Acronis Protected Workspace: proteggere l'anello più debole della catena di sicurezza

Laptop, desktop e workstation rappresentano al tempo stesso degli strumenti imprescindibili e un enorme rischio per la sicurezza. I dipendenti li utilizzano ovunque, e ciò li espone a una vasta gamma di minacce.

Per i Managed Service Provider (MSP), i dispositivi sono le risorse più importanti e al tempo stesso le più vulnerabili. Proteggerli non è affatto facile, perché gli MSP si avvalgono di numerosi strumenti diversi, che, se non sono integrati in modo nativo, non funzionano in sinergia tra loro e possono generare falle nella copertura.

La gestione di più strumenti comporta inoltre l'utilizzo di interfacce diverse, il che aumenta la complessità, introduce nuovi rischi e richiede spesso competenze specialistiche. Riepilogando, le infrastrutture di sicurezza degli ambienti di lavoro, quando assemblate con strumenti eterogenei, aumentano i costi operativi, generano inefficienze e riducono la protezione complessiva.

Infine, a rendere ogni giornata imprevedibile contribuisce l'AI, sfruttata della criminalità informatica per creare infinite varianti delle minacce. La posta in gioco è alta: gli attacchi riusciti comportano interruzioni operative, perdita di produttività e danni alla reputazione sia per gli MSP che per i loro clienti, senza contare i problemi di conformità che investono molti settori.

Cyber Security, protezione dati e gestione degli endpoint nativamente integrate per gli ambienti di lavoro

Le sfide aziendali per la protezione degli ambienti di lavoro per gli MSP

Molte aziende non dispongono delle risorse necessarie a gestire la sicurezza degli ambienti di lavoro e si rivolgono agli MSP per ottenere assistenza. Ai service provider viene delegato il compito di proteggere ogni laptop o desktop, ovunque si trovi, in modo da salvaguardare i dati senza compromettere la produttività.

Il ritmo e la natura globale delle attività aziendali rendono questo compito arduo per i service provider. Il problema è in parte dovuto alla vastità degli ambienti. Centinaia o migliaia di dispositivi costituiscono un'enorme superficie di attacco che gli MSP devono proteggere. Un singolo endpoint compromesso può originare un attacco informatico in grado di interferire con l'operatività del cliente.

I clienti hanno spesso dipendenti che utilizzano dispositivi da varie ubicazioni, inviando dati in tutto il mondo. Il lavoro a distanza è un ulteriore fattore nella sfida per la protezione degli ambienti di lavoro. La mobilità dei dispositivi, le operazioni globali e l'aspettativa di una risposta sempre rapida espongono i dispositivi dei dipendenti al rischio di attacchi informatici. In settori come quello sanitario e finanziario, ambienti di lavoro poco protetti possono mettere a rischio la conformità alle normative.

La sfida della sicurezza degli ambienti di lavoro per gli MSP

La protezione degli spazi di lavoro è particolarmente impegnativa per gli MSP, perché gli strumenti di Cyber Security destinati ai dispositivi non garantiscono l'efficienza necessaria ai service provider. La frammentazione degli strumenti, come l'utilizzo dell'antivirus di un'applicazione, del backup di un'altra e del sistema di monitoraggio e gestione remoti (RMM) di un'altra ancora, rendono la protezione dell'ambiente di lavoro costosa e soggetta a errori.

Ogni elemento che compone la protezione richiede un'app e una configurazione univoca, e il numero di combinazioni tra dispositivi diventa praticamente illimitato. Gli MSP devono avere personale a sufficienza per gestirli tutti. Devono assumere più tecnici o dedicare tempo alla loro formazione per le diverse applicazioni disconnesse e sperare che non commettano errori.

Tempi di risposta lenti, errori e stress dei tecnici sono le conseguenze della gestione di diversi strumenti con più console. In più, resta il rischio delle integrazioni non funzionanti che possono creare enormi falle nella sicurezza.

Non essendo mai completamente "spenti", gli ambienti di lavoro sono un bersaglio costante degli attacchi informatici. Inoltre, i dipendenti dei clienti spesso si fidano troppo dei propri dispositivi, generando un ulteriore livello di vulnerabilità. Agli MSP è indispensabile una soluzione per la protezione degli ambienti di lavoro che offra funzionalità di sicurezza complete ma che sia, al contempo, anche facile da gestire.

"In molte aziende, l'infrastruttura di sicurezza frammentaria dell'ambiente di lavoro ha comportato un aumento della complessità e dei costi operativi e una riduzione dell'efficacia della sicurezza."

