRUST
Health Information Trust Alliance

Frameworks

CIS CSC
CIS Critical Security Controls

NIST CSF
NIST Cybersecurity Framework

Telco

ISO 27011
Information Security Management System

NIST Special Publications

NIST 800-53
Security and Privacy Controls for Information Systems and Organizations

NIST 800-171
Controlled Unclassified Information in Nonfederal Systems and Organizations

General

ISO 27001, 27002, 27015, and 27018
Information Security Management System

COBIT
Control Objectives for Information Technologies

SOC2
Service Organization Control

NCCoE
National Cybersecurity Center of Excellence

CISA
Cybersecurity Information Sharing Act

netwrix

NIS 2

	Auditor	Data Classification	Endpoint Protector	Privilege Secure	Privilege Secure for Endpoints	Change Tracker	Password Secure	PingCastle	Recovery for Active Directory	Directory Manager	Identity Manager	Threat Manager	Threat Prevention
a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici	✓	✓	✓			✓		✓		✓			
b) gestione degli incidenti	✓	✓	✓					✓				✓	✓
c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	✓	✓			✓	✓			✓	✓	✓		
d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;	✓			✓	✓		✓	✓		✓	✓		
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;						✓							
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;	✓		✓	✓	✓	✓	✓	✓		✓	✓		
g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;	✓		✓	✓	✓		✓						
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura			✓										
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli asset;				✓			✓			✓	✓		
j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.				✓	✓		✓				✓		

netwrix

Next Steps

Richiedi la tua Demo personalizzata

netwrix.com/demo

Scarica il white paper

"AD Security Self-Assessment"
netwrix.com/whitepaper

Download software

Active Directory Risk Assessment from Netwrix

netwrix

VICSAM
ICT - Cloud & Security Services

Real security for the real world

WatchGuardONE | GOLD PARTNER

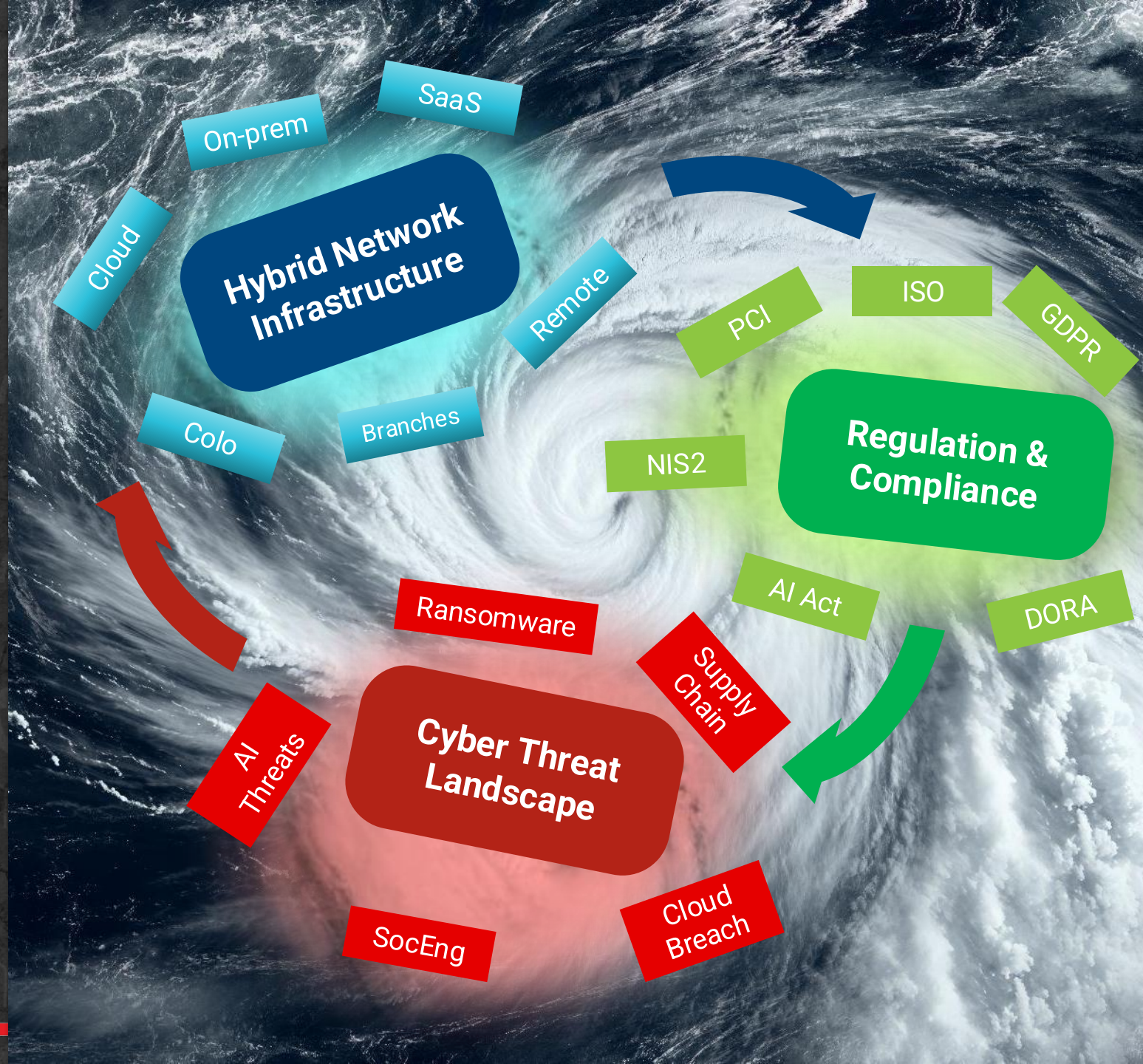
Intervento a cura di

Luca Manidi

Channel Account Manager, Italy

VICSAM GROUP DIGITAL WEEK

Tre fronti che si preparano a una complessa tempesta di sicurezza informatica



Real Security for the Real World

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Infrastruttura IT ibrida complessa e mutevole

