Cisco Stealthwatch Enterprise

Per hardware UCS

Stealthwatch™ Enterprise è la soluzione di analisi della sicurezza e visibilità leader del settore che sfrutta la telemetria aziendale dell'infrastruttura di rete esistente. Offre rilevamento avanzato delle minacce, risposta accelerata alle minacce e segmentazione della rete semplificata utilizzando il machine learning multilivello e la modellazione comportamentale avanzata, il tutto nella rete estesa.

Con Stealthwatch Enterprise, ottieni visibilità in tempo reale che ti permette di ottenere informazioni migliori sulle attività che si verificano all'interno della rete. Puoi scalare tale visibilità al cloud, alla rete, alle filiali, al data center, fino agli endpoint.

Al cuore di Stealthwatch Enterprise ci sono: la licenza Flow Rate, Flow Collector, la console di gestione e Flow Sensor. Per ulteriori funzionalità, consultare le singole schede tecniche qui sotto:

- Licenza Cisco Stealthwatch Endpoint: disponibile come licenza aggiuntiva per estendere la visibilità ai dispositivi degli utenti finali.
- Cisco Stealthwatch Cloud: disponibile come offerta di prodotti per fornire visibilità e rilevamento delle minacce all'interno delle infrastrutture di cloud pubblico come Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform.
- **Licenza Threat Intelligence**: un feed di intelligence globale sulle minacce supportato da Cisco Talos, gruppo di intelligence sulle minacce leader del settore, fornisce un ulteriore livello di protezione da botnet e altri attacchi sofisticati. Correla l'attività sospetta nell'ambiente di rete locale con i dati su migliaia di campagne e server di comando e controllo noti per fornire un rilevamento altamente affidabile e una risposta più rapida alle minacce. Cisco Talos esamina 1,5 milioni di campioni univoci di malware e blocca 20 miliardi di minacce al giorno.

Vantaggi del sistema

Con una panoramica e un’analisi del traffico di rete eccezionali, Stealthwatch Enterprise migliora notevolmente:

- Il rilevamento delle minacce in tempo reale
- La reazione agli incidenti e l’analisi forense
- La segmentazione della rete
- Le prestazioni della rete e la pianificazione della capacità
- La conformità ai requisiti normativi

Componenti indispensabili del sistema

Licenza Flow Rate

La licenza Flow Rate serve per la raccolta, la gestione e l'analisi della telemetria dei flussi e dei flussi aggregati nella console di gestione. La licenza Flow Rate definisce anche il volume dei flussi che possono essere raccolti e dipende dai flussi al secondo (fps). Le licenze possono essere combinate in qualsiasi modo per raggiungere il livello desiderato di capacità dei flussi.

Flow Collector

Flow Collector sfrutta la telemetria aziendale, ad esempio NetFlow, IPFIX e altri tipi di dati dei flussi dell'infrastruttura esistente, come router, switch, firewall, endpoint e altri dispositivi dell'infrastruttura di rete. Flow Collector può anche ricevere e raccogliere la telemetria da origini di dati proxy, che possono essere analizzate da Global Threat Analytics (in precedenza Cognitive Threat Analytics), il motore di machine learning multilivello, per una visibilità approfondita del traffico di rete e Web. Inoltre, Stealthwatch Enterprise, tramite Encrypted Traffic Analytics, può usare l'analisi per individuare schemi dannosi nel traffico criptato in modo da identificare le minacce e accelerare la risposta. Anche se questa funzionalità è integrata nel sistema senza costi aggiuntivi, andrà attivata dopo l'implementazione.

I dati telemetrici vengono analizzati per fornire una panoramica completa delle attività di rete. Mesi o addirittura anni di dati possono essere archiviati per creare un audit trail da usare per migliorare le indagini forensi e le iniziative di conformità. Il volume di informazioni telemetriche raccolte dalla rete dipende dalla capacità dei Flow Collector implementati. Possono essere installati diversi Flow Collector. I Flow Collector sono disponibili come appliance hardware o come macchine virtuali. La tabella 1 illustra i vantaggi di Flow Collector.

