Lenovo ThinkShield

Protezione avanzata e conformità NIS2 per le PMI

www.asacomputer.com

2024

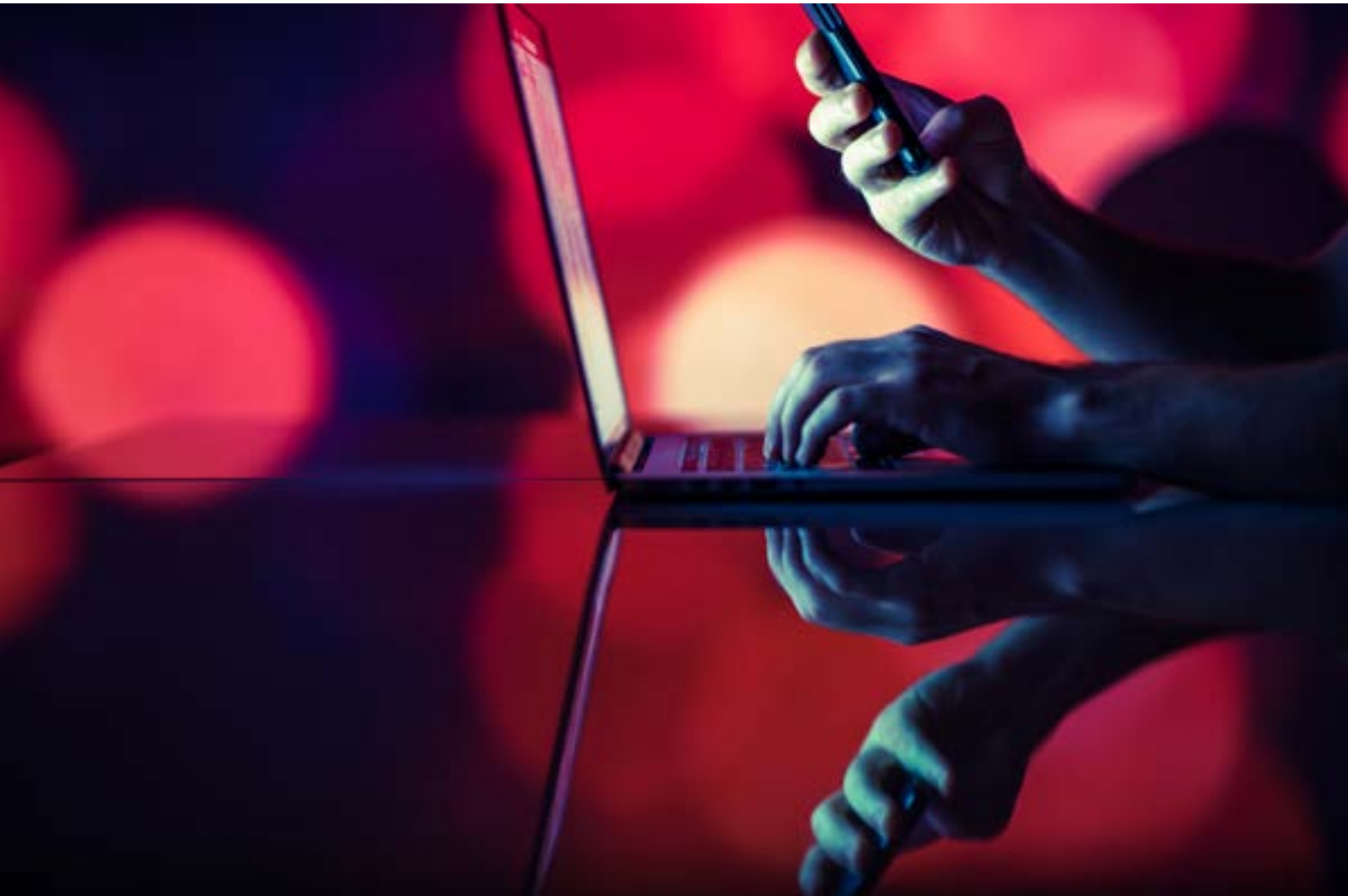
Contenuti

Introduzione

Nel contesto delle crescenti minacce informatiche e delle normative sempre più stringenti, la sicurezza informatica è diventata essenziale per ogni azienda.

Con l'introduzione della direttiva NIS2, che richiede alle aziende di garantire alti standard di sicurezza informatica e resilienza contro attacchi sempre più sofisticati, Lenovo ha sviluppato ThinkShield, una soluzione di sicurezza completa.

