DDRop, un interposer da 159 dollari rimette in discussione le garanzie del confidential computing

Un circuito stampato che costa meno di duecento dollari, inserito per pochi minuti fra processore e memoria, basta a far leggere alla CPU dati vecchi come se fossero attuali. DDRop sfrutta questo difetto. La ricerca è stata divulgata il 14 settembre 2026 da nove ricercatori di KU Leuven, ETH Zurigo, Durham University e Google. Intel e AMD hanno riconosciuto i risultati, ma hanno risposto che gli attacchi fisici alla memoria restano fuori dal proprio modello di minaccia.

Quella risposta pesa più di quanto sembri. Il confidential computing viene venduto come la tecnologia che protegge i dati anche dal fornitore di infrastruttura. Se gli scenari esclusi dal modello di minaccia sono gli stessi che una valutazione sui trasferimenti di dati deve esaminare, il problema smette di essere solo tecnico.

Che cosa è stato pubblicato

Lo studio si intitola «DDRop: Active Memory Interposer Attacks on Confidential VMs by Dropping DDR5 Writes» e sarà presentato alla conferenza ACM CCS 2026, in programma all’Aia dal 15 al 19 novembre. Gli autori hanno pubblicato il sito divulgativo ddropattack.eu. Hanno inoltre rilasciato a sorgente aperto schemi, disegni della scheda, firmware del microcontrollore e codice degli attacchi sul repository GitHub del progetto.

Gli attacchi funzionano su tre tecnologie: Intel TDX, Intel Scalable SGX e AMD SEV-SNP. La cronaca internazionale ha dato

risalto alle prime due. La terza risulta colpita allo stesso modo, come indicano sia l’abstract sia la tabella riassuntiva dello studio.

Il difetto: la cifratura protegge il contenuto, non l’attualità

Le tre tecnologie cifrano la memoria per proteggere i carichi di lavoro dall’ipervisore e dall’operatore del centro dati. Per reggere quantità di memoria grandi, però, rinunciano a una garanzia: la freschezza crittografica.

Freschezza significa poter stabilire se il valore letto da un indirizzo sia davvero l’ultimo che vi è stato scritto. Senza quella garanzia il processore può confermare che la memoria è cifrata, non che è attuale. Un dato vecchio si decifra perfettamente.

Da qui nasce l’attacco. Se una scrittura non arriva al modulo di memoria, al suo posto resta il contenuto precedente. Se quel contenuto è stato collocato dall’attaccante, il motore di cifratura lo decifra senza rilevare alcuna anomalia.

Le due piattaforme colpite usano schemi diversi ma condividono il limite. Intel TDX cifra con AES in modalità XTS e chiavi assegnate per dominio. AMD SEV-SNP usa AES in modalità XEX con chiavi per ospite e, scrivono i ricercatori, non prevede né integrità crittografica né freschezza.

TDX offre in via opzionale una modalità di integrità crittografica, che aggiunge a ogni linea di cache un codice di autenticazione da 28 bit. Intel lo descrive come derivato da SHA-3 e avverte che il suo inserimento riduce la copertura dei bit di correzione d’errore. Neppure quella modalità, però, introduce la freschezza.

Come funziona l’interposer

Un interposer è una scheda che si frappone fisicamente fra il processore e il modulo di memoria, e che può osservare o alterare i segnali che li collegano. Quelli già noti per DDR5 erano ingombranti: richiedevano analizzatori logici e imponevano di abbassare la frequenza del bus, un intervento che un controllo all’avvio potrebbe individuare.

L’interposer di DDRop è invece una scheda compatta di interruttori analogici. Lavora alla frequenza nativa della memoria e si installa in pochi minuti.

Il meccanismo sfrutta il controllo di parità del bus comandi. I moduli di memoria usati nei server montano un componente che verifica la parità di ogni comando in arrivo. Quando trova un errore scarta il comando e lo segnala alla CPU su una linea di allerta, che ne provoca il reinvio.