Gartner, 2025 Strategic Roadmap for Workspace Security

Acronis Protected Workspace offre servizi su misura per gli MSP

Acronis Protected Workspace presenta una serie di servizi integrati in modo nativo che consentono agli MSP di fornire protezione ai dispositivi dei clienti con rischi minimi e la massima efficienza. Sono disponibili con tariffazione a workload o a gigabyte e includono:

Servizi in Acronis Protected Workspace

Acronis Backup per Workstation	Archivia e protegge i dati per i laptop, i desktop e le workstation dei clienti.
Acronis Advanced Backup per Workstation	Estende le funzionalità di backup in cloud per proteggere in modo proattivo i dati degli ambienti di lavoro di oltre 20 tipi di workload, evitando ogni interruzione operativa.
Acronis Endpoint Detection and Response (EDR)	Monitora attivamente gli endpoint, bloccando gli attacchi prima che possano causare danni e attivando il ripristino con un solo clic.
Acronis Extended Detection and Response (XDR)	Fornisce una protezione attiva e totale, per prevenire, rilevare, analizzare, rispondere e avviare il ripristino dopo gli incidenti.
Acronis Remote Monitoring and Management (RMM)	Servizi di amministrazione e monitoraggio di altissima qualità, con un approccio incentrato sulla sicurezza. Combina automazione totale, accelerazione con AI e ML e un efficiente motore di scripting. Individua e protegge gli ambienti di lavoro connessi con Device Sense™.
Acronis Data Loss Prevention (DLP)	Impedisce la fuga di dati dagli endpoint senza richiedere competenze complesse in termini di installazione o privacy.
Acronis Active Protection	Protegge attivamente tutti i dati presenti sui sistemi dei clienti, inclusi documenti, file multimediali, programmi e altro ancora.
Anti-malware Acronis	Protegge in modo proattivo e in tempo reale i sistemi dei clienti da attacchi informatici avanzati sfruttando l'euristica comportamentale e statica basata sull'intelligenza artificiale e tecnologie antivirus, anti-malware, anti-ransomware.

Gli MSP hanno inoltre la possibilità di scegliere pacchetti basati su soluzioni, tra cui:

Backup delle workstation	Sicurezza degli endpoint e RMM	Protezione Ultimate
Acronis Backup per workstation con storage da 300 GB incluso	Acronis Active Protection	Pacchetto Security + RMM
	Anti-malware Acronis	Pacchetto Backup + Cloud Storage
	Acronis EDR	Acronis Advanced Backup
	Acronis XDR	Acronis DLP
	Acronis RMM	

Protezione dell'ambiente di lavoro integrata in modo nativo

Agli MSP è necessario un approccio unificato, efficiente e redditizio per la protezione, la gestione e il ripristino degli ambienti di lavoro. Acronis Protected Workspace combina tutti i servizi indispensabili agli MSP in un'unica soluzione nativamente integrata: un agente, una licenza e una console per gestire ogni aspetto della protezione. È un'idea semplice ma efficiente, che consente ai tecnici di gestire più ambienti di lavoro migliorando la sicurezza.

Acronis Protected Workspace offre inoltre:

- **Integrazione nativa** di sicurezza degli endpoint, RMM e backup in una sola console.
- **Protezione totale:** anti-malware con AI, rilevamento e risposta degli endpoint (EDR), rilevamento e risposta estesi (XDR), rilevamento del ransomware e analisi comportamentale in linea con i principi del NIST Cybersecurity Framework.
- **Efficienza operativa:** risoluzione più rapida dei ticket, servizio clienti migliorato, costi di formazione ridotti.
- **Flessibilità:** modelli di licensing pensati per gli MSP, con la possibilità di creare pacchetti di protezione personalizzati.

"Acronis è la nostra piattaforma base e copre ogni aspetto. L'efficienza che offre è insuperabile, fa risparmiare tempo, riduce i costi e minimizza le attività di formazione. La presenza di un'unica console rende la gestione dell'intero stack semplice e lineare".

– Joshua Aaronson, co-fondatore, Panda Technology

Acronis Protected Workspace offre agli MSP tutto ciò di cui hanno bisogno per proteggere i dispositivi

Acronis Protected Workspace permette agli MSP di superare gli ostacoli della protezione di laptop, desktop e workstation senza dover gestire applicazioni di sicurezza eterogenee. I service provider possono distinguersi dai competitor offrendo protezione migliore, tempi di risposta più rapidi e un servizio clienti superiore.

Guarda Acronis Protected Workspace in azione CONTATTACI

Acronis

Maggiori informazioni su www.acronis.com