ENDPOINT SECURITY

STORMSHIELD **EVOLUTION**

Aumentate il livello di protezione delle vostre postazioni di lavoro grazie a una soluzione EDR proattiva

Implementazione
IN LOCO
E SAAS

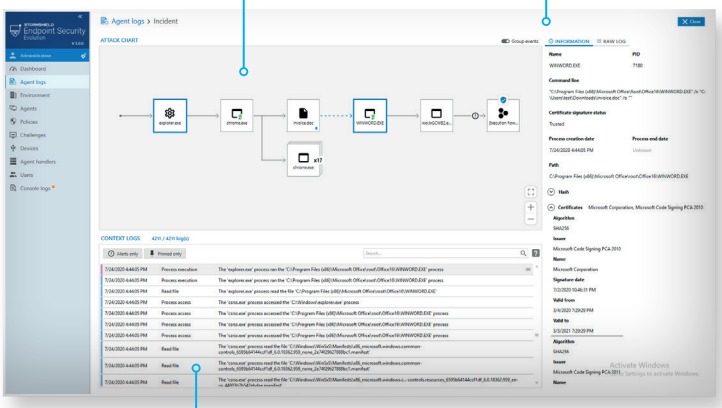
API REST
ECOSISTEMA
DI INTEGRAZIONE

Altamente personalizzabile
PARAMETRI DI SICUREZZA
REGOLABILI

Autonoma
PROTEZIONE DI AMBIENTI
NON CONNESSI

VISTA DETTAGLIATA

GRAFICO DI ATTACCO



ELENCO DEGLI EVENTI

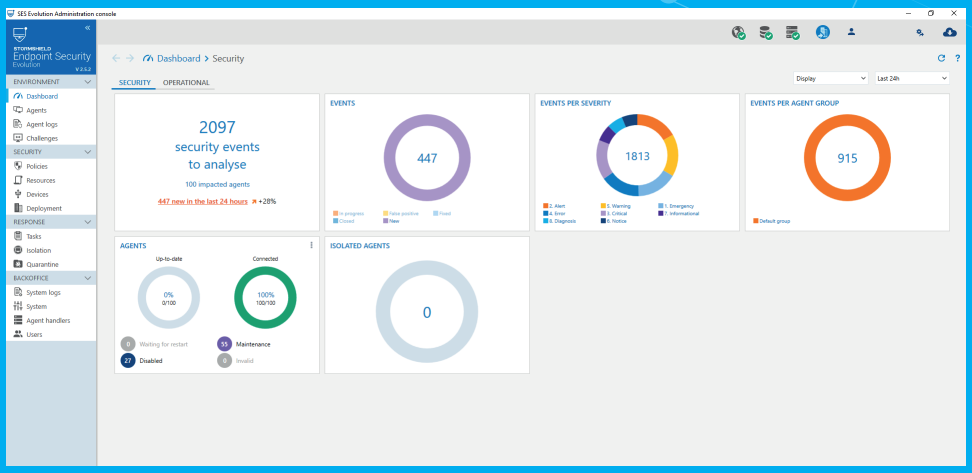
Protezione ottimale con la nostra soluzione EDR

Stormshield Endpoint Security Evolution è la soluzione di protezione per endpoint e server di nuova generazione. Basato su una tecnologia di analisi senza firme, l'agente rileva attacchi e minacce, rispondendo di conseguenza.

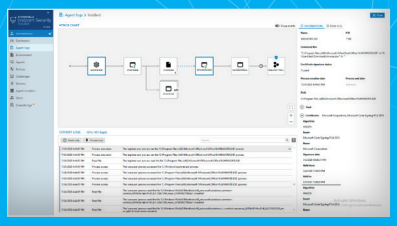
Sicurezza proattiva
- Attacco bloccato in tempo reale
- Analisi e correzioni predefinite e personalizzabili
- Grafico degli attacchi e Threat Hunting (IoC, regole Yara, ecc.)

