STORMSHIELD

I sistemi DPI e la sicurezza della rete

La tecnologia IPS Stateful DPI negli ambienti OT

In sintesi

Al giorno d'oggi, la segmentazione delle reti operative rappresenta una strategia di primo livello nella lotta contro i cyber-attacchi. Tuttavia, per far fronte a nuove e sempre più sofisticate minacce, è necessario l'impiego di soluzioni d'ispezione approfondita (DPI - *Deep Packet Inspection*) dei messaggi scambiati, per anticipare la protezione delle reti sensibili.

Per vincere questa sfida in ambito OT, le soluzioni di sicurezza implementate devono soddisfare rigorosi requisiti in termini **di disponibilità, integrità e riservatezza**, determinati dalle varie attività aziendali che le reti operative supportano.

L'implementazione di un sistema IPS (*Intrusion Prevention System*) il più vicino possibile alle apparecchiature deve quindi rispettare questi aspetti per poter applicare una politica di sicurezza proattiva e sostenibile garantendo la sicurezza delle reti operative.

A tal fine, occorre soddisfare quattro aspetti principali:

- una **soluzione integrata** che garantisca una conoscenza approfondita dei protocolli industriali;
- la **capacità di monitorare la conformità dei messaggi operativi** per meglio individuare le anomalie e preservare le risorse della rete OT;
- una **protezione proattiva contro diverse tipologie di minacce** per contrastare gli attacchi mirati ed evitare interruzioni della produzione;
- un **approccio contestuale allo scambio di messaggi** per garantire la conformità con le procedure operative.

Il presente white paper illustra i vari meccanismi che un sistema IPS deve adottare per svolgere la sua missione di rilevamento e protezione dagli attacchi. Offre inoltre una panoramica degli elementi che devono essere integrati in un IPS per adattarlo alle proprie esigenze di sicurezza.

Questo white paper è destinato ai manager tecnici, ai responsabili della manutenzione, delle attività e delle operazioni addetti alla gestione delle infrastrutture critiche e ai responsabili della sicurezza dei sistemi informatici.

Stormshield
In tutto il mondo, le aziende, le istituzioni governative e gli organismi di difesa hanno bisogno di partner fidati che sostengano la loro trasformazione digitale e garantiscano la sicurezza informatica delle loro infrastrutture, dei loro utenti e dei loro dati. Le tecnologie Stormshield, certificate al più alto livello europeo (EU Restricted, NATO Restricted, EAL3/EAL4+ Common Criteria e visti di sicurezza rilasciati dall'ANSSI), rispondono concretamente alle sfide legate alle infrastrutture IT e OT per proteggere le vostre attività. Le nostre soluzioni di sicurezza vi consentiranno di svolgere la vostra attività in tutta tranquillità.

Sommario

1. Il contesto
2. I rischi informatici associati alle reti operative
3. I sistemi di difesa: sonda industriale o IPS?
4. Principi generali dell'Intrusion Prevention System
   Firma o ricerca mirata del protocollo: due approcci al monitoraggio della conformità al protocollo

   L'analisi contestuale come fulcro della sicurezza degli scambi

   La ricerca di minacce per la rete

   La necessità di firme personalizzate
5. I criteri per la scelta del giusto IPS
6. Il motore *Stateful DPI* Stormshield

Il contesto

I cyber-attacchi contro le infrastrutture operative diventano sempre più sofisticati. Sequenziati in diversi stadi, diventano virulenti e troppo complessi da rilevare dai vari sistemi di protezione. Le Advanced Persistent Threat (APT) sono attacchi informatici che utilizzano un insieme di tecniche e metodi strategicamente combinati al fine di raggiungere un obiettivo ben definito. Restano inattive per un periodo di tempo prolungato in modo da non destare sospetti e in genere mirano all'estrazione di dati ad alto valore aggiunto (brevetti, segreti industriali, ecc.).