L’interposer forza l’errore di parità e allo stesso tempo scollega la linea di allerta. Il modulo scarta la scrittura, il processore non riceve alcuna segnalazione, e la scrittura sparisce senza lasciare traccia.

La distinta base pubblicata dagli autori indica 159 dollari per un singolo sistema, calcolati su una produzione di dieci unità e al netto di ricerca, sviluppo e montaggio. Lo studio dichiara un costo complessivo inferiore a 200 dollari. Per confronto, gli stessi autori ricordano che un attacco passivo del 2020 richiedeva strumentazione da circa 170.000 dollari.

Che cosa ottiene l’attaccante su Intel TDX

Su TDX l’attacco colpisce le tabelle delle pagine sicure. Sono la struttura con cui il modulo TDX traduce gli indirizzi di una macchina virtuale protetta, e il modulo le gestisce in via

esclusiva proprio per impedire all’ipervisore di manometterle.

Quando l’ipervisore chiede una nuova pagina di tabella, il modulo TDX la inizializza scrivendo voci vuote. L’interposer scarta quelle scritture. Al loro posto resta un testo cifrato che l’attaccante ha collocato in precedenza e che si decifra in voci di tabella malevole. Il meccanismo è deterministico e riesce a ogni tentativo.

Da lì derivano due casi di studio verificati sulla piattaforma di prova.

Nel primo, l’attaccante corrompe gli attributi della struttura che controlla una macchina virtuale vittima, con l’obiettivo di attivarne il bit di debug. Non può però scegliere il risultato, perché il testo cifrato che inserisce è stato prodotto con un’altra chiave e si decifra in valori imprevedibili. Ogni tentativo ha quindi una probabilità del cinquanta per cento di riuscita, e va ripetuto finché il bit non risulta attivo.

A quel punto l’ipervisore legge la memoria in chiaro della vittima attraverso l’interfaccia di debug, poi ripristina il testo cifrato originale. I ricercatori verificano che, dopo il ripristino, il rapporto di attestazione della vittima risulta invariato. Dall’esterno non si vede nulla.

Nel secondo caso l’attaccante avvia una propria macchina virtuale con il codice che preferisce, poi ne riscrive la misura di avvio sostituendola con quella del carico di lavoro legittimo. Alla richiesta di attestazione il modulo TDX restituisce un rapporto firmato che contiene la misura falsificata.

È un punto da leggere con attenzione. La falsificazione riguarda l’attestazione della macchina dell’attaccante, non quella della vittima. L’effetto pratico resta grave, perché un verificatore remoto accetta come attendibile un ambiente che non lo è.

Su AMD SEV-SNP e su Scalable SGX

Su SEV-SNP i ricercatori sfruttano l'interfaccia che consente di spostare le pagine di memoria di un ospite. È esposta all'ipervisore, che il modello di sicurezza considera non attendibile.

Dopo uno spostamento la posizione di origine non viene azzerata, e questo vale sia per il processore sicuro AMD sia per il modulo TDX. Combinando uno spostamento preparatorio e un secondo spostamento con le scritture soppresse, l'attaccante fa sì che una pagina della vittima erediti il contenuto in chiaro di un'altra pagina della stessa vittima.

Sulla piattaforma di prova AMD la copia riguarda metà delle linee di cache della pagina bersaglio, per come la memoria è distribuita fra i canali.

Su Scalable SGX i ricercatori dimostrano il meccanismo di base, cioè la lettura di dati obsoleti da parte di un'enclave. Non hanno costruito una catena di attacco completa.

Due architetture restano fuori dalla verifica sperimentale. Arm CCA non è stata provata perché non esiste ancora silicio commerciale che la supporti, e gli autori scrivono che potrebbe essere colpita allo stesso modo. Le GPU NVIDIA per il confidential computing usano invece memoria integrata nel pacchetto del chip: i bus di comando e dati non sono raggiungibili da un avversario fisico, quindi un interposer non è installabile.

