MEET IT

Datasheet

EPDR

ENDPOINT PROTECTION DETECTION & RESPONSE

Le aziende del Gruppo MEET IT

3CiME TECHNOLOGY ICT & INNOVATION

Via di Corticella, 89/2
40128 Bologna BO

+39 05 14070383
www.3cime.com | info@3cime.com

ntnuovetecnologie 25

Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it

SICUREZZA AVANZATA E COMPLETA PER GLI ENDPOINT

Sempre un passo avanti alle violazioni.

EPDR è una soluzione di sicurezza avanzata, **potenziata dall'AI**, che riunisce **EPP EndPoint Protection** ed **EDR EndPoint Detection & Response** in un unico prodotto per la sicurezza completa degli endpoint, ovvero laptop, computer e server.

Protegge i dispositivi da minacce avanzate quali: ransomware, malware, APT, phishing, spyware, rootkit e tanto altro, riducendo la superficie di attacco e fornendo completa visibilità sui tuoi dispositivi aziendali, compresi gli smartphone.

La soluzione è gestita in modalità as a service dal team tecnico certificato di MEET IT su piattaforma in cloud.

Include le funzionalità **Zero Trust** e **Threat Hunting**, fornite come servizi gestiti all'interno della piattaforma.

PRINCIPALI FUNZIONALITÀ

- Monitoraggio e analisi continua degli endpoint
- Protezione perimetrale
- Rilevamento e classificazione di tutte le attività
- Blocco dei comportamenti anomali di utenti, macchine e processi
- Prevenzione di processi sconosciuti e valutazione vulnerabilità

Per una sicurezza ancora più avanzata è possibile scegliere il servizio in modalità **Advanced** che aggiunge telemetria estesa (IoC, IOC STIX/Yara), policy avanzate e shell remota per investigazioni approfondite.

BENEFICI

- **Copertura** estesa contro tanti tipi di minacce
- Metodo **Zero-Trust**
- **Automazione** avanzata
- **Integrazione completa (sinergia tra rete, endpoint, wifi e identità)**
- **Dashboard centralizzata**
- **Protezione preventiva** e **risposta attiva** agli attacchi
- **Gestione completa** del servizio, dalla configurazione al mentenimento
- Massimi livelli di **sicurezza** e **controllo enterprise**

VISITA IL SITO *MEETIT.CLOUD*

Patch Management

Identifica, fornisce priorità e implementa patch fondamentali per il sistema operativo e per le applicazioni di terze parti, in modo da impedire gli attacchi informatici e **ridurre le vulnerabilità note**.

Full Encryption

La crittografia completa è la **prima linea di difesa** per proteggere i dati in modo efficace. Il servizio utilizza BitLocker per crittografare e decrittografare i dischi e fornisce alle organizzazioni un'autenticazione pre-boot.

Advanced Reporting Tool

Gli specialist IT sono sommersi da una quantità enorme di dati e notifiche da gestire, spesso poco utili, e faticano a dare priorità alle informazioni davvero importanti. L'Advanced Reporting Tool fornisce **security intelligence in tempo reale** grazie a informazioni approfondite su applicazioni, rete, operazioni e azioni giornaliere degli utenti.

Data Control

Si tratta dello strumento che **semplifica la gestione della protezione dei dati sensibili e personali**. Supporta le aziende nel rilevare, classificare, verificare e monitorare i dati personali non strutturati sugli endpoint, aiutando gli utenti a gestire meglio i dati in termini di consenso, avvisi e obblighi normativi e di conformità.