Di conseguenza, anche se la maggior parte delle aziende e delle organizzazioni dichiara di essere consapevole dei rischi informatici e delle implicazioni che questi possono comportare (perdita o furto di dati, interruzioni della produzione, ecc.), spesso sono più a rischio di quanto pensino. Con l'emergere negli ultimi anni dell'*Internet Of Things* (IIoT), i cyber-attacchi prendono di mira le aziende appartenenti ai settori più disparati, come l'aeronautica, l'energia nucleare, l'elettricità, la salute, ecc. Aziende di vitale importanza per la società che diventano bersagli privilegiati.

> La sfida è sviluppare un'architettura in grado di garantire la trasmissione, l'elaborazione e **il mantenimento dell'integrità dei dati** tra i sistemi.
>
> Cigref

In alcuni casi, tuttavia, tali società conoscono i punti deboli dei loro sistemi, ma non dispongono dei mezzi per sostituire le applicazioni e/o le tecnologie interessate. Questo scenario è comune nell'ambito delle reti operative e critiche, come quelle del settore sanitario, che utilizzano applicazioni supportate solo da sistemi operativi datati. Nel settore industriale alcuni componenti, seppur obsoleti, vengono mantenuti, accrescendo così il rischio di subire un attacco innestato silenziosamente da tempo. Come emerge da uno studio condotto nel novembre 2019[1], alcune vulnerabilità e lacune sono state sfruttate degli autori di attacchi informatici per oltre dieci anni e continuano a esserlo tutt'oggi.

Tuttavia, la cybersicurezza industriale resta ancora una disciplina relativamente nuova. L'esperienza nell'ambito del mondo IT[2], come ad esempio l'analisi dei rischi, risulta inoltre utile per fornire una risposta adeguata ed efficace operando adeguamenti minimi.

Questo white paper si propone di affrontare e analizzare i metodi di protezione delle reti di tipo IPS e le sfide associate alla sicurezza delle reti OT.

[1] Stormshield, www.stormshield.com/news/what-will-2020-cybersecurity-trends-be/

[2] Stormshield, www.stormshield.com/news/it-ot-networks-why-convergence-is-delicate/

I rischi informatici associati alle reti operative

Negli ultimi anni, la trasformazione digitale contraddistinta dalla convergenza IT/OT o dall'utilizzo del Edge/Cloud Computing[3] ha portato le reti aziendali industriali di qualsiasi dimensione ad una maggiore iperconnettività. I progetti **di eccellenza operativa**, connessi all'Industria 4.0 (come l'ottimizzazione avanzata tra la catena di produzione e l'ERP aziendale) rendono le reti operative più permeabili ai rischi informatici.

Bisogna riconoscere che nel mondo OT, non appena vengono connessi sistemi e macchine precedentemente isolati dalla rete, aumenta la possibilità di hackeraggio con gravi conseguenze: danni materiali, interruzione della produzione o furto di processi industriali.

Con l'attuale convergenza IT/OT, molti produttori iniziano a implementare una governance globale dei loro siti per poter beneficiare di una migliore visibilità sulle reti operative. Pertanto, al fine di garantire un buon monitoraggio delle problematiche legate alla cybersicurezza industriale, **il mondo IT e il mondo OT devono dialogare analizzando e valutando i rischi per facilitare un'efficiente implementazione dei processi di amministrazione e gestione della sicurezza della rete.**

Recentemente, in seguito all'attacco del ransomware EKANS (o Snake) **siamo (ri)diventati consapevoli della pericolosità** dei rischi che un'intrusione nella rete aziendale può causare. Ci sono fattori che possono favorire questo tipo di rischio: ad esempio, la mancanza di omogeneità tra le apparecchiature installate e le postazioni di controllo o la componentistica industriale con standard e/o requisiti diversi. Elementi simili che coesistono nello stesso ambiente possono causare guasti che portano al collasso dell'intero sistema.[4]

[3] Forbes, www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/#5f46307f24ae

[4] Stormshield, www.stormshield.com/news/the-manufacturing-industries-faced-with-cyber-threats/

Come ha sottolineato in un precedente documento Vincent Riondet, responsabile del team di progetto e servizi di cybersicurezza di Schneider Electric France, nella maggior parte dei siti industriali " *utilizziamo infrastrutture approssimativamente vecchie con architetture di rete e sistemi operativi più o meno recenti, che non necessariamente integrano standard di sicurezza avanzati, perché sono costosi da aggiornare* ".