Perché il vecchio Client SGX resiste

La prima generazione di SGX, destinata a processori per postazioni di lavoro e ormai dismessa, si difende da sola. Assegna un contatore a ogni linea di cache e costruisce su

quei contatori un albero di integrità, la cui radice resta in memoria interna al processore. Scartare una scrittura rende l’albero incoerente, e il controllore di memoria se ne accorge.

Il prezzo di quella robustezza era la dimensione dell’area protetta, limitata a 256 megabyte. La lezione architetturale è esattamente questa: integrità e freschezza sono state sacrificate per rendere la cifratura scalabile ai carichi di lavoro cloud.

Non è un incidente di percorso, ed è Intel stessa a dirlo. Il 12 marzo 2026, sei mesi prima della divulgazione di DDRop, Simon Johnson, che in Intel guida lo sviluppo di TDX, ha esposto il ragionamento alla conferenza OC3 di Berlino.

Tre forze, secondo quelle slide, definiscono il perimetro di sicurezza accettabile: il livello di garanzia, il costo e le prestazioni. La formula è netta: è il costo totale di possesso a definire il confine reale della sicurezza. L’architettura ottimale massimizza la sicurezza verificabile dentro un involucro economicamente sostenibile.

Lo stesso intervento riconosce il limite della cifratura AES-XTS, diventata standard di fatto del settore perché efficiente e facile da distribuire. Offre una protezione limitata quando l’attaccante può osservare o manipolare la memoria cifrata, e la ricerca accademica recente ha dimostrato attacchi contro diverse implementazioni che la impiegano. Protezioni crittografiche più forti sono possibili, aggiunge Intel, ma non senza far salire il costo della piattaforma.

La risposta di Intel e AMD

Intel ha pubblicato l’annuncio di sicurezza 2026-09-14-001. L’azienda riconosce la ricerca e afferma che gli scenari descritti ricadono fuori dal proprio modello di minaccia per il confidential computing. Dichiara inoltre di valutare

ulteriori irrobustimenti architetturali e meccanismi di rilevamento, fra cui gli endorsement di proprietà della piattaforma.

L’annuncio elenca quattro condizioni dell’attacco: accesso fisico al server, installazione fisica dell’interposer, esecuzione di software privilegiato, impossibilità di sfruttamento da remoto. Ai clienti raccomanda pratiche di difesa in profondità: limitare e sorvegliare l’accesso fisico ai server, mantenere procedure sicure di gestione della filiera e dell’hardware, applicare il privilegio minimo, tenere aggiornati i sistemi.

AMD ha pubblicato il bollettino AMD-SB-3048 e assume una posizione più netta. La tecnica si fonda su un attacco fisico al bus di memoria, che resta fuori dal modello di minaccia pubblicato per SEV-SNP. AMD dichiara di non assegnare alcun identificativo CVE e di non prevedere mitigazioni. Elenca come prodotti interessati le serie EPYC 4004, 4005, 8004, 9004 e 9005, con le rispettive varianti embedded a partire dalla serie 4005, e i processori Instinct MI300A.

L’appendice etica dello studio ricostruisce le tempistiche. La prima segnalazione a Intel risale al 4 novembre 2025, con estensioni il 19 febbraio e l’8 aprile 2026. AMD è stata avvisata il 28 gennaio 2026, Arm il 29 aprile. AMD ha chiesto un periodo di riservatezza, e la data di divulgazione coordinata è stata fissata al 14 settembre 2026 con il consenso di Intel. Alla chiusura di questo articolo non risultano comunicazioni specifiche dei principali fornitori cloud né un bollettino di Arm.

La contromisura allo studio non blocca l’attacco: identifica chi

tiene l’hardware

L’annuncio di sicurezza rinvia a un documento tecnico che chiarisce la direzione presa. Si intitola «Platform Ownership Endorsements for Confidential Computing», ha identificativo 871281 ed è aggiornato al 2 febbraio 2026. Descrive un’architettura che consente a una parte remota di stabilire chi detiene fisicamente la piattaforma su cui gira il carico di lavoro.