Tabella 1. Vantaggi principali di Flow Collector

Vantaggio	Descrizione
Rilevamento delle minacce	Acquisisce i record proxy e li associa ai record dei flussi, fornendo le informazioni di URL e delle applicazioni degli utenti per ogni flusso, in modo da aumentare l'analisi del contesto. Questo processo migliora la capacità dell'azienda di individuare le minacce con precisione e riduce il tempo medio di conoscenza (MTTK, Mean Time To Know).
Monitoraggio dei flussi del traffico	Monitora i flussi del traffico in centinaia di segmenti di rete contemporaneamente, in modo da individuare il comportamento di rete sospetto. Questa funzionalità è particolarmente importante per le grandi aziende.
Conservazione dei dati per lunghi periodi	Consente alle aziende e agli enti di conservare grandi quantità di dati per lunghi periodi.
Scalabilità	Ha ottime prestazioni in ambienti a velocità estremamente elevata ed è in grado di proteggere ogni parte della rete che può essere raggiunta da IP, a prescindere dalle dimensioni.
Deduplicazione e stitching	Esegue la deduplicazione in modo da contare una sola volta tutti i flussi che possono aver attraversato più di un router, quindi collega le informazioni dei flussi per offrire la visibilità completa di una transazione della rete.
Scelta dei metodi di consegna	È possibile ordinare la versione Appliance (Appliance Edition), un dispositivo scalabile adatto ad aziende di qualsiasi dimensione, oppure la Virtual Edition, progettata per eseguire le stesse funzioni dell'appliance, ma in un ambiente VMware. Questa soluzione è scalabile in modo dinamico in base alle risorse allocate.

* Il numero massimo di flussi al secondo può cambiare a seconda delle condizioni della rete.

Specifiche di Flow Collector

- Stealthwatch Flow Collector 4200 - Codice prodotto: ST-FC4200-K9
- Stealthwatch Flow Collector 5200 - Codice prodotto: ST-FC5200-K9
- Stealthwatch Flow Collector Virtual Edition può essere configurato come FCVE-1000, FCVE-2000 o FCVE-4000 - Codice prodotto: L-ST-FC-VE-K9

Nota: queste specifiche si applicano al sistema Stealthwatch versione 6.9.1 e più recenti

Console di gestione

La console di gestione di Stealthwatch aggrega, organizza e presenta l'analisi di un massimo di 25 Flow Collector, Cisco Identity Services Engine e altre fonti. Utilizza le rappresentazioni grafiche del traffico di rete, le informazioni sull'identità, i report di riepilogo personalizzati e l'intelligence di sicurezza e di rete integrata per fornire un'analisi completa.

La capacità della console determina il volume di dati telemetrici che possono essere analizzati e presentati, nonché il numero di Flow Collector implementati. La console è disponibile come appliance hardware o macchina virtuale. La tabella 2 elenca i vantaggi delle console.

Tabella 2. Principali vantaggi della console di gestione

Vantaggio	Descrizione
Dati aggiornatissimi in tempo reale	Fornisce il flusso di dati per il monitoraggio del traffico in centinaia di segmenti di rete contemporaneamente, permettendo di individuare il comportamento di rete sospetto. Questa funzionalità è particolarmente importante per le grandi aziende.
Funzionalità di rilevamento e assegnazione di priorità alle minacce della sicurezza	Rileva rapidamente e assegna le priorità alle minacce della sicurezza, determina l'utilizzo improprio della rete e le prestazioni subottimali e gestisce la reazione agli eventi nell'intera azienda, il tutto da un unico centro di controllo.
Gestione delle appliance	Configura, coordina e gestisce le appliance Cisco StealthWatch, incluse Flow Collector, Flow Sensor e UDP Director.
Utilizzo di vari tipi di dati di flussi	Sfrutta tipi diversi di dati di flussi, inclusi NetFlow, Internet Protocol Flow Information Export (IPFIX) e sFlow. Risultato: un'economica protezione della rete basata sui comportamenti.
Scalabilità	Supporta anche le esigenze delle reti di grandi dimensioni. Ha ottime prestazioni in ambienti a velocità estremamente elevata ed è in grado di proteggere ogni parte della rete che può essere raggiunta da IP, a prescindere dalle dimensioni.
Audit trail delle transazioni della rete	Fornisce un audit trail completo di tutte le transazioni della rete per consentire indagini di analisi forense più efficaci.
Mappe dei flussi relazionali personalizzabili e in tempo reale	Offre visualizzazioni grafiche sullo stato attuale del traffico dell'azienda. Gli amministratori possono creare facilmente mappe della rete in base a qualsiasi criterio, come posizione, funzione o ambiente virtuale. Creando una connessione tra due gruppi di host, gli operatori possono analizzare rapidamente il traffico tra i due. Quindi, semplicemente selezionando un punto di dati in questione, possono ottenere informazioni ancora più dettagliate su quello che succede in qualsiasi momento.
Opzioni di consegna flessibili	Puoi ordinare l'appliance fisica, un dispositivo scalabile adatto ad aziende di ogni dimensione, oppure la Virtual Edition, progettata per svolgere le stesse funzioni dell'appliance, ma in un ambiente VMware.