L'applicazione di barriere di protezione multiple come la segmentazione, il controllo dei flussi, il rilevamento e la prevenzione delle intrusioni può essere molto utile per combattere le minacce che si insinuano nei flussi di rete. Inoltre, non è più sufficiente eseguire il controllo degli accessi attraverso la sola autorizzazione o meno di un protocollo di comunicazione (mediante la sua porta); ora bisogna anche analizzare i comandi inviati tramite i protocolli aziendali autorizzati.

Pertanto, la messa in sicurezza dell'architettura di rete deve ruotare intorno alla protezione e all'aggiornamento di tali misure per evitare la perdita di dati o l'interruzione dei processi aziendali. Qual è lo scopo? Migliorare la lotta contro i cyber-attacchi che possono verificarsi in qualsiasi momento. **Per questo motivo è essenziale implementare sistemi di difesa proattivi e il più possibile vicini alle infrastrutture critiche.**

I sistemi di difesa: sonda industriale o IPS?

Sebbene sia essenziale monitorare le infrastrutture industriali, non esiste un'unica griglia di valutazione tecnica applicabile a tutte le architetture operative. Una delle domande da porsi è: **chi gestisce i messaggi di allerta generati e come?** Infatti, al di là degli aspetti tecnici, l'installazione di una sonda industriale richiede **un team operativo qualificato,** in grado di gestire e analizzare **una grande quantità d'informazioni** per individuare gli eventi critici e risalire alle potenziali problematiche legate alla sicurezza, se presenti.

Anche se queste soluzioni possono essere complementari, l'eventuale scelta tra una sonda industriale e una soluzione IPS deve basarsi su una serie di parametri, a seconda dell'utilizzo. A tale scopo è necessario un esame dettagliato dell'intera architettura della rete operativa. A seconda delle proprie esigenze, **occorre misurare la criticità della sicurezza di ciascun elemento per individuare la protezione adeguata**.

È altresì importante pensare a come la propria nuova soluzione si integrerà nella politica globale di sicurezza informatica, nonché nei processi e nell'organizzazione attuali e futuri.

LO SAPEVATE?

I sistemi IPS offrono spesso le stesse funzionalità IDS (Intrusion Detection System) delle sonde industriali. Rispetto alle sonde, i sistemi IDS non offrono lo stesso livello di accuratezza nella capacità di individuazione, ma garantiscono il riconoscimento dei flussi che attraversano il dispositivo.

È consigliabile **implementare gradualmente l'IPS attraverso una procedura di analisi del traffico di rete in IDS.**. Questa fase preparatoria consente di mappare i flussi e di individuare i potenziali falsi positivi prima di attivare la prevenzione attiva delle intrusioni per bloccare i flussi illegittimi.

Una sonda industriale è uno strumento **passivo** in grado di **rilevare** potenziali flussi malevoli all'interno della rete	**Un sistema IPS** è uno strumento di protezione **attivo** in grado di **individuare** e **bloccare** potenziali flussi malevoli all'interno della rete
• Non blocca i pacchetti di rete	• Agisce bloccando i pacchetti sospetti
• Necessita di un intervento umano per la gestione degli incidenti	• È autonomo nella gestione degli allarmi innescati
• Visualizza una copia completa della rete	• Si posiziona all'interno della rete
• Fornisce una grande quantità d'informazioni	• Avvisa solo in caso di problemi
• È sensibile alle azioni di flooding	• Blocca questo tipo di attacchi
• È "invisibile" nella rete in caso di attacco	• Può essere individuato più facilmente

LO SAPEVATE?

Esistono soluzioni IPS che integrano un **sistema di sicurezza (funzione di bypass) per garantire, se necessario, la continuità dell'attività operativa in caso di malfunzionamento.**

Principi generali dell'Intrusion Prevention System

In breve

Il ruolo principale dell'IPS è **monitorare i pacchetti di rete e il loro contenuto in tempo reale, al fine di applicare regole predefinite a seconda dell'attacco rilevato e dell'obiettivo designato.**.