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Infrastruttura IT ibrida complessa e mutevole

Il 96% delle aziende utilizza il cloud pubblico

L'84% delle aziende utilizzano il cloud privato

Un dipendente medio utilizza 24 applicazioni SaaS al giorno

Il 67% delle organizzazioni tecnologiche con meno di 100 dipendenti sono completamente remote

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Progressi nella regolamentazione e nella conformità:

- **Direttiva NIS2:** Rafforzare i requisiti di cybersecurity nella maggior parte delle organizzazioni.
- **DORA:** Digital Operational Resilience Act. Regolamento UE per rafforzare la resilienza delle organizzazioni finanziarie.
- **CRA:** Legge sulla resilienza informatica. Requisiti obbligatori di cybersicurezza per i fornitori di software e hardware nell'UE.
- **Legge UE sull'IA:** Un regolamento per promuovere un'IA affidabile e sicura.
- **CIRCIA:** Cyber Incident Reporting for Critical Infrastructure Act. Legge statunitense che impone al settore delle infrastrutture critiche di segnalare gli incidenti informatici.

Copyright © 2025 WatchGuard Technologies, Inc. Tutti i diritti riservati

Il panorama della sicurezza informatica in rapida evoluzione

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Ingegneria sociale pericolosamente intelligente: Trend

Assistenza AI
Miglioramento dello spear phishing
Miglioramento della pretestuosità

Cons lungo
Attacco alla supply chain attraverso XY Utils

Vishing e SMS
Deepfake

Dipendenti fake
KnowBe4 fake
Dipendente NK

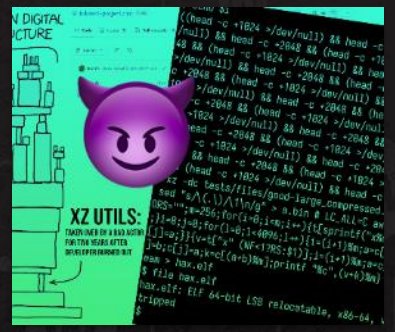
Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Attacchi alla supply chain software mirati alle fondamenta

L'81% delle organizzazioni globali ha subito un impatto negativo da una violazione informatica della supply chain

Un aumento del 12% dei segreti di sviluppo e dei dati sensibili esposti tramite repository open-source nel 2024

Il 45% delle organizzazioni globali sarà colpito da un attacco alla supply chain quest'anno - *Gartner*



XZ Utils Hack

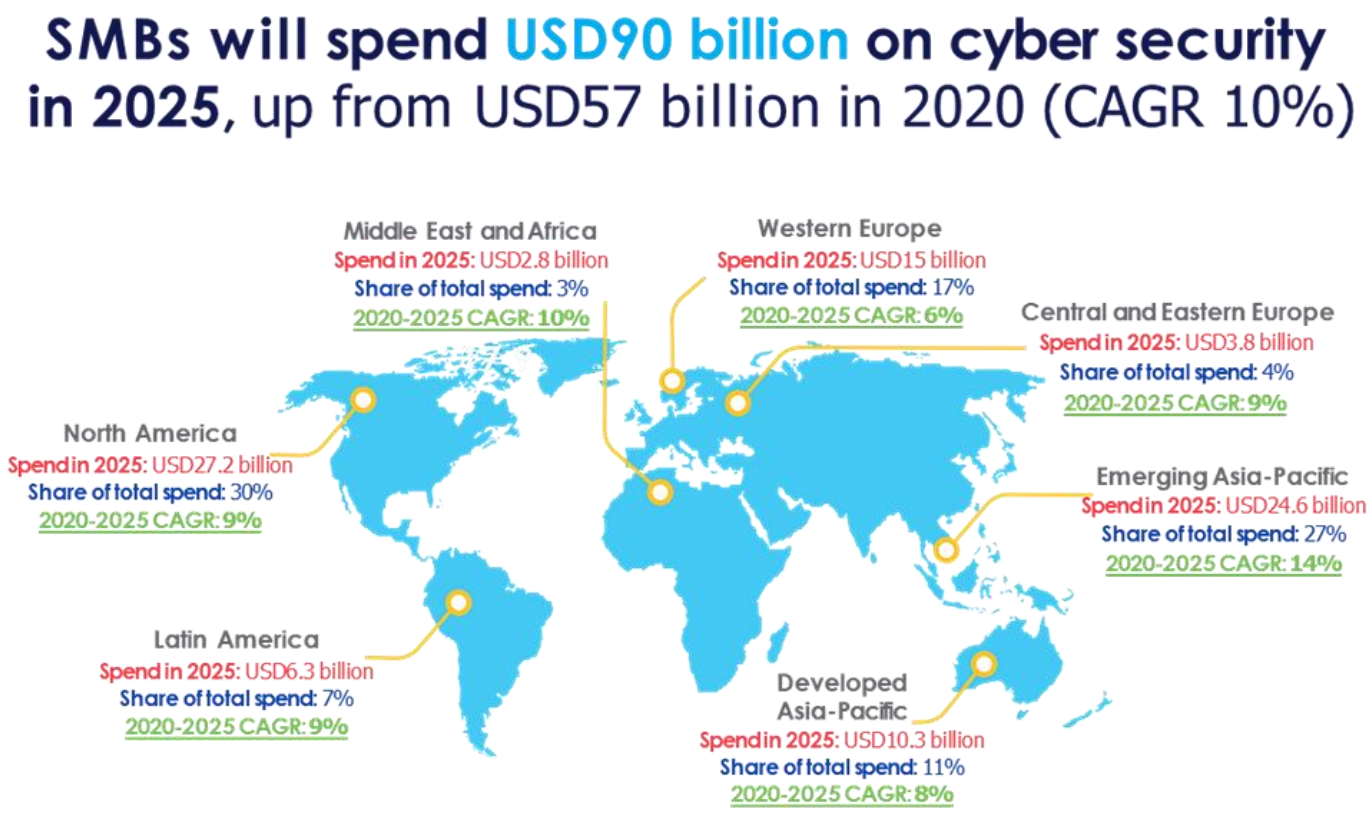
Violazione Cloud Oracle

Violazione Supporto Okta

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Le PMI si rendono conto di essere un obiettivo primario

