



**PREVENZIONE DAGLI ATTACCHI  
RANSOMWARE SU STORAGE E BACKUP**

# SENTINEL

*Datasheet*

Le aziende del Gruppo MEET IT



Via di Corticella, 89/2  
40128 Bologna BO

+39 051 4070383  
[www.3cime.com](http://www.3cime.com) | [info@3cime.com](mailto:info@3cime.com)



Viale Alcide De Gasperi, 37  
33100 Udine UD

+39 0432 524001  
[info@ntonline.it](mailto:info@ntonline.it) | [www.ntonline.it](http://www.ntonline.it)



## HARDENING DEL SISTEMA

### Gestione Avanzata della Security Posture per Sistemi di Storage e Protezione Dati

IL SERVIZIO

**Sentinel** è un sistema esperto per l'hardening dei sistemi di Storage e Protezione dei Dati.

Verifica che la configurazione dei sistemi di storage e protezione dati sia allineata alle best practice dei Vendor e conforme agli standard di settore e ai requisiti normativi. Lavora in modo continuo, passivo e senza agenti, e non accede in alcun modo ai dati contenuti nei sistemi.

FOCUS

La criminalità informatica ha capito che colpire i sistemi di protezione dati (backup, replica, snapshot, archiviazione a lungo termine, DR) è il fattore decisivo per estorcere un **Ransom** (riscatto)

PUNTI CHIAVE

- **MASSIMA RESISTENZA AGLI ATTACCHI**  
Assicura che i sistemi di storage e protezione dei dati siano sempre pronti a resistere agli attacchi.
- **VALIDAZIONE CONTINUA DELLA SICUREZZA**  
Elimina le attività manuali di verifica, validando continuativamente la conformità alle baseline richieste.
- **PREVENZIONE DEL DISALLINEAMENTO**  
Previene il disallineamento delle configurazioni, monitorando tutte le modifiche ai parametri di sicurezza.
- **RISOLUZIONE RAPIDA DEI RISCHI**  
Fornisce indicazioni precise per ridurre i tempi di risoluzione dei problemi rilevati.
- **PROVE DI CONFORMITÀ PER AUDIT**  
Fornisce prove concrete di conformità in sede di audit IT.
- **OPERATIVITÀ INVISIBILE E SICURA**  
Lavora in modo passivo, senza agenti e senza accedere in alcun modo ai dati contenuti nei sistemi.

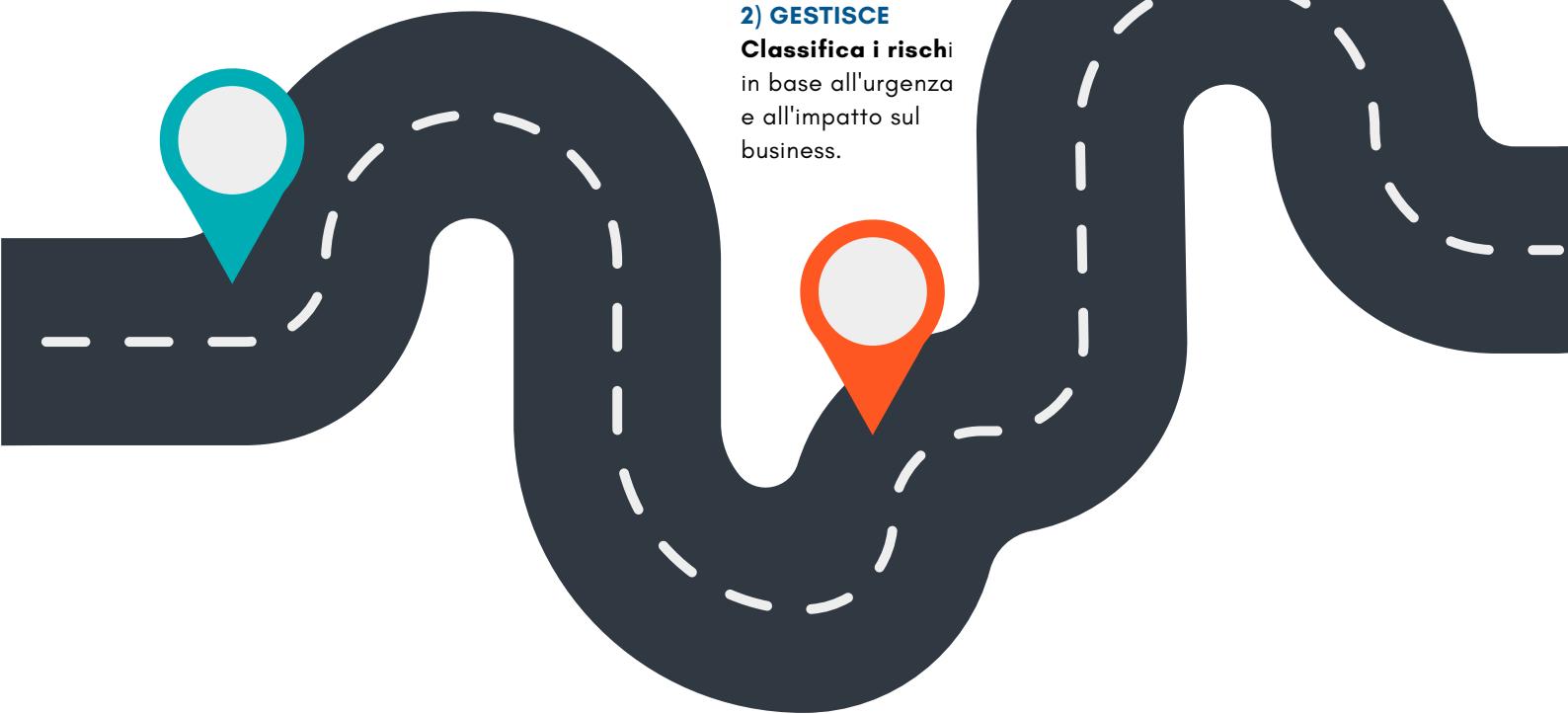
VISITA IL SITO [MEETIT.CLOUD](http://MEETIT.CLOUD) 