Analisi comportamentale
- Protezione senza firme contro gli attacchi Zero-Day
- Combatte le tecniche di sfruttamento delle vulnerabilità
- Protezione anti ransomware

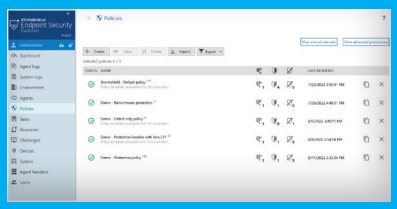
Protezione contestuale
- I criteri di sicurezza si adattano dinamicamente all'ambiente anche quando sono offline
- Criteri personalizzabili per gruppo di utenti
- Politiche di sicurezza predefinite e aggiornamenti da parte dei team Stormshield Customer Security Lab



Dashboard



Vista dettagliata di un incidente



Politica di sicurezza

FUNZIONALITÀ

Protezione Zero-Day contro minacce conosciute e sconosciute

Tecniche di analisi

- Corruzione della memoria (buffer overflow, heap spray)
- Escalation dei privilegi (token stealing)
- Furto di informazioni sensibili (keylogging, process access)
- Process hollowing e sue varianti
- Iniezione di codice (application hooking)
- Protezione contro gli attacchi fileless

Protezione contro il ransomware

- Processo di crittografia malevolo
- Ripristino i file criptati dal ransomware
- Windows Shadow Copy
- Politica di backup

Protezione senza firme

Rimedi personalizzati

- Kill di un processo
- Eliminazione di un file
- Eliminazione o modifica della chiave di registro o il suo valore
- Esecuzione script PowerShell per azioni personalizzate (arresto e rimozione di un servizio, ecc.)
- Quarantena automatica del malware
- Isolamento delle postazioni di lavoro compromesse

Identificazione degli indicatori di compromissione (IoC)

- Testo sospetto (nome del file, dell'host, dell'oggetto, ecc.)
- Informazioni di rete (indirizzi IP, URL sospetti, DNS)
- Hash SHA1, SHA256, MD5 e SSDEEP
- Ricerca immediata, programmata o su rilevazione di indicatori di compromissione
- Protezione contro l'elusione dei dispositivi di rilevamento EDR

Controllo dispositivo

- Reti WiFi • Chiavetta USB • Bluetooth - Accesso al volume del disco • Connessioni di rete • Controllo dell'esecuzione

Agente ottimizzato

- Utilizzo della memoria
- Utilizzo della CPU

Politica di sicurezza

- Adattamento dinamico in base al contesto
- Analisi comportamentale e set di regole per il controllo dei dispositivi fornite e gestite da Stormshield
- Gestione delle regole Yara

Amministrazione centralizzata

- Gestione delle policy per gruppi di agenti
- Gestione degli amministratori in base al ruolo
- Attivazione / disattivazione dei moduli per gruppi di agenti
- API REST per l'integrazione con prodotti di terze parti
- Report di attività con indicatori MCS e MCO in formato HTML
- Notifica automatica via e-mail degli avvisi di sicurezza

COMPATIBILITÀ

AGENTE

Risorse
CPU:
1 core 1 Ghz (min.) - 2 core 2 GHz (consigliato)

RAM:
1 GB (min.) - 2 GB (consigliato)

Spazio su disco:
100 MB (installazione) - 200 MB (dati)

Sistema operativo
Client:
Windows 7 SP1, 8.1, 10 e 11

Server:
Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 (inclusa la versione Core)

AMMINISTRAZIONE

Possibilità di gestione SaaS o on-premise

PER LA GESTIONE ON-PREMISE

Backend
CPU:
1 core 1 Ghz (min.) - 2 core 2GHz (consigliato)

RAM:
1 GB (min.) - 2 GB (consigliato)

Spazio su disco:
100 MB (installazione) - 200 MB (dati)

Server:
Windows Server 2012 R2, 2016, 2019 e 2022 (inclusa la versione Core)

Gestione agente
CPU:
2 core 2 GHz (minimo)

RAM:
2 GB (minimo)

Spazio su disco:
200 MB (installazione) - 1 GB (dati - minimo)

Client:
Windows 10 e 11

Server:
Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 (inclusa la versione Core)

Database:
SQL Server 2017 e successivi