- Il 63% delle PMI britanniche e il 53% di quelle francesi hanno subito un incidente informatico nel 2023.
- L'82% degli attacchi ransomware prende di mira aziende con meno di 1.000 dipendenti.
- Il costo medio di una violazione in Europa è stato di 3,1 milioni di euro, con tempi di recupero superiori ai 30 giorni.
  - In Francia il costo medio è di 230.000 euro.
  - In Italia il costo di una violazione è aumentato del 13,7%, raggiungendo i 4,3 milioni di euro.



Copyright © 2025 WatchGuard Technologies, Inc. Tutti i diritti riservati

I lavoratori da remoto sono vulnerabili

Il 67% delle violazioni di dati è legato a lavoratori remoti e ibridi

Il malware Infostealer è ora la seconda tecnica utilizzata dopo il phishing.

Il 65% delle credenziali rubate viene messo in vendita sul dark web il giorno stesso

Il 60% di tutti gli incidenti di cybersecurity coinvolge l'errore umano

L'ingegneria sociale è rimasta la prima causa di violazione per 15 anni di fila.

La formazione sulla sicurezza è solo una piccola parte: è possibile una maggiore protezione

Autenticazione forte (MFA)

Le ricerche dimostrano che il 99,9% dei casi di compromissione degli account avrebbe potuto essere evitato con l'MFA.

Rilevamento e risposta (MDR e XDR)

Il rilevamento e la risposta alle minacce spostano l'attenzione da "prevenire tutto" a "rilevare e contenere rapidamente".

Copyright © 2025 WatchGuard Technologies, Inc. Tutti i diritti riservati

WatchGuard

Quanti di noi oggi possono davvero dire di avere questi cinque elementi di base ben implementati e funzionanti?

Pacchetto di servizi di base

1. Firewall
2. MFA
3. EDR
4. Patch Management
5. Backup and Disaster Recovery Plan

Real Security
for the Real World

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved


WatchGuard
Meno Rumore. Più azione
Sicurezza Reale con MDR.

Stato della Cybersecurity

Il problema

- Superfici di attacco in crescita
- Le minacce sono sempre più complesse
- Competenze limitate
- Prodotti e Servizi costosi rendono la sicurezza inaccessibile a molti

Risultati e rischi

- Postura vulnerabile
- Scarse capacità di rilevamento e risposta lenta
- Copertura limitata fuori orario

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

PERCHÉ MDR?

Perché le minacce di oggi si muovono velocemente e la maggior parte dei team non riesce a tenere il passo.

- Le minacce 24 ore su 24, 7 giorni su 7 richiedono una difesa 24 ore su 24, 7 giorni su 7
- Gli attaccanti bypassano facilmente gli strumenti tradizionali.
- I team IT non hanno il tempo, gli strumenti o le competenze per rispondere.
- MDR colma le lacune con risposte esperte, non solo avvisi.
- Riduci il rischio senza aggiungere un onere interno.

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Core MDR

Endpoint

Servizio di cybersecurity completamente gestito, 24 ore su 24, 7 giorni su 7, che offre protezione di alto livello per endpoint e Microsoft 365 senza richiedere a partner o utenti finali di mantenere il proprio Security Operations Center (SOC)

Combina il rilevamento delle minacce basato su AI unitamente all'azione umana intepretata da personale esperto per rilevare, investigare e rispondere alle minacce informatiche in modo rapido ed efficiente

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Core MDR per Microsoft

WatchGuard Core MDR per Microsoft migliora Defender con il monitoraggio delle minacce basato su AI, il supporto SOC esperto e l'integrazione perfetta, fornendo una risposta più rapida, una migliore visibilità e una sicurezza più forte per partner e clienti.

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Total MDR

AuthPoint MFA | Endpoint | NetSec

WatchGuard Total MDR è un servizio di rilevamento e risposta alle minacce completamente gestito, 24 ore su 24, 7 giorni su 7, che unifica **lo stack di sicurezza WatchGuard** – endpoint, firewall, identità e rete – oltre a selezionati ambienti cloud di terze parti come Microsoft 365, Azure, AWS CloudTrail e Google Workspace.

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

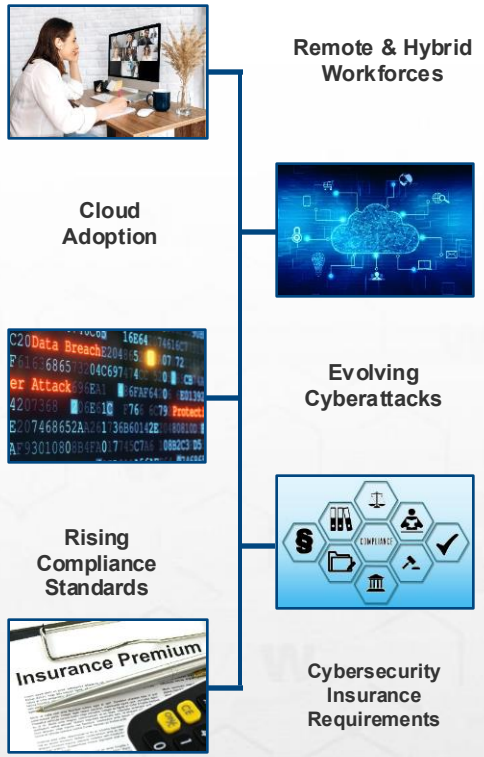
FireCloud Total Access

Lavoro remoto sicuro, semplificato
Il futuro dello Zero Trust erogato dal cloud per PMI