Specifiche della console di gestione

- Stealthwatch Management Console 2200 - Codice prodotto: ST-SMC2200-K9
- Stealthwatch Management Console Virtual Edition può essere configurata come SMC VE o SMC VE 2000 - Codice prodotto: L-ST-SMC-VE-K9

Nota: queste specifiche si applicano al sistema Stealthwatch versione 6.9.1 e più recenti

Componenti opzionali del sistema

Flow Sensor

Flow Sensor è un componente opzionale di Stealthwatch Enterprise e produce telemetria per segmenti dell'infrastruttura di switching e routing che non possono generare NetFlow in modo nativo. Inoltre fornisce visibilità sui dati del livello applicativo. Oltre a tutta la telemetria raccolta da Stealthwatch, Flow Sensor offre ulteriore contesto della sicurezza per migliorare l'analisi di sicurezza di Stealthwatch. La modellazione comportamentale avanzata e il machine learning multilivello basato su cloud vengono applicati a questo set di dati per rilevare le minacce avanzate ed eseguire indagini più veloci.

Flow Sensor viene installato su una porta di mirroring o su un network tap e genera telemetria in base al traffico osservato. Il volume della telemetria generata dalla rete è determinata dalla capacità dei Flow Sensor implementati. Possono essere installati vari Flow Sensor. I Flow Sensor sono disponibili come appliance hardware o virtuali per monitorare gli ambienti delle macchine virtuali. Funziona anche in ambienti in cui una soluzione di monitoraggio overlay che richiede un contesto di sicurezza aggiuntivo si adatta meglio al modello operativo del reparto IT.

La tabella 3 elenca i principali vantaggi di Flow Sensor.

Tabella 3. Vantaggi principali di Flow Sensor

Vantaggio	Descrizione
Visibilità delle applicazioni di layer 7	Fornisce la visibilità effettiva sulle applicazioni di Layer 7 raccogliendo le informazioni sulle applicazioni insieme alla cattura dei pacchetti (PCAP) on-demand ad-hoc. Include funzioni dei dati come RTT (Round Trip Time), SRT (Server Response Time), ritrasmissioni.
Prestazioni e analisi a livello di pacchetto	Fornisce la visibilità effettiva sulle applicazioni di Layer 7 raccogliendo le informazioni sulle applicazioni insieme alla cattura dei pacchetti (PCAP) on-demand ad-hoc. Include funzioni dei dati come RTT (Round Trip Time), SRT (Server Response Time), ritrasmissioni.
Avvisi sulle anomalie di rete	Ulteriori dati telemetrici di Flow Sensor, come le informazioni sugli URL per il traffico Web e i dettagli dei flag TCP, consentono di generare avvisi con intelligence contestuale in modo che il personale di sicurezza possa intervenire rapidamente e mitigare i danni.
Riduzione dei costi	Migliora l'efficienza operativa e riduce i costi identificando e isolando la causa principale di un problema o di un incidente in pochi secondi.
Scelta dei metodi di consegna	È possibile ordinare la versione Appliance (Appliance Edition), un dispositivo scalabile adatto ad aziende di qualsiasi dimensione, oppure la Virtual Edition, progettata per svolgere la stessa funzione dell'appliance, ma in un ambiente VMware o KVM Hypervisor.

* Questi numeri vengono generati nei nostri ambienti di test, basandosi sui dati medi dei clienti.