DA NON CONFONDERE

Esistono 2 tipi diversi di IPS:

- **HIPS (Host-Based Intrusion Prevention System)**: IPS per il monitoraggio delle postazioni di lavoro.
- **NIPS (Network Intrusion Prevention System)**: IPS per il monitoraggio della rete.

Come funziona?

I sistemi di prevenzione delle intrusioni sono posti all'interno della rete che proteggono. Analizzano i pacchetti di rete per verificare preventivamente la conformità al protocollo e il monitoraggio dei comandi.

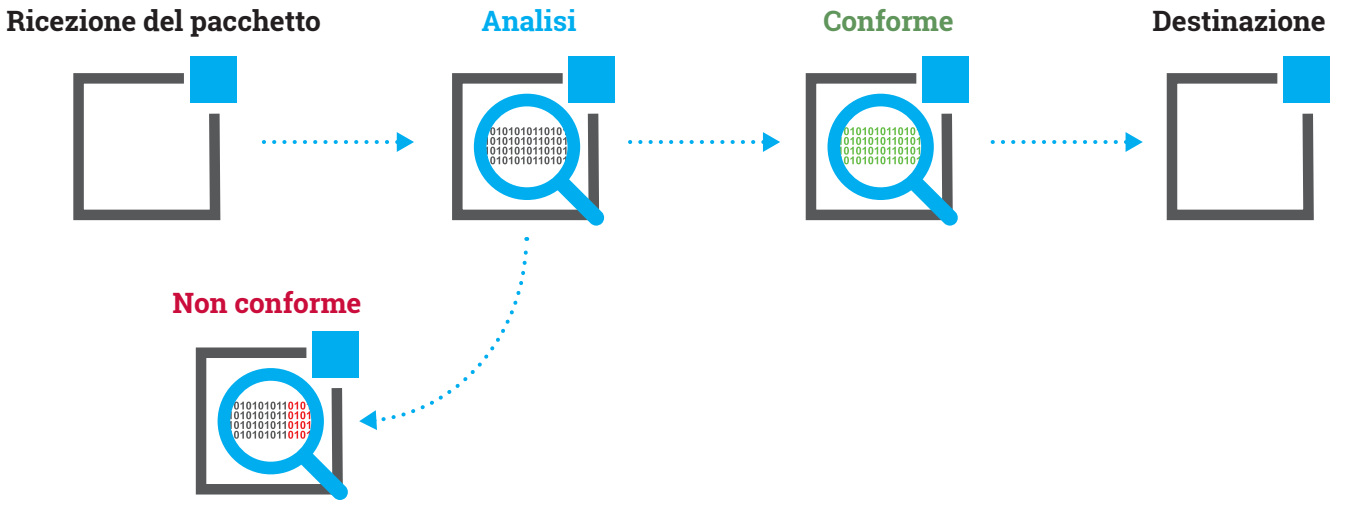
Alcuni sistemi IPS sono anche in grado di individuare comportamenti anomali.

I sistemi IPS verificano poi che i pacchetti di rete non contengano un insieme di dati che corrispondono alle firme dei malware noti, per bloccare i tentativi di attacco.

Che cosa offre l'IPS?

Questa tecnologia garantisce la protezione della rete per un'infrastruttura informatica e/o operativa.

A tal fine, il supporto dei protocolli aziendali utilizzati costituisce un criterio di selezione del sistema IPS da non trascurare, al fine di garantire una buona copertura nella protezione dei comandi di controllo.

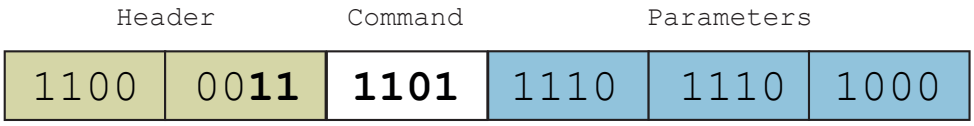


Firma o ricerca del protocollo mirata: due approcci al monitoraggio della conformità al protocollo

I migliori motori IPS garantiscono la decodifca dei protocolli utilizzati e verificano la conformità (lunghezza del pacchetto dati, tipo di protocollo, ecc.) di ciascun messaggio rispetto al formato previsto definito negli standard di tali protocolli. Sono in grado di analizzare le informazioni in modo molto dettagliato, da cui il termine ***Deep Packet Inspection*** **(DPI)** frequentemente utilizzato.