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

The Problem: Remote Work & Cloud Apps Have Broken Security

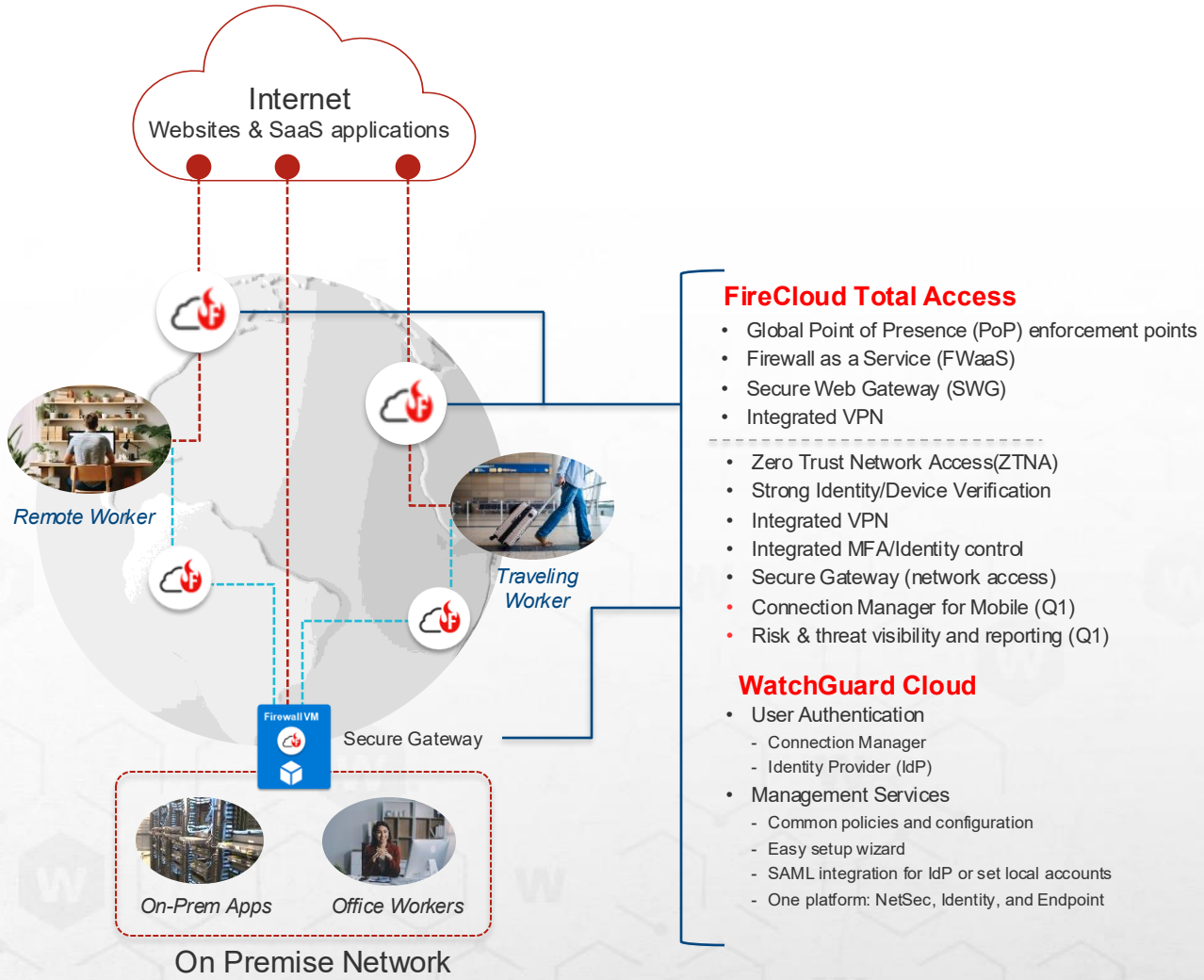
- La sicurezza perimetrale è obsoleta.
- Il cloud e il SaaS hanno sfumato i confini.
- Le VPN sono lente, troppo permissive e creano autostrade per gli attacchi.
- La Shadow IT e la proliferazione di soluzioni SaaS aumentano il rischio e la perdita di dati.
- I team IT affrontano complessità, pressioni normative e costi in aumento.



Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

FireCloud Total Access

- **Protezione Sempre Attiva** – Sicurezza continua per utenti e dispositivi su Internet, SaaS e applicazioni private.
- **Difesa Completa dalle Minacce** – Ispezione SSL, gestione dei certificati e scansione del traffico bidirezionale per fermare attacchi avanzati.
- **Controllo degli Accessi Zero Trust** – Politiche basate sull'identità, applicazione per singola app e gestione delle risorse secondo il principio del minimo privilegio.
- **Prestazioni Ottimizzate** – Eliminazione dei colli di bottiglia delle VPN, riduzione del carico sui firewall e miglioramento della velocità grazie ai servizi erogati dal cloud.
- **Distribuzione Flessibile** – Agente leggero, infrastruttura PoP globale e gateway virtuali che si adattano ad ambienti ibridi e cloud.
- **Gestione della Sicurezza Semplificata** – Politiche centralizzate, monitoraggio e reportistica tramite WatchGuard Cloud.



Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

FireCloud Components

FireCloud Connection Manager: Un agente leggero che:

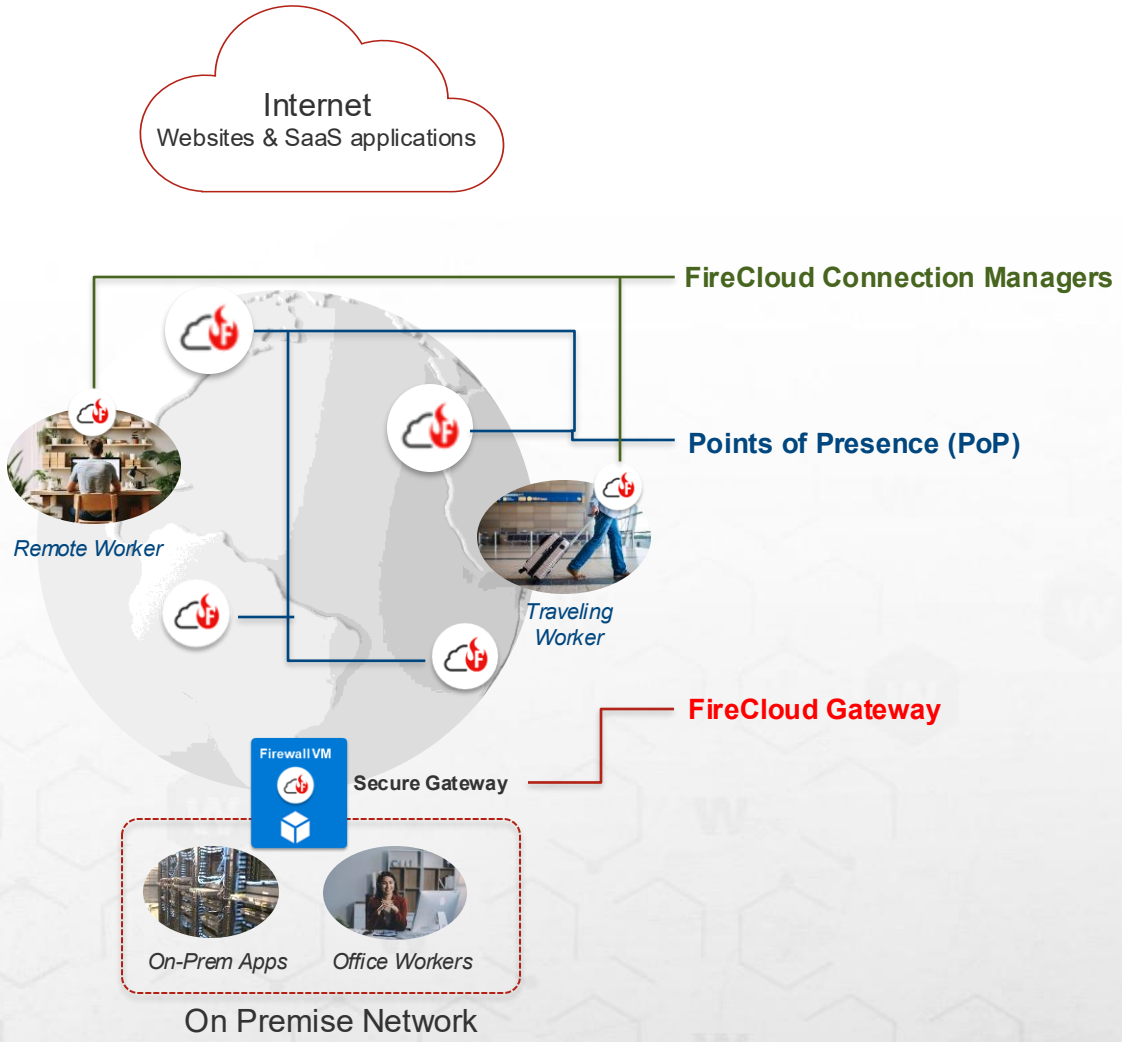
- Gestisce l'autenticazione
- Instrada il traffico verso i PoP
- Condivide le policy e protegge le comunicazioniInfrastruttura FireCloud

Point of Presence (PoP): Una rete globale in espansione di punti di controllo cloud-based che:

- Criptano, ottimizzano, instradano e terminano il traffico
- Funzionano come punti di applicazione delle policy e dello Zero Trust
- Ottimizzano le prestazioni e garantiscono scalabilità e ridondanza

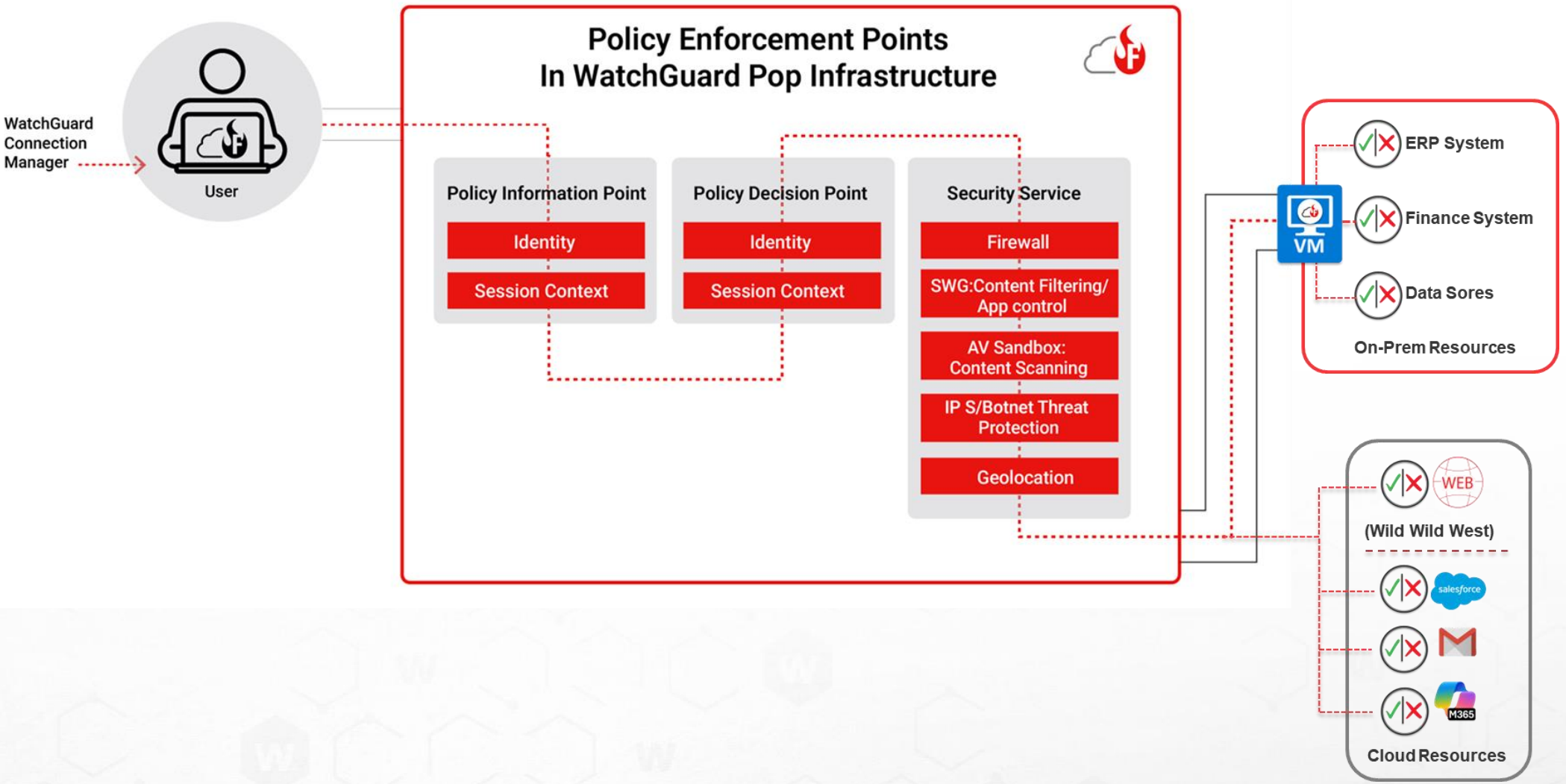
FireCloud Gateways: Un'appliance virtuale distribuita al perimetro che:

- Fornisce connessioni sicure e criptate tra i PoP FireCloud e le applicazioni private
- Abilita l'accesso Zero Trust Network Access (ZTNA) alle applicazioni on-premise senza necessità di porte aperte
- Applica policy basate sull'identità per l'accesso autenticato degli utenti
- Supporta ambienti virtuali/server Windows



Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Protects Users Accessing On-premise Resources



Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Risks and Threats Visibility and Control

- **FireCloud Reporting**

Sicurezza

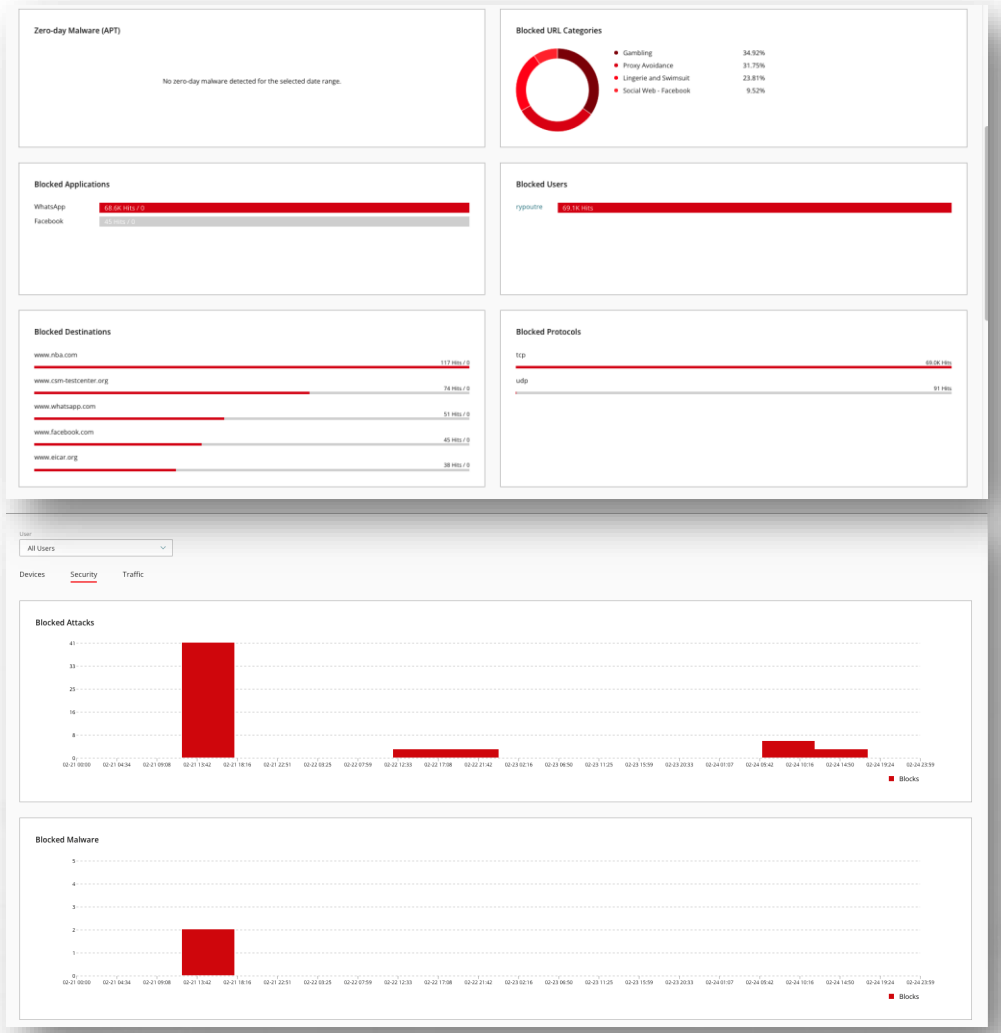
- Minacce bloccate, inclusi malware
- Applicazioni, URL/siti web bloccati
- Blocco del traffico per paese tramite filtro geolocalizzato

Traffico

- Applicazioni usate più frequentemente
- Siti web visitati più frequentemente
- Attività utente più attiva e traffico per area geografica
- Connessioni approvate e bloccate per area geografica