Specifiche di Flow Sensor

- Stealthwatch Flow Sensor 1200 - Codice prodotto: ST-FS1200-K9
- Stealthwatch Flow Sensor 2200 - Codice prodotto: ST-FS2200-K9
- Stealthwatch Flow Sensor 3200 - Codice prodotto: ST-FS3200-K9
- Stealthwatch Flow Sensor 4200 - Codice prodotto: ST-FS4200-K9
- Stealthwatch Flow Sensor Virtual Edition - Codice prodotto: L-ST-FS-VE-K9

Nota: queste specifiche si applicano a Cisco Stealthwatch versione 6.9.1 e più recenti

UDP Director

UDP Director semplifica la raccolta e la distribuzione dei dati della rete e della sicurezza in tutta l'azienda. Aiuta a ridurre la potenza di elaborazione su router e switch di rete ricevendo informazioni fondamentali sulla rete e sulla sicurezza da più posizioni e quindi trasmettendole a un singolo flusso di dati a una o più destinazioni. La tabella 4 elenca i principali vantaggi di UDP Director.

Tabella 4. Vantaggi principali di UDP Director

Vantaggio	Descrizione
Riduce le interruzioni dell'operatività e del servizio non pianificate	UDP Director High Availability è disponibile sull'appliance UDP Director 2200.
Semplifica la sicurezza e il monitoraggio della rete	UDP Director aggrega e fornisce una singola destinazione standardizzata per le informazioni di NetFlow, sFlow, syslog e del protocollo SNMP (Simple Network Management Protocol). Le appliance UDP Director possono ricevere dati da qualsiasi applicazione UDP senza connessione e poi ritrasmetterli a destinazioni diverse, duplicando i dati se necessario.
Può dirigere i dati UDP da qualsiasi sorgente a qualsiasi destinazione	Riceve i dati da qualsiasi applicazione UDP senza connessione e poi li ritrasmette a destinazioni diverse, duplicando i dati se necessario.
Elimina la necessità di riconfigurare l'infrastruttura	Dirige i dati di log puntuali (NetFlow, sFlow, syslog, SNMP) a una singola destinazione senza la necessità di riconfigurare l'infrastruttura quando vengono aggiunti o rimossi nuovi strumenti.

Specifiche di UDP Director

- Stealthwatch UDP Director 2200 - Codice prodotto: ST-UDP2200-K9
- Cisco Stealthwatch UDP Director Virtual Edition - Codice prodotto: L-ST-UDP-VE-K9

Informazioni per l'ordinazione

La guida agli ordini del sistema Cisco Stealthwatch illustra chiaramente i modelli, i componenti e i tipi di licenza del sistema. Per effettuare un ordine, contattare il rappresentante Cisco di riferimento.

L'assistenza e il supporto

Sono disponibili vari programmi di servizi per il sistema Cisco Stealthwatch. Questi servizi consentono di proteggere gli investimenti nell'infrastruttura di rete, ottimizzarne le operazioni e prepararla per le nuove applicazioni che ne estendono l'intelligence e aumentano le capacità di crescita dell'azienda. Per ulteriori informazioni sui servizi professionali, vedere l'home page del supporto tecnico.

Cisco Capital

I finanziamenti Cisco Capital® possono essere utili per acquistare la tecnologia necessaria per conseguire i propri obiettivi e rimanere competitivi. Aiutiamo a ridurre le spese in conto capitale (CapEx), accelerare la crescita e ottimizzare gli investimenti e il ROI. I finanziamenti Cisco Capital offrono flessibilità nell'acquisto di hardware, software, servizi e apparecchiature integrative di terze parti. Ed è previsto un solo pagamento fisso. Cisco Capital è disponibile in oltre 100 paesi. Altri dettagli.

Per ulteriori informazioni

Per ulteriori informazioni su Cisco Stealthwatch, visita https://www.cisco.com/go/stealthwatch o contatta il rappresentante dell'account di Cisco Security per scoprire come l'azienda può ottenere visibilità in tutta la rete estesa partecipando a una prova gratuita di Stealthwatch Visibility Assessment.

Sede centrale Americhe
Cisco Systems Inc.
San Jose. CA (USA)

Sede centrale Asia e Pacifico
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito web Cisco all'indirizzo **www.cisco.com/go/offices**.

Stampato negli Stati Uniti C78-739398-03 04/18