Questo white paper illustra come ThinkShield offra una protezione avanzata contro attacchi zero-day, ransomware, vulnerabilità firmware e altre minacce critiche, e come Lenovo si differenzi dalla concorrenza grazie a tecnologie esclusive come Sepio e Eclypsium.



Introduzione alla Direttiva NIS2

La direttiva NIS2 (Network and Information Security Directive) è stata creata dall'Unione Europea per rafforzare la sicurezza delle reti e delle informazioni, soprattutto nei settori critici e per le infrastrutture essenziali.

I 10 punti chiave della NIS2 includono:

1. Gestione del rischio di sicurezza informatica, per l'identificazione dei rischi e l'adozione di misure preventive.

2. Sicurezza delle catene di fornitura, che impone la verifica delle pratiche di sicurezza di tutti i fornitori.

3. Protezione contro attacchi informatici, che comporta la difesa contro ransomware e attacchi zero-day.

4. Incident Response, cioè capacità di rispondere tempestivamente agli incidenti di sicurezza.

5. Monitoraggio e audit, per la sorveglianza continua delle reti e dei sistemi.

6. Gestione delle vulnerabilità e aggiornamenti tempestivi per le vulnerabilità scoperte.

7. Conformità alle normative - rispetto delle leggi europee e locali in materia di sicurezza.

8. Collaborazione e condivisione delle informazioni - partenariati tra le aziende e le autorità per migliorare la sicurezza.

9. Protezione dei dati e privacy per una protezione rigorosa dei dati sensibili.

10. Piani di continuità operativa per garantire la continuità delle operazioni anche in caso di attacco.

Lenovo ThinkShield risponde direttamente a questi requisiti, garantendo conformità ai punti chiave della direttiva NIS2 attraverso soluzioni di sicurezza integrate, protezione continua e gestione del ciclo di vita dei dispositivi.

Lenovo ThinkShield e le soluzioni esclusive per la sicurezza

Una delle caratteristiche principali che differenziano Lenovo dalla concorrenza è l'integrazione di tecnologie esclusive come Sepio e Eclypsium, ma anche come Cigent, Bufferzone e Sentinel One, che offrono un livello di protezione unico nel mercato.

Sepio fornisce una soluzione unica nel suo genere che rileva e previene attacchi Man-in-the-Middle (MiTM) hardware. Questa tecnologia, esclusiva di Lenovo, monitora i componenti hardware in tempo reale, identificando qualsiasi dispositivo non autorizzato che potrebbe essere utilizzato per infiltrarsi nelle reti aziendali. Il vantaggio di Sepio è la sua capacità di rilevare minacce invisibili, come dispositivi di attacco collegati fisicamente o inseriti in modo subdolo nella supply chain.

Il firmware rappresenta uno degli aspetti più vulnerabili di un dispositivo. Lenovo ThinkShield, grazie alla collaborazione con Eclypsium, fornisce la Firmware Defense, una protezione esclusiva che rileva e previene vulnerabilità firmware e zero-day. Questo sistema non solo monitora costantemente il firmware alla ricerca di exploit, ma implementa anche patch e aggiornamenti di sicurezza in modo proattivo, proteggendo così i dispositivi anche dagli attacchi più sofisticati.

Cigent

Cigent rappresenta una soluzione esclusiva che protegge i dati direttamente sul disco, garantendo che nessun attacco possa accedere alle informazioni sensibili. Questa protezione è particolarmente cruciale in settori regolamentati e nelle aziende che gestiscono dati sensibili, offrendo un livello di sicurezza superiore rispetto alla concorrenza.

Bufferzone

Bufferzone affronta direttamente i rischi di phishing e download di malware da siti web infetti. Il software crea una "zona sicura" per ogni file o applicazione scaricata da fonti non verificate, garantendo che l'attacco non possa diffondersi oltre l'ambiente virtuale isolato. In questo modo, gli utenti possono navigare e interagire con i contenuti senza mettere in pericolo i sistemi aziendali principali.

SentinelOne

SentinelOne è una componente chiave del portafoglio di soluzioni di sicurezza Lenovo ThinkShield, integrata per fornire una protezione avanzata contro minacce moderne, in particolare attacchi mirati e sofisticati come quelli zero-day, ransomware e altre forme di malware evoluto. SentinelOne si distingue per la sua capacità di rilevare, rispondere e neutralizzare le minacce in tempo reale, utilizzando tecnologie di **Endpoint Detection and Response (EDR)** e **Extended Detection and Response (XDR)**, basate su intelligenza artificiale.

Queste tecnologie differenziano Lenovo dai concorrenti, che spesso non offrono una protezione hardware così profonda o una gestione proattiva delle vulnerabilità del firmware. La combinazione di Sepio e Eclypsium consente a Lenovo di fornire un livello di sicurezza che non solo previene gli attacchi, ma li identifica prima che possano causare danni.

Protezione contro attacchi Zero-Day e Ransomware

Gli attacchi zero-day e il ransomware sono infatti due delle minacce più pericolose nel panorama attuale della cybersecurity. Lenovo ThinkShield ha integrato soluzioni avanzate per affrontare entrambe le minacce:

Attacchi Zero-Day

Gli attacchi zero-day sfruttano falle sconosciute, ed è qui che entra in gioco la protezione ThinkShield Firmware Defense. Lenovo garantisce che ogni dispositivo sia dotato di un BIOS sicuro e protetto, con monitoraggio continuo per rilevare anomalie. In combinazione con Eclypsium, Lenovo offre una protezione proattiva, correggendo le vulnerabilità firmware prima che possano essere sfruttate.

Ransomware Rollback e Sandboxing

Per contrastare i ransomware, Lenovo ThinkShield ha sviluppato il sistema Ransomware Rollback, che permette di annullare le modifiche apportate dai ransomware e ripristinare i file e i sistemi a uno stato precedente all'attacco. Inoltre, la tecnologia di sandboxing isola i file sospetti in un ambiente sicuro, consentendo all'IT di testare senza mettere a rischio l'intero sistema.

Gestione della sicurezza su ampia scala

Una delle sfide più complesse per le aziende è la gestione della sicurezza su una grande flotta di dispositivi. Lenovo ThinkShield fornisce soluzioni integrate che centralizzano e semplificano la gestione della sicurezza:

Patch e aggiornamenti automatici

ThinkShield automatizza il processo di aggiornamento dei dispositivi, garantendo che tutti i sistemi siano protetti con le ultime patch di sicurezza, riducendo la vulnerabilità agli attacchi zero-day e alle minacce emergenti.

Gestione remota e visibilità completa

Lenovo Device Manager consente la gestione remota dell'intera flotta di dispositivi, offrendo visibilità in tempo reale su stato di sicurezza, aggiornamenti e conformità.

Geofencing e wipe remoto

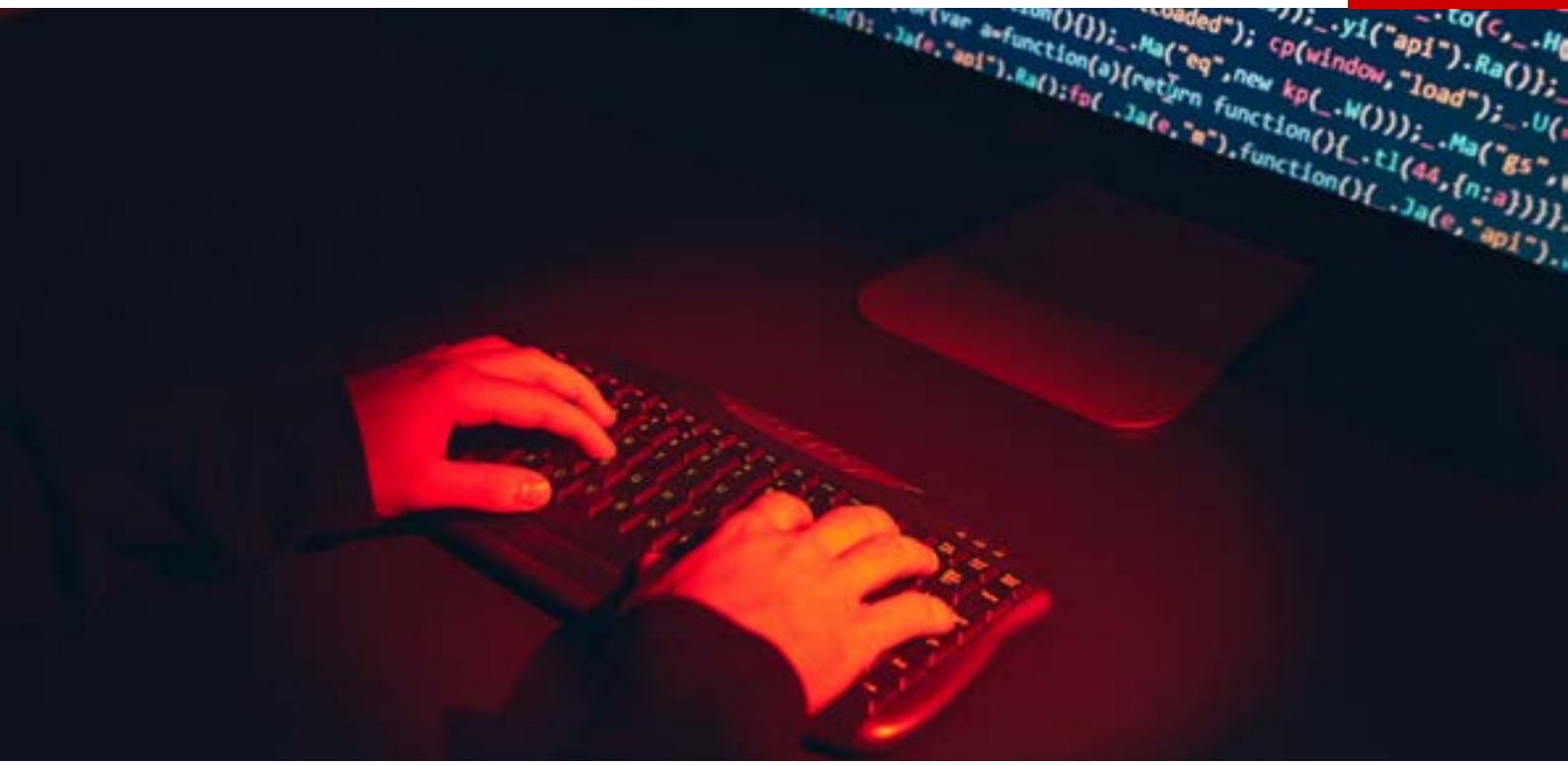
ThinkShield permette anche di impostare geofencing per limitare l'accesso ai dati aziendali a specifiche aree geografiche. In caso di smarrimento o furto del dispositivo, è possibile eseguire una cancellazione remota per proteggere i dati sensibili.