FUNZIONALITÀ COMPLETE

PROTEZIONE

- Protezione malware noto e zero day
- Protezione ransomware noto e zero day
- Protezione da exploit noti e zero day
- Protezione anti-phishing
- Protezione da vari vettori di attacco (web, email, rete, dispositivi)
- Protezione tradizionale con firme generiche e ottimizzate
- Protezione da minacce persistenti avanzate (APTs)
- Servizio Zero Trust per le applicazioni
- Servizio di ricerca delle minacce: Attacco con indicatori deterministici mappati su MITRE ATT&CK
- Servizio di ricerca delle minacce: Attacco con indicatori non deterministici mappati su MITRE ATT&CK con telemetria contestuale
- Query all'Intelligenza collettiva basata su cloud
- Blocco comportamentale
- Firewall personale e gestito
- §IDS/HIPS
- Protezione dagli attacchi di rete
- Controllo dispositivi
- Filtro degli URL per categoria (monitoraggio della navigazione web)

MONITORAGGIO

- Monitoraggio dei rischi per gli endpoint
- Monitoraggio continuo basato su cloud di tutte le attività dei processi
- Conservazione dei dati per un anno per indagini retrospettive sugli attacchi
- Valutazione delle vulnerabilità

RILEVAMENTO

- Rilevamento di applicazioni attendibili compromesse
- Zero-Trust Application Service
- Alert istantanei sui rischi per la sicurezza completamente configurabili
- Ricerca di regole STIX IOC e YARA
- eXtended Detection and Response (XDR)

CONTENIMENTO

- Isolamento di computer in tempo reale dalla console cloud

RISPOSTA E CORREZIONE

- Possibilità di eseguire il rollback e correggere le azioni degli aggressori
- Quarantena centralizzata
- Analisi e disinfezione automatiche
- Copie shadow
- Capacità di bloccare le applicazioni sconosciute e indesiderate
- eXtended Detection and Response (XDR)

ENDPOINT SECURITY AND MANAGEMENT

Indagine

- Protezione malware noto e zero day
- Protezione ransomware noto e zero day
- Protezione da exploit noti e zero day
- Protezione anti-phishing
- Protezione da vari vettori di attacco (web, email, rete, dispositivi)
- Protezione tradizionale con firme generiche e ottimizzate
- Protezione da minacce persistenti avanzate (APTs)
- Servizio Zero Trust per le applicazioni
- Servizio di ricerca delle minacce: Attacco con indicatori deterministici mappati su MITRE ATT&CK
- Servizio di ricerca delle minacce: Attacco con indicatori non deterministici mappati su MITRE ATT&CK con telemetria contestuale
- Query all'Intelligenza collettiva basata su cloud
- Blocco comportamentale
- Firewall personale e gestito
- §IDS/HIPS
- Protezione dagli attacchi di rete
- Controllo dispositivi
- Filtro degli URL per categoria (monitoraggio della navigazione web)

Riduzione della superficie di attacco

- Modalità di blocco nella protezione avanzata
- Tecnologia anti-exploit
- Blocco del programma tramite hash o nome (ad es. PowerShell)
- Controllo dei dispositivi
- Protezione Web
- Aggiornamenti automatici
- Rilevamento automatico degli endpoint non protetti
- Gestione delle patch per sistemi operativi e applicazioni di terze parti (componente aggiuntivo)
- Sicurezza per connessioni VPN (richiede Firebox)
- Accesso sicuro alla rete Wi-Fi tramite access point
- Policy di sicurezza avanzate

Gestione della sicurezza degli endpoint

- Console basata su cloud centralizzata
- Ereditarietà delle impostazioni tra gruppi ed endpoint
- Possibilità di eseguire configurazioni e applicare impostazioni sulla base di un gruppo
- Possibilità di eseguire configurazioni e applicare impostazioni sui singoli endpoint
- Implementazione in tempo reale delle impostazioni dalla console agli endpoint
- Gestione della sicurezza basata su viste degli endpoint e filtri dinamici
- Possibilità di programmare task ed eseguirli dalle viste degli endpoint
- Possibilità di assegnare ruoli preconfigurati agli utenti della console
- Possibilità di personalizzare gli alert locali
- Verifica delle attività degli utenti
- Installazione mediante pacchetti MSI, URL per il download e invio di e-mail agli utenti finali
- Report su richiesta e programmati a diversi livelli, con varie opzioni di granularità
- Indicatori delle prestazioni (KPI) per la sicurezza e dashboard di gestione
- Disponibilità API