Utenti

- Informazioni su utenti e dispositivi autenticati
- Policy di sicurezza applicate per utente e gruppo
- Informazioni sul client, incluse le versioni del sistema operativo
- Filtraggio per utenti, eventi, versioni client e utenti inattivi



Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

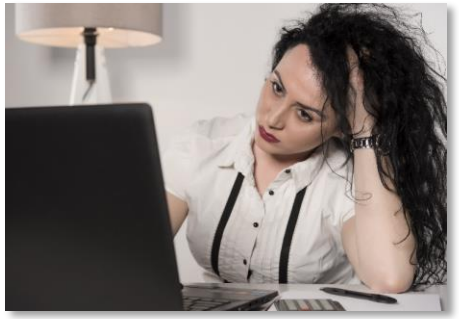
FireCloud Critical Use Case Coverage

Secure Remote & Hybrid Work

- La sicurezza continua consente ai dipendenti di lavorare in modo sicuro da qualsiasi luogo, proteggendoli dalle minacce web anche su reti non gestite.
- Aumenta la produttività, protegge dalle minacce online, riduce le violazioni dei dati, garantisce la conformità, tutela la reputazione del marchio e riduce il carico di lavoro per l'IT.

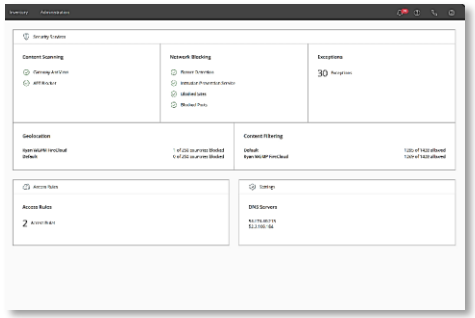
Secure Access to Cloud & Private Resources

- Applica policy basate sull'identità e ispezione del traffico, consentendo agli utenti di connettersi in modo sicuro solo alle applicazioni SaaS e cloud pubbliche autorizzate.
- Accesso fluido e basato sull'identità alle applicazioni interne (es. finanza, HR, CRM) senza esporle a Internet.



Modernizing Legacy VPN Infrastructure

- Sostituisci le VPN con un accesso sicuro, Zero Trust a livello di applicazione, per eliminare le porte esposte, ridurre la superficie di attacco e bloccare i movimenti laterali.
  Elimina tunnel, regole firewall e il carico delle VPN legacy per ridurre i costi di supporto, semplificare la gestione e migliorare l'esperienza utente.



Centralized Policy Enforcement Across Devices and Locations

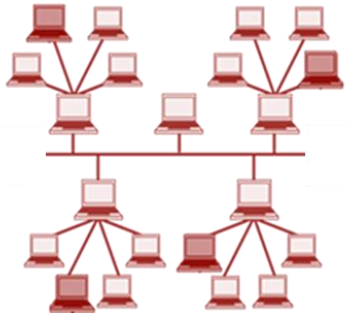
- Gestisci centralmente e applica policy di sicurezza e accesso coerenti, indipendentemente dalla posizione dell'utente o dal dispositivo utilizzato.
- Semplifica le operazioni, garantisce la conformità ed elimina le falle di sicurezza causate da configurazioni decentralizzate e da soluzioni multi-prodotto.

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

WatchGuard ThreatSync+ NDR

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Il Network e’ vulnerabile



La rete resta vulnerabile

- Dispositivi sconosciuti e vulnerabilità sono nascosti all'interno della tua rete
- Informazioni sensibili sono distribuite in più sedi
- Le risorse IoT sono sconosciute e non protette

La visibilità della rete è più importante che mai per ridurre i rischi.

Ransomware/Cyberattacks

- Le difese perimetrali vengono aggirate
- Gli attacchi ransomware sono in aumento
- Un numero record di vulnerabilità viene sfruttato

Il rilevamento e la risposta alle minacce in modo rapido e preciso sono fondamentali per proteggere la tua organizzazione.

Risorse/staff limitati

- Più strumenti, più superfici di attacco, maggiore complessità
- Carenza di personale, limitazioni operative, attività difficili da gestire
- Difficoltà nel reperire o mantenere talenti

Devi fare di piu’ con meno. La tecnologia deve supportare I processi.

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Perche’ NDR e’ critico per la tua strategia difensiva

I cattivi hanno molta scelta

Network Detection and Response

Analisi continua 24/7 dei flussi di rete

- All’interno della rete – traffico est/ovest
- Attraverso le DMZ verso l’esterno – traffico nord/sud

Fornisce visibilità su tutti i dispositivi presenti nella rete

- Può identificare, classificare e etichettare tutti i dispositivi, inclusi quelli IoT
- Può generare allarmi per dispositivi rogue e Shadow IT

Allerta quando vengono rilevate fasi di attacco

- La difesa perimetrale è stata superata
- Gli attacchi sono attivi all’interno della rete

NDR è fondamentale per la tua strategia difensiva

- Gli attacchi hanno bisogno della tua rete per avere successo: ricognizione, C2, movimenti laterali ed esfiltrazione
- Gli attacchi sono rumorosi. Il traffico di flusso di rete è ideale per l’AI. Le attività anomale vengono identificate rapidamente e con precisione
- Gli aggressori non possono nascondersi dall’NDR, né bypassarlo. La tua rete è la tua migliore fonte di verità

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

Introduzione a WatchGuard ThreatSync+ NDR

Cloud Nativo

Elimina il tempo e i costi, il carico dell'hardware
Basso TCO complessivo per una sicurezza di rete di classe mondiale.

Motore AI Avanzata

Trova rapidamente minacce nascoste nella tua rete che sono state mancate da altre difese – ransomware, vulnerabilità e attacchi alla catena di approvvigionamento..

Completa visibilita' dei rischi

Copertura massima su tutta la tua rete – nord/sud, est/ovest e dispositivi.