Il meccanismo funziona in quattro passaggi. Il proprietario raccoglie, durante la filiera di fornitura o la manutenzione, gli identificativi univoci generati da ciascuna piattaforma al primo avvio. Su quegli identificativi emette un’attestazione firmata di proprietà. In fase di attestazione remota il verificatore controlla anche quell’attestazione. Approva soltanto le piattaforme il cui proprietario sia riconosciuto come affidabile nel garantire la protezione fisica.

Intel raccomanda il formato CoRIM e annuncia quattro strumenti di supporto, che dichiara non ancora rilasciati. Il documento è esplicito su ciò che l’architettura non fa: nessuna piattaforma può essere completamente sicura contro gli attacchi fisici.

La risposta di Intel, quindi, non elimina la soppressione delle scritture. Sposta la questione dal piano tecnologico a quello della custodia: chi ha in mano quel server, e su quale base ci fidiamo di lui.

I limiti dell’attacco

Va detto con altrettanta chiarezza che cosa DDRop non fa. L’attacco richiede due condizioni insieme: il controllo del software privilegiato e un accesso fisico al server bersaglio, seppure breve e una sola volta. Non è sfruttabile da remoto e non riguarda computer portatili o telefoni.

Gli esperimenti completi sono stati eseguiti su server con due processori. In quelle macchine la memoria di ciascun processore resta separata, e questo confina gli effetti dell'interposer. Su macchine con un solo processore, scrivono gli autori, servirebbe un controllo temporale molto più preciso dei guasti iniettati.

L'interposer usato è volutamente semplice e agisce su tutti i comandi diretti al modulo, comprese le letture. Scartare una lettura provoca l'arresto del sistema, quindi l'attacco resta limitato alle scritture. Un dispositivo più sofisticato, basato su FPGA, supererebbe il limite a costo di complessità e spesa maggiori.

Va infine segnalato che non risultano casi di sfruttamento fuori dal laboratorio. Nessuna delle fonti primarie consultate riporta incidenti reali.

Dove la questione diventa giuridica

Da qui in avanti il testo propone una lettura. I riferimenti normativi sono verificati sui testi ufficiali; il collegamento fra DDRop e quei riferimenti è un'interpretazione della redazione.

Gli autori indicano tre vie realistiche per ottenere l'accesso fisico: personale interno al centro dati con accesso ai rack, manomissione lungo la filiera di fornitura durante trasporto o installazione, accesso imposto da autorità giudiziarie o governative. I primi due scenari appartengono al rischio operativo. Il terzo è il perno attorno a cui ruota da anni la valutazione dei trasferimenti verso paesi terzi.

La sentenza Schrems II della Corte di giustizia, del 16 luglio 2020, fissa il metodo di quella valutazione. Le garanzie adeguate previste dall'articolo 46 del GDPR devono assicurare un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione. Per stabilire se lo assicurino vanno

considerate due cose insieme: le clausole contrattuali fra esportatore e importatore, e gli elementi dell'ordinamento del paese terzo che riguardano un eventuale accesso delle autorità pubbliche ai dati trasferiti.

Al punto 134 la Corte assegna il compito al titolare o al responsabile del trattamento stabiliti nell'Unione, cioè all'esportatore. Spetta a lui verificare caso per caso, se del caso in collaborazione con il destinatario, se il diritto del paese di destinazione garantisca una protezione adeguata. Deve fornire, se occorre, garanzie supplementari rispetto a quelle offerte dalle clausole.

Il punto 135 chiude il ragionamento. Quando le misure supplementari non bastano, l'esportatore o, in subordine, l'autorità di controllo devono sospendere o far cessare il trasferimento. Il terzo punto del dispositivo lo ripete come obbligo dell'autorità, quando la protezione richiesta dal diritto dell'Unione non possa essere garantita «con altri mezzi».

Quello stesso punto contiene però una riserva decisiva per leggere il quadro di oggi: l'obbligo vale «a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione». Dove una decisione di adeguatezza si applica, il trasferimento non richiede né lo strumento dell'articolo 46 né misure supplementari.