La DPI (Deep Packet Inspection) valuta l'intestazione di un pacchetto trasmesso e i dati associati eliminando qualsiasi non conformità al protocollo.

Prendiamo l'esempio di un pacchetto di rete legittimo, che veicola un comando:



Valutando la conformità al protocollo, un sistema IPS cercherà specifche sequenze di bits con due scopi principali:

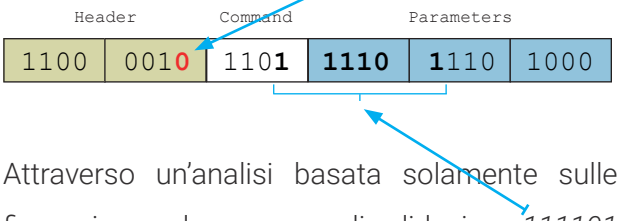
1. **Riconoscimento del protocollo**: in primo luogo, riconoscere il protocollo in transito attraverso la ricerca di marcatori caratteristici.
2. **Conformità al protocollo**: assicurarsi quindi che le sequenze di byte, corrispondenti al protocollo individuato, siano presenti nel pacchetto di rete.

Ad esempio si potrebbe ricercare la sequenza di validazione "111101" **evidenziata qui sopra in grassetto**.

LO SAPEVATE?

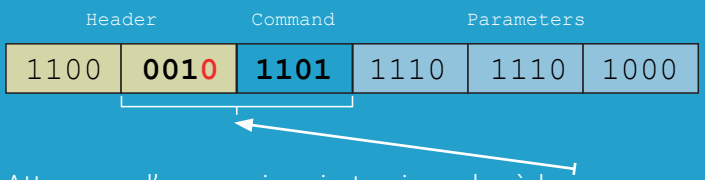
L'implementazione specifca dei protocolli nel settore industriale utilizza per lo più valori di comando personalizzati (custom command). **L'analisi del protocollo basata sulle frme non riconosce questi valori, generando quindi errori di rilevamento.**

Consideriamo ora il pacchetto **illegittimo** (malformato):.



Attraverso un'analisi basata solamente sulle firme si cerca la sequenza di validazione *111101* **in qualsiasi punto del pacchetto**.

Con questo approccio tale sequenza viene rilevata all'interno del pacchetto (evidenziata in grassetto) nonostante non sia nella giusta posizione. La tecnica basata sull'analisi delle firme lascia passare il pacchetto malformato (generando un falso negativo).



Attraverso l'approccio mirato si cercherà la sequenza di validazione **solamente nella posizione in cui dovrebbe trovarsi**. Con l'approccio mirato, il pacchetto malformato viene quindi bloccato.

Pertanto, l'analisi del protocollo mirata presenta due grandi vantaggi:

1. Valutazione precisa di conformità al protocollo
2. Limitazione degli errori di rilevamento

L'analisi contestuale come fulcro della sicurezza degli scambi

Questo approccio consente di bloccare i cyber-attacchi contestualizzando i messaggi scambiati tra due elementi della rete. A tal fine, l'**analisi contestuale** verifica che la sequenza dei messaggi scambiati segua la logica definita nello standard del protocollo e non mostri alcun comportamento anomalo.

Tramite questa analisi è possibile esaminare e verificare il messaggio derivante da uno scambio tra due dispositivi tenendo conto dei messaggi precedenti. **Questa tecnologia avanzata protegge e garantisce l'integrità delle vostre risorse di rete e degli ambienti operativi.**

Consideriamo l'esempio di un'apparecchiatura "A" che può essere gestita da più controller. Il controller "A" richiederà l'assunzione del comando inviando un'apposita richiesta. L'apparecchiatura "A" riconoscerà tale richiesta inviando l'accettazione del comando a condizione che non sia già gestita da un altro controller. Partendo da questo esempio, immaginiamo che un aggressore assuma il comando dell'apparecchiatura "A". Il sistema IPS visualizzerà un pacchetto inviato spontaneamente dall'apparecchiatura "A" che accetta una richiesta di acquisizione che non è stata identificata dal sistema. Grazie all'analisi degli elementi di contesto, l'IPS può riconoscere tale comportamento come anomalo e quindi bloccarlo.