Come Lenovo si allinea ai 10 punti della NIS2

Da quanto sopra descritto, risulta evidente come Lenovo ThinkShield sia perfettamente allineato ai requisiti di conformità della NIS2, offrendo soluzioni che coprono tutte le aree chiave della normativa sopra riportate.

Lenovo ThinkShield si dimostra infatti perfettamente in linea con i requisiti di conformità della direttiva NIS2, offrendo soluzioni complete che coprono tutte le aree critiche della normativa. ThinkShield fornisce una protezione multilivello che permette alle aziende di identificare e mitigare i rischi in tempo reale, prevenendo attacchi alla catena di fornitura grazie all'integrazione di Sepio, che monitora l'hardware e blocca possibili intrusioni.

Le sue difese proattive contro attacchi zero-day e ransomware, insieme alla protezione del firmware, sono perfettamente conformi ai requisiti NIS2. ThinkShield facilita la gestione delle vulnerabilità automatizzando gli aggiornamenti di sicurezza, riducendo al minimo i tempi di esposizione. Inoltre, gli strumenti di monitoraggio continuo e di risposta agli incidenti consentono di minimizzare i tempi di inattività, garantendo operazioni sicure e ininterrotte.



La piattaforma ThinkShield centralizza la gestione della sicurezza, monitorando in tempo reale le operazioni aziendali e garantendo la conformità normativa sia a livello locale che europeo. Oltre alla protezione dei dati tramite crittografia avanzata, ThinkShield promuove la collaborazione tra i team di sicurezza e le autorità, facilitando lo scambio di informazioni su minacce e incidenti.

Infine, con strumenti per la resilienza operativa, ThinkShield assicura la continuità delle attività aziendali anche in caso di attacco, proteggendo le infrastrutture critiche e soddisfacendo tutti i requisiti imposti dalla NIS2.

In sintesi, Lenovo ThinkShield è la soluzione di sicurezza più avanzata e completa per le aziende che desiderano conformarsi alla direttiva NIS2 e proteggere i propri dispositivi e dati contro le minacce informatiche più sofisticate. Grazie a tecnologie esclusive come Sepio e Eclypsium, Bufferzone e Cigent, Lenovo offre una protezione che va oltre i tradizionali standard di mercato, garantendo una sicurezza completa e un vantaggio competitivo. La gestione centralizzata, la protezione hardware e firmware avanzata e l'allineamento alla NIS2 rendono Lenovo ThinkShield una scelta strategica per le aziende che vogliono affrontare con sicurezza le sfide del futuro digitale.

Contattaci oggi per scoprire come Lenovo ThinkShield può proteggere la tua azienda.

Corso Vercelli, 89
28100 Novara

+39 0321 466664

commerciale@asacomputer.com

WWW.ASACOMPUTER.COM