Per gli Stati Uniti quella decisione esiste dal 10 luglio 2023, ed è il Data Privacy Framework. Il Tribunale dell'Unione europea lo ha confermato il 3 settembre 2025 nella causa Latombe, e l'impugnazione davanti alla Corte di giustizia, depositata il 31 ottobre 2025, è tuttora pendente. Copre però solo i destinatari statunitensi certificati. Fuori da quel perimetro, cioè per gli importatori non aderenti e per gli altri paesi terzi, resta in piedi la valutazione caso per caso.

Le raccomandazioni 01/2020 del Comitato europeo per la protezione dei dati, adottate nella versione 2.0 il 18 giugno 2021 per dare seguito a quella sentenza, contengono due passaggi decisivi.

Il primo è al punto 53. Misure contrattuali e organizzative, da sole, in genere non impediscono l'accesso ai dati da parte delle autorità pubbliche di un paese terzo quando la legislazione applicabile è problematica. Solo misure tecniche correttamente attuate possono, in certe situazioni, rendere inefficace quell'accesso.

Il secondo è il caso d'uso 6 dell'allegato 2, ai punti 94 e 95. Riguarda il trasferimento verso fornitori cloud che devono accedere ai dati in chiaro per erogare il servizio. Vale però solo in una condizione: quando i poteri di accesso delle autorità del paese di destinazione eccedono ciò che è necessario e proporzionato in una società democratica. In quel caso il Comitato dichiara di non riuscire a immaginare, allo stato dell'arte, una misura tecnica efficace a impedire che l'accesso leda i diritti fondamentali degli interessati.

Due precisazioni completano il quadro. Il Comitato non esclude sviluppi tecnologici futuri capaci di raggiungere le finalità aziendali senza richiedere l'accesso in chiaro. E il punto 95 chiarisce che cifratura in transito e cifratura a riposo, anche combinate, non bastano se l'importatore possiede le chiavi.

Il confidential computing viene presentato proprio come la tecnologia che colma quella lacuna. Non è una lettura giornalistica.

I materiali con cui Intel ha presentato TDX alla conferenza OC3 del marzo 2023 elencano tre gruppi di motivazioni all'adozione. Il secondo riguarda i dati aziendali riservati o regolati, con richiamo esplicito al GDPR, e le collaborazioni fra più parti soggette a obblighi di conformità. Il terzo è

intitolato al controllo del dato e alla sovranità. La sua prima voce è «get the cloud provider out of my trust boundary», cioè togliere il fornitore cloud dal proprio perimetro di fiducia.

La stessa presentazione confronta i perimetri di fiducia con e senza TDX. Fuori dal perimetro finiscono lo stack cloud e i suoi amministratori, il BIOS, il firmware, il sistema operativo ospitante e l'ipervisore. Il livello fisico non compare nel confronto. Quella cornice non è invecchiata: nell'intervento del marzo 2026 il confidential computing viene descritto come tecnologia fondativa, che protegge il dato in uso in ambienti cloud, sovrani e aziendali.

Anche i fornitori di servizi la presentano così. La documentazione di Azure confidential computing afferma che, quando la funzionalità è attiva e configurata correttamente, Microsoft non può accedere ai dati non cifrati del cliente. Lo stesso testo descrive un modello di minaccia costruito per togliere all'operatore del fornitore la possibilità di accedere a codice e dati durante l'esecuzione.

Il sito dei ricercatori elenca fra i contesti d'uso i servizi confidenziali di AWS, Google Cloud, Microsoft Azure e IBM Cloud, oltre alla scoperta privata dei contatti di Signal e all'elaborazione privata di WhatsApp.

DDRop non dimostra che quei servizi siano stati violati. Dimostra che la garanzia su cui poggiano ha un confine dichiarato, e che quel confine esclude proprio la categoria di avversario che la valutazione dei trasferimenti deve considerare. Gli «altri mezzi» richiamati dalla Corte, quando si parla di dato in elaborazione