VANTAGGI

Questo tipo di soluzione IPS, denominato **Stateful DPI**, aumenta il **livello di sicurezza dell'infrastruttura operativa e riduce quindi il rischio di compromettere le risorse di rete.**

Infatti, effettuando l'**analisi contestuale** delle sequenze di pacchetti che transitano nella rete operativa, questo tipo di IPS permette di esaminare le informazioni relative agli scambi tra due dispositivi. **Esso prende in considerazione diversi parametri del messaggio attuale confrontandoli con quelli già scambiati**. Questi parametri possono essere: la direzione della comunicazione tra i due dispositivi, il tipo di comando da eseguire o i valori del comando da applicare.



La ricerca di minacce per la rete insite negli scambi

Il malware Triton costituisce un valido esempio della vulnerabilità delle reti OT e conferma l'importanza di un sistema IPS per individuare le minacce che giungono dalla rete, anche quando l'attacco rispetta la conformità al protocollo e segue la logica definita nel relativo standard. Infatti, l'IPS cerca nei dati del pacchetto di rete una sequenza di byte corrispondente a una firma di attacco nota.

Va però osservato che alcuni malware sono in grado di evolvere. Le sue mutazioni richiedono ovviamente nuove firme specifiche: se queste non vengono implementate nell'IPS, il sistema non sarà in grado di rilevarle. **Per questo motivo, si raccomanda di utilizzare un IPS in grado di sfruttare delle firme proattive che comprenderanno le varie mutazioni di un attacco, permettendo il loro rilevamento.**

VANTAGGI

La protezione proattiva presenta un ulteriore vantaggio significativo: il numero di firme necessarie nel database è ridotto, **la ricerca di modelli di attacco noti nella rete è più rapida e la latenza di rete introdotta dall'analisi risulta ridimensionata.**

Ancora meglio, se il motore dell'IPS è in grado di sfruttare l'analisi dettagliata eseguita durante il controllo di conformità al protocollo per individuare solo le firme di attacco rilevanti in ogni parte dei messaggi, **le prestazioni vengono ulteriormente aumentate e di conseguenza la percentuale di falsi positivi viene drasticamente ridotta.**

Triton: un cyber-attacco contro gli ICS

Il malware Triton è stato sviluppato per colpire i sistemi ICS di un impianto petrolchimico saudita al fine di provocare un'esplosione. Fortunatamente, gli aggressori hanno commesso un errore, innescando un arresto di emergenza dei sistemi critici e rivelando di fatto l'intrusione nella rete.

Stuxnet: una variante dei "worms informatici"

Il virus Stuxnet è stato progettato per attaccare le centrifughe della centrale nucleare iraniana di Natanz. La complessità di questo malware si basa su un'ottima conoscenza dei processi industriali e delle vulnerabilità del sistema operativo Windows. Gli autori del cyber attacco hanno utilizzato exploit zero-day sofisticati e poco comuni.

Successivamente, sono state utilizzate delle varianti di Stuxnet per attaccare altre infrastrutture industriali.

Alcune organizzazioni industriali ed esperti del settore hanno pubblicato delle guide di best practice per la corretta gestione dei sistemi di controllo. Tra le altre cose, menzionano la necessità di segmentare la rete, controllare gli accessi, acquisire sistemi consolidati, implementare antivirus e motori di prevenzione delle intrusioni di tipo IPS.

Di fronte a questo tipo di minaccia, un sistema IPS proattivo che tenga conto delle potenziali mutazioni dello stesso malware è un aiuto essenziale, se non addirittura vitale, per la sopravvivenza del sistema industriale.

