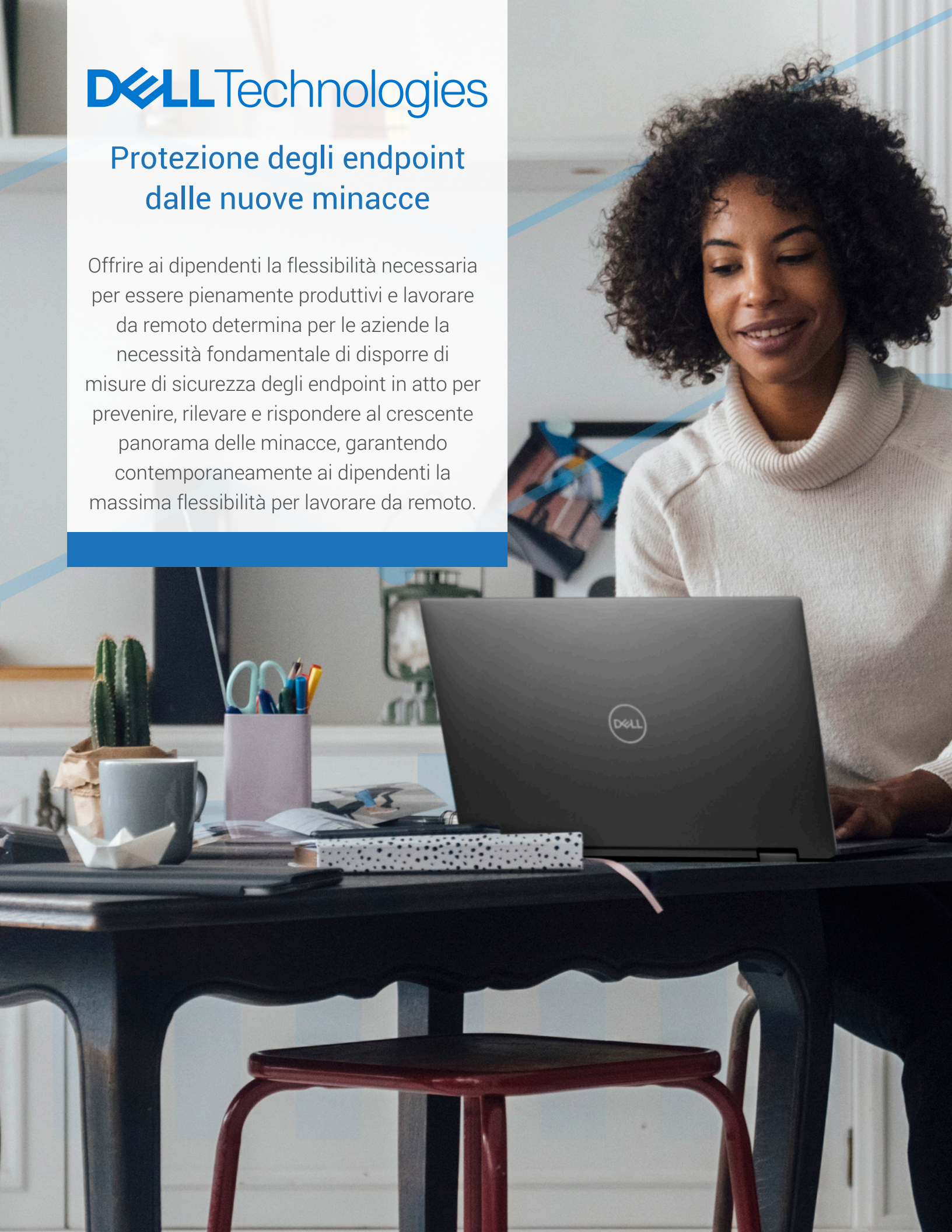
DELL Technologies

# Protezione degli endpoint dalle nuove minacce

Offrire ai dipendenti la flessibilità necessaria per essere pienamente produttivi e lavorare da remoto determina per le aziende la necessità fondamentale di disporre di misure di sicurezza degli endpoint in atto per prevenire, rilevare e rispondere al crescente panorama delle minacce, garantendo contemporaneamente ai dipendenti la massima flessibilità per lavorare da remoto.