Sentinel verifica che la configurazione dei sistemi di storage e protezione dati siano allineati alle best practice dei Vendor e conformi agli standard di settore e ai requisiti normativi garantendo la visibilità completa sui rischi per la sicurezza di questi sistemi.

### 1) ANALIZZA

Analizza in modo continuo sistemi di storage e protezione dei dati, rilevando automaticamente configurazioni errate e vulnerabilità. Si tratta di un sistema esperto che utilizza una base di conoscenza che comprende:

- **Best practice di sicurezza** dei principali Vendor di storage e backup
- **Standard** (NIST, ISO, CIS, DORA, SNIA, PCI ecc.) applicati ai sistemi di storage e backup
- **Vulnerabilità** (CVE) nell'ambiente di archiviazione e protezione dei dati
- **Baseline di sicurezza** comunemente adottate



Sentinel è un sistema **esperto**, una **libreria vasta** e **continuamente aggiornata di controlli automatizzati per best practice**, linee guida dei fornitori, standard e linee guida di settore, allerte, baseline di sicurezza comuni e vulnerabilità.

**SENZA AGENTI**

Non necessita dell'installazione di agenti.

**SCANSIONE AUTENTICATA**

Effettua una scansione autenticata con account in sola lettura.

**TECNOLOGIA**

Sfrutta diverse chiamate specifiche per i dispositivi, utilizzando comandi di sistema e API dedicate.

**RISERVATEZZA DATI**

Non accede in alcun modo ai dati immagazzinati.

**CONTROLLI DI SICUREZZA VALIDATI**

Liste di Controllo accessi (System)	<input checked="" type="checkbox"/>	Copie di Backup immutabili	<input checked="" type="checkbox"/>
Comunicazione di Sistema Autenticata (Zero Trust)	<input checked="" type="checkbox"/>	Crittografia delle comunicazioni interne	<input checked="" type="checkbox"/>
Liste di controllo accessi (Shares)	<input checked="" type="checkbox"/>	Registrazione eventi o Log	<input checked="" type="checkbox"/>
Blocco degli account	<input checked="" type="checkbox"/>	Regole per le Password	<input checked="" type="checkbox"/>
Principi di Isolamento dei Backup	<input checked="" type="checkbox"/>	Best practice di sicurezza per reti SAN	<input checked="" type="checkbox"/>
Multi-Factor Authentication	<input checked="" type="checkbox"/>	Certificati SSL	<input checked="" type="checkbox"/>
Passwords di Default	<input checked="" type="checkbox"/>	Crittografia avanzata	<input checked="" type="checkbox"/>
Crittografia dei dati a riposo	<input checked="" type="checkbox"/>	Restrizioni di sessione	<input checked="" type="checkbox"/>
Linee Guida #StopRansomware della CISA	<input checked="" type="checkbox"/>	Utenti e Controllo degli Accessi Basato sui Ruoli (RBAC)	<input checked="" type="checkbox"/>
Software / Firmware / OS Non più supportato	<input checked="" type="checkbox"/>	Servizi e protocolli non utilizzati disabilitati (Funzionalità minima)	<input checked="" type="checkbox"/>
Avvisi di Sicurezza High-Severity	<input checked="" type="checkbox"/>	E MOLTO ALTRO	
Sistema di gestione rafforzato (CLI, Web)	<input checked="" type="checkbox"/>		

VISITA IL SITO

MEETIT.CLOUD