L'importanza delle firme personalizzate

Un sistema IPS deve essere in grado di conoscere e gestire i messaggi scambiati tramite protocolli industriali per proteggere adeguatamente il sistema operativo. Ogni parametro trasmesso nei messaggi di comando deve essere correttamente analizzato e verificato, poiché ogni comunicazione di rete agisce direttamente su un particolare processo aziendale.

Un sistema IPS deve essere in grado di offrire la personalizzazione delle firme per implementare il controllo dei messaggi di comando in conformità con i processi aziendali e i vincoli operativi.

Le soluzioni IPS possono garantire questa verifica attraverso firme personalizzate. L'obiettivo: controllare i messaggi di comando in modo che siano conformi ai processi aziendali e ai vincoli operativi. Questo rappresenta il punto più critico in un ambiente operativo, affinché i valori non superino determinati limiti che potrebbero mettere a repentaglio l'intero processo.

Prendiamo ad esempio una diga per la gestione idrica, dove i comandi di controllo devono necessariamente considerare la portata supportata da una paratoia (in questo caso la portata totale è da 50 a 5.000 m^3/s). Anche se i sistemi ICS/SCADA più recenti sono meno sensibili, è importante per le infrastrutture più datate che i valori trasmessi al controller rispettino questi limiti per evitare flussi più elevati con gravi conseguenze, come le inondazioni.

È altresì di fondamentale importanza poter verificare questi valori in tempo reale.

700+
protocolli proprietari

UMAS, S7, TSAA, SAAT, HNZ, ...

20+
protocolli standardizzati

Modbus, UMAS, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA...

VANTAGGI

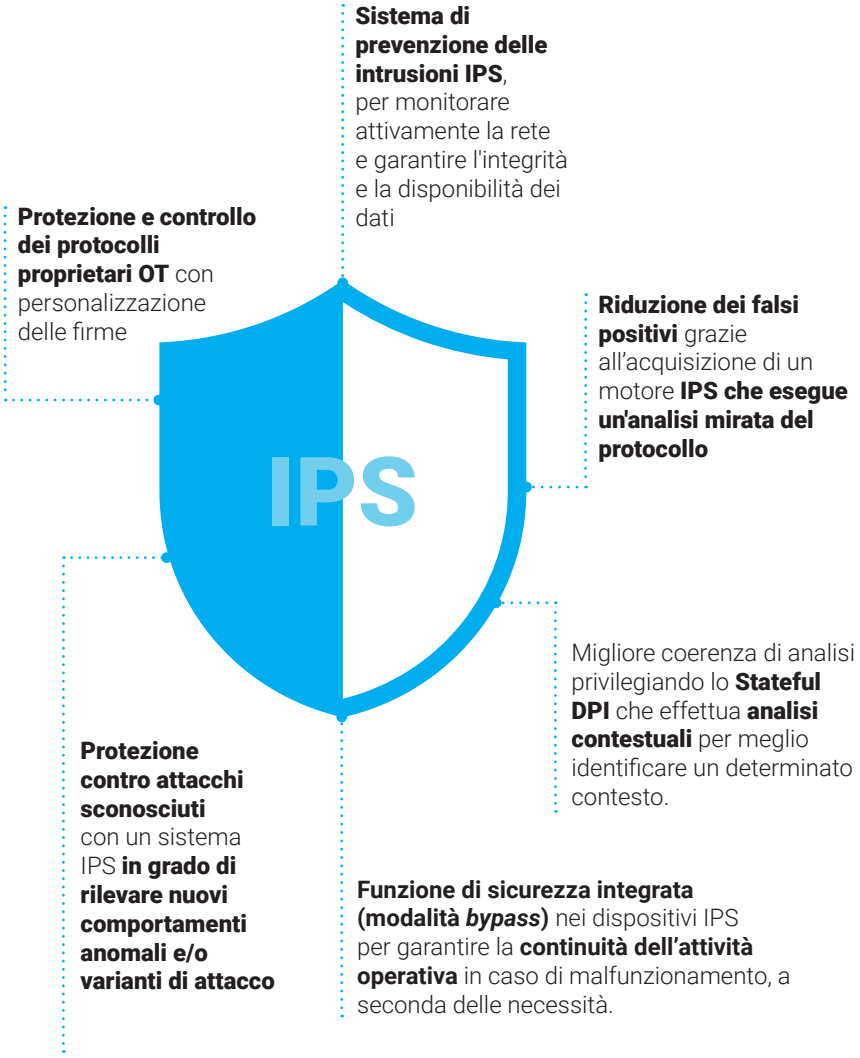
Le firme personalizzate consentono di:

- **adattarsi** al contesto aziendale;
- **implementare** l'analisi del protocollo su protocolli proprietari;
- **controllare** i cosiddetti valori sensibili relativi alla sicurezza del sistema operativo;
- **garantire** il buon funzionamento dei processi operativi.

I criteri per la scelta del giusto IPS

La scelta di un sistema IPS può sembrare un compito difficile e delicato, tenendo conto delle sfide sopra esposte.

Il diagramma sottostante vi fornirà una rapida panoramica delle caratteristiche più importanti.



LO SAPEVATE?

I sistemi di protezione costituiti da diversi componenti rendono la loro integrazione più complessa. Oltre alla molteplicità degli strumenti di gestione, licenza e certificazione, queste soluzioni aumentano generalmente la latenza sulla rete.

Ottimizzate la produttività della vostra azienda scegliendo una soluzione IPS all-in-one facile da implementare e semplice da usare. La sua chiara interfaccia grafica migliora l'integrazione e la gestione dell'IPS, fornendo una maggiore visibilità dei sistemi da proteggere.

Il motore*Stateful DPI* Stormshield

Dotarsi di un sistema di alta qualità per la prevenzione delle intrusioni e la segmentazione delle reti operative serve a garantire la disponibilità e l'integrità dei vostri sistemi

Potenti analisi di flusso

CONTROLLO DELLA CONFORMITÀ AI PROTOCOLLI
combinando il controllo dei pacchetti e la conformità al protocollo dell'applicazione

DPI su 10+ protocolli supportati
Modbus, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA, etc.

Un IPS industriale

basato su analisi multiple per assicurare una risposta proattiva, che previene anche gli attacchi zero-day

Analisi contestuale

Studio del comportamento secondo il contesto aziendale

Ottimizzazione dell'integrazione dell'IPS all'interno dell'OS incorporato

Ricerca di firme contestuali in un database più granulare e mirato

Analisi del protocollo mirata e contestuale per ridurre la latenza e limitare i falsi positivi

Prestazioni superiori grazie a...

FIRME PERSONALIZZATE
PERCHÉ NE AVETE BISOGNO?

1. Monitorare la conformità ai processi operativi
2. Prevenire danni alla strumentazione industriale e all'ambiente
3. Adottare un'idonea analisi del protocollo

Gestione intuitiva

Soluzione all-in-one

Interfaccia utente chiara e facile da usare

COMPETENZA NELLA PROTEZIONE DELLE RETI OT: CO-DESIGN CON FORNITORI, INTEGRATORI INDUSTRIALI E CLIENTI

www.stormshield.com

STORMSHIELD

La scelta europea della sicurezza informatica

In tutto il mondo, le aziende, le istituzioni governative e gli organismi di difesa hanno bisogno di partner fidati che sostengano la loro trasformazione digitale e garantiscano la sicurezza informatica delle loro infrastrutture, dei loro utenti e dei loro dati. Le tecnologie Stormshield, certificate al più alto livello europeo (EU Restricted, NATO Restricted, EAL3/EAL4+ Common Criteria e visti di sicurezza rilasciati dall'ANSSI), rispondono concretamente alle sfide legate alle infrastrutture IT e OT per proteggere le vostre attività. **Le nostre soluzioni di sicurezza vi consentiranno di svolgere la vostra attività in tutta tranquillità.** www.stormshield.com

Qualsiasi diffusione, riproduzione o rappresentazione, anche parziale, del presente white paper per scopi diversi dall'uso privato su qualsiasi supporto è vietata e può comportare la responsabilità civile e penale per chiunque non si attenga a tale divieto.