Mentre i responsabili IT si preparano con lungimiranza alla fine della pandemia di COVID-19, molti stanno pianificando una nuova normalità con un numero di lavoratori remoti più alto che mai. Anche se molte aziende e i loro dipendenti trarranno vantaggio da una maggiore produttività e da uno stile di lavoro più flessibile, c'è un prezzo da pagare in termini di protezione. Il picco del lavoro da remoto a causa del COVID-19 ha reso più difficile la difesa degli endpoint: l'84% dei responsabili IT afferma che la protezione di una forza lavoro remota è più difficile.[1] Una delle possibili spiegazioni è l'aumento del 148% degli attacchi ransomware alle organizzazioni globali nel pieno dell'epidemia pandemica.[2] Ciò che rende questa statistica deludente è che le persone che lavorano da casa si affidano alle e-mail come mezzo principale di comunicazione aziendale, il che ha portato a un aumento del 350% negli attacchi di phishing.[3]

## Tendenze di cyber-sicurezza in corso

L'improvviso passaggio al lavoro da remoto avviene in un contesto in cui si verificano molte problematiche e preoccupazioni per la cyber-sicurezza, che mettono a dura prova la competenza dei professionisti della sicurezza informatica. Questi comprendono:

1. Attacchi a livello di BIOS: vulnerabilità sfruttate in hardware o chip. Quando il BIOS viene compromesso, spesso l'hacker rimane nascosto durante l'accesso alla rete e ai dati del dispositivo. Il 63% delle aziende ha affrontato situazioni di rischio o una violazione dei dati a causa di tali attacchi.[4]
2. Minacce persistenti avanzate (APT, Advanced Persistent Threats): minacce sofisticate che spesso si nascondono in silenzio raccogliendo informazioni su comportamenti come preludio al furto di dati importanti. Le vittime potrebbero non rendersi conto dell'attacco silenzioso per molto tempo, 108 giorni in media[5].
3. Malware basato su file e senza file
   - Malware basato su file: in genere i tipi di file con estensioni familiari, ad esempio .DOCX e .PDF, utilizzati dai dipendenti per svolgere il loro lavoro. Quando un utente apre il file, viene eseguito il codice dannoso incorporato.
   - Malware senza file: in genere un programma legittimo che infetta un computer. Quando l'utente avvia un programma da un'e-mail, il malware senza file infetta il computer e potenzialmente la rete, eludendo con successo molte tecnologie di sicurezza.
4. Attacchi basati sullo stato nazionale, tipicamente provenienti da Cina, Corea del Nord, Russia e Iran. Con la competenza tecnologica e il supporto finanziario di tali Stati nazionali, spesso gli attacchi sono sofisticati e dannosi. Tuttavia, molti di questi attacchi sfruttano i sistemi che non dispongono degli aggiornamenti e delle patch più recenti. L'unità CISA dell'FBI invia regolarmente avvertenze sulla sicurezza.

L'improvviso passaggio al lavoro da remoto avviene in un contesto in cui si verificano molte problematiche e preoccupazioni per la cyber-sicurezza, che mettono a dura prova la competenza dei professionisti della sicurezza informatica.

1. "The State of DLP 2020", Tessian.
2. Blog di VMware Carbon Black, Patrick Upatham e Jim treinen, 15 aprile 2020.
3. Report di Google, come citato in PCMAG.com, 30 marzo 2020.
4. "Match Present-Day Security Threats with BIOS-Level Control", documento di Forrester Consulting sulla leadership di pensiero commissionato da Dell, giugno 2019.
5. The 2018 U.S. State of Cybercrime Survey.

5. Attacchi basati sul cloud: in aumento via via che le applicazioni per la produttività e la collaborazione basate sul cloud sostituiscono le applicazioni desktop. Con l'utilizzo di oltre 2.400 servizi cloud in un'azienda media, il 93% delle organizzazioni è moderatamente o estremamente preoccupato per la sicurezza del cloud.[6] La protezione deve includere la prevenzione della perdita dei dati (DLP) e la protezione dalle minacce nel cloud. Inoltre, l'autenticazione dell'utente deve essere protetta contro lo spoofing e i dati devono essere crittografati da e verso il cloud.
6. Normative in materia di conformità volte a proteggere le informazioni di identificazione personale (PII). Per evitare che le informazioni personali finiscano nelle mani sbagliate e in ultima analisi utilizzate per il furto di identità, alcuni settori hanno adottato rigorose normative con sanzioni rigide. Tra cui HIPAA nell'assistenza sanitaria, PCI-DSS nel settore dei servizi finanziari e della vendita al dettaglio e GDPR per le aziende che operano con i cittadini europei.
7. Rischio intollerabile: risultato di 6 mila miliardi di dollari di perdite per criminalità informatica previsto nel 2021, un aumento da 3 mila miliardi di dollari nel 2015. Le perdite sono dovute a danni e distruzione di dati, furto di fondi, perdita di produttività, furto di proprietà intellettuale, furto di dati personali e finanziari, interruzioni post-attacco, danni di reputazione e altro ancora, secondo Cybersecurity Ventures.[7]