Threat Detection & Remediation automatizzate

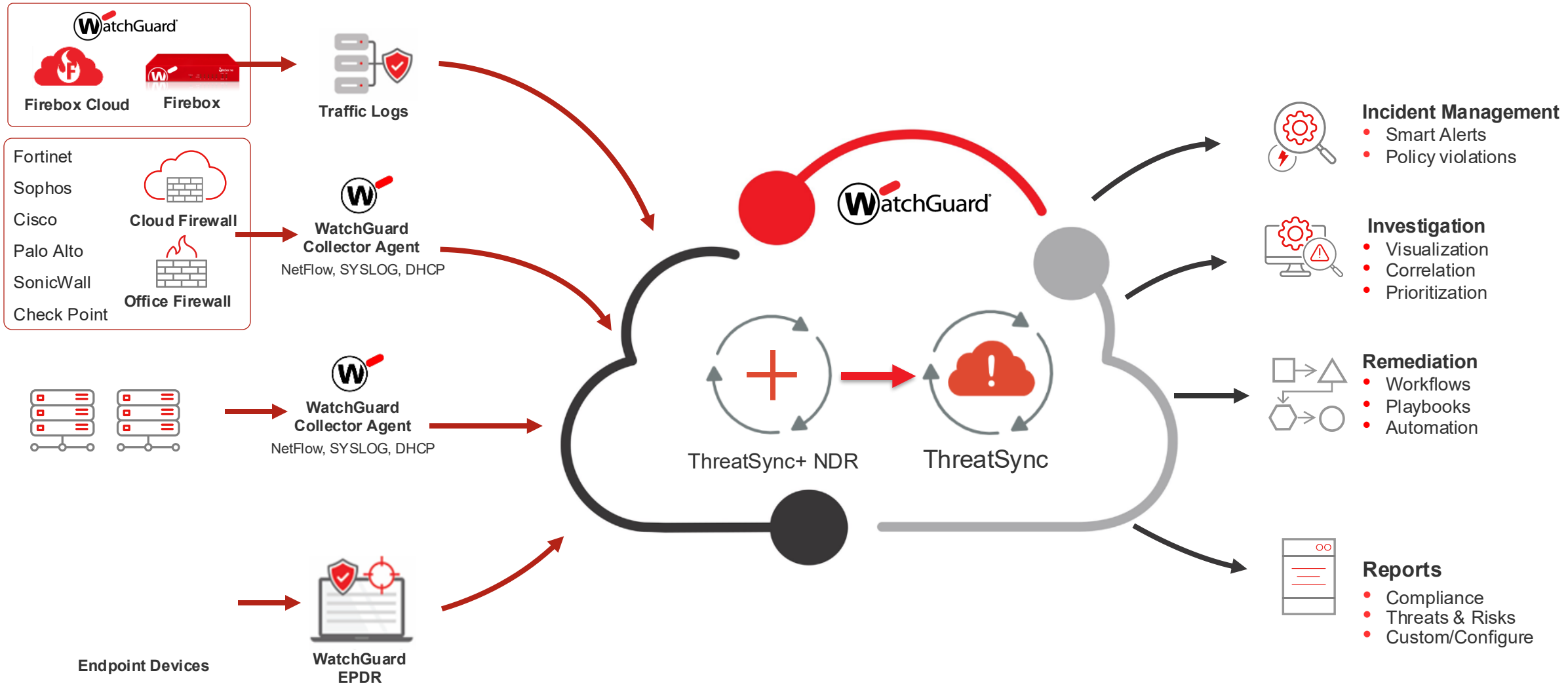
Migliora i tempi di risposta risparmiando tempo e denaro senza aumentare il personale.

Continuo monitoring delle compliance

Semplifica la reportistica sulle conformita' e visibilita'

Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

WatchGuard's NDR Architecture Optimizes Your Investment



Copyright © 2025 WatchGuard Technologies, Inc. All Rights Reserved

VICSAM
ICT - Cloud & Security Services

La parola all'esperto

Panel di approfondimento a cura di Davide Guzzi con:

Massimiliano Grassi

Marketing Director EMEA ReeVo

Michele Gadda

Engineering Manager di Yamaha Motor Racing

REEVO

YAMAHA FACTORY RACING

2025 OFFICIAL SPONSOR

VICSAM GROUP DIGITAL WEEK

VICSAM GROUP DIGITAL WEEK

Cassago
20-24
Ottobre
2025

Il valore di una sinergia vincente

La partnership tra **ReeVo** e **Yamaha Motor Racing** nasce dall'incontro tra due realtà che condividono visione, innovazione e attenzione alla performance.

Com'è nata la collaborazione tra ReeVo e Yamaha Motor Racing?

Quali valori comuni vi hanno spinto a stringere questa partnership?

VICSAM GROUP

VICSAM GROUP DIGITAL WEEK

Cassago
20-24
Ottobre
2025

Moto GP: dove nasce l'innovazione che cambia le moto di domani

La **MotoGP** è un laboratorio estremo di innovazione, dove tecnologia, strategia e organizzazione si fondono per spingere al limite le pre stazioni.

In un contesto così estremo come la MotoGP, quanto margine esiste ancora per innovare sui motori, considerando i regolamenti tecnici sempre più stringenti? Dove si gioca oggi la vera sfida: potenza, affidabilità, elettronica, altro?

Quanto incide invece l'evoluzione organizzativa di un Team per eccellere nella MotoGP? (es. sappiamo che avete portato parte della progettazione in Italia)

Come si bilancia la ricerca della massima prestazione e di evolvere costantemente con la necessità di convivere, durante un'intera stagione, con un numero limitato di propulsori utilizzabili?

Quanto delle innovazioni sviluppate nei motori MotoGP riesce davvero a "scendere" nelle moto stradali? Ci puoi fare un esempio concreto di una tecnologia passata dalla pista alla produzione di serie?

VICSAM GROUP


Grazie