## Ripensare la sicurezza degli endpoint

**Sicurezza degli endpoint: parte della sicurezza aziendale**
Di fronte a un numero di lavoratori remoti senza precedenti, molti dei quali devono gestire i dati sensibili per svolgere il proprio lavoro, i responsabili IT devono valutare lo stato attuale della sicurezza degli endpoint nelle rispettive organizzazioni. Tuttavia, anziché considerare la sicurezza degli endpoint singolarmente, è opportuno considerarla come parte integrante della sicurezza aziendale per implementare la protezione in modo approfondito e guardare oltre gli endpoint per includere lo storage, le reti e i servizi basati sul cloud. Un approccio olistico alla creazione di "dispositivi affidabili" all'interno dell'azienda deve tenere conto di questi fattori:

**Sicurezza integrata**
Anziché affidarsi esclusivamente al software per la protezione degli endpoint, un approccio completo richiede l'utilizzo di dispositivi affidabili: dispositivi di end-user computing con sicurezza integrata al proprio interno. Tali dispositivi proteggono le informazioni personali e svolgono un ruolo importante in materia di conformità alle normative, in caso di smarrimento o furto di un dispositivo. I dispositivi degli utenti finali devono altresì includere tecnologie per lo schermo per la privacy, che limitano la possibilità per i colleghi e i visitatori dell'ufficio di visualizzare le informazioni riservate sullo schermo del computer.

I responsabili IT dovrebbero prendere in considerazione la sicurezza degli endpoint come parte integrante della sicurezza aziendale.

6. Cybersecurity Insider Cloud Security Reports, 2018, 2019.
7. Cybersecurity Ventures, 2020.

**Protezione al di sopra e al di sotto del sistema operativo**
**Al di sopra del sistema operativo.** L'IT ha bisogno di visibilità, monitoraggio e sicurezza dei dati, nonché di prevenzione, rilevamento e correzione delle minacce. La crittografia su dispositivi è inoltre molto importante per soddisfare i requisiti di conformità, tuttavia, non dovrebbe rallentare le prestazioni per ridurre la produttività degli utenti.

**Al di sotto del sistema operativo.** Richiede la protezione del BIOS e l'autenticazione dei chip a causa della frequenza degli attacchi al firmware e all'hardware. Un BIOS compromesso può fornire agli utenti malintenzionati l'accesso a tutti i dati su un endpoint, incluse le credenziali, per consentire agli autori di attacchi di spostarsi all'interno della rete di un'organizzazione e di attaccare l'infrastruttura di IT più ampia.

**AI e ML**

Oggi, con gli attacchi che diventano sempre più sofisticati, l'utilizzo dell'intelligenza artificiale e dell'apprendimento automatico per il rilevamento e la correzione dei problemi sono essenziali per la protezione degli endpoint. Osservando i modelli comportamentali, gli algoritmi di intelligenza artificiale e di apprendimento automatico sono in grado di rilevare attività anomale che potrebbero indicare e prevenire una violazione.

**Supply chain sicura**

Nel processo di produzione, è possibile che gli hacker introducano componenti compromessi per consentire un attacco backdoor. Una volta incorporati in un prodotto fabbricato, tali componenti potrebbero consentire una violazione essere estremamente dannosa e difficile da rilevare. È quindi fondamentale che i fornitori e i produttori implementino rigorose misure di sicurezza in punti critici lungo la supply chain.

## Dispositivi affidabili Dell

Dell crea la sicurezza in ogni PC con queste tecnologie:

**SafeBIOS con indicatori di attacco (IoA) BIOS:** fornisce visibilità alle modifiche del BIOS per impedire manomissioni. Dell mantiene un'immagine protetta dall'host per verificare l'integrità del BIOS. SafeBIOS è ora integrato con VMware Carbon Black Audit and Remediation, che aumenta la visibilità degli attacchi tramite creazione di report automatizzati e consente l'accesso remoto per correggere il problema del danneggiamento del BIOS.

**SafeID:** fornisce l'autenticazione basata su chip. Le credenziali degli utenti finali vengono verificate utilizzando un chip di sicurezza dedicato, anziché fare affidamento su un software meno sicuro.

**SafeScreen:** protegge gli schermi che potrebbero mostrare informazioni sensibili a colleghi, visitatori, addetti alla manutenzione o ad altre persone non autorizzate.

**SafeGuard and Response.** Con tecnologia VMware Carbon Black e Secureworks Technologies, il portafoglio Dell include:

**VMware Carbon Black:** una piattaforma di protezione degli endpoint nativa del cloud che combina il consolidamento del sistema intelligente e la prevenzione di comportamenti necessaria per tenere a bada le minacce emergenti, utilizzando un unico agent leggero e una console di facile utilizzo.

I dispositivi affidabili proteggono le informazioni personali e svolgono un ruolo importante in materia di conformità alle normative, in caso di smarrimento o furto di un dispositivo.

**Servizi gestiti Secureworks:** raccolgono e correlano la telemetria da cloud, rete ed endpoint per individuare le minacce all'interno dell'azienda. Fornendo una risposta agli incidenti leader del settore, i servizi gestiti Secureworks sono integrati con la piattaforma VMware Carbon Black e molte altre piattaforme.

**SafeData.** La collaborazione, sempre un segno distintivo delle organizzazioni di successo, assume un'importanza maggiore nell'era del lavoro da remoto intensificato. La collaborazione della forza lavoro di oggi richiede la sicurezza dei dati sia sul dispositivo sia nel cloud, che non rallenta l'utente finale. Dell collabora con Netskope e Absolute per assicurare la sicurezza degli endpoint olistici.

**Netskope.** Adottando un approccio incentrato sui dati, la tecnologia Netskope protegge i dati creati ed esposti nel cloud. Grazie alla visibilità in tempo reale, all'accesso al cloud, al monitoraggio e alla prevenzione dalla perdita dei dati, Netskope ridefinisce il cloud, la rete e la sicurezza dei dati. I team hanno il giusto equilibrio tra protezione e velocità, consentendo loro di proteggere il percorso di Digital Transformation dell'organizzazione.

**Absolute.** Dell integra la tecnologia Absolute nel firmware di ogni dispositivo, garantendo a ogni endpoint un link di self-healing al dashboard Absolute basato sul cloud. In questo modo, i manager possono monitorare, gestire e proteggere gli endpoint e i dati su di essi, anche quando sono fuori dalla rete. Tecnologia Absolute:

- Individua e gestisce i dispositivi.
- Fornisce la persistenza di VPN e software di sicurezza.
- Implementa una soluzione air-gap per consentire il ripristino dagli attacchi
- Include soluzioni per la protezione dei dati multi-cloud che possono essere definite dal software o basate su appliance.

La collaborazione della forza lavoro di oggi richiede la sicurezza dei dati sia sul dispositivo sia nel cloud, che non rallenta l'utente finale.

## Conclusioni

Il picco dei lavori da remoto a causa della pandemia di COVID-19 aumenta i pericoli in un panorama di cyber-sicurezza già pieno di minacce. È necessario un nuovo approccio olistico alla protezione degli endpoint. Ripensare la protezione degli endpoint ha inizio con dispositivi affidabili protetti sia al di sopra sia al di sotto del sistema operativo. Tale strategia va anche oltre gli endpoint stessi per intraprendere una visione aziendale della sicurezza informatica che include server, reti, servizi basati sul cloud e conformità alle normative. Il portafoglio di dispositivi affidabili Dell incarna un approccio così completo. La protezione degli endpoint di Dell consente all'azienda di includere soluzioni per la protezione dei dati multi-cloud, che possono essere fornite come soluzioni definite dal software e/o basate su appliance. In particolare, i dispositivi affidabili Dell consentono agli utenti di mantenere una produttività elevata, sconfiggendo gli attacchi sempre più sofisticati nel nuovo paradigma del lavoro da remoto.

**Per ulteriori informazioni, consultare:**
**https://www.delltechnologies.com/it-it/endpoint-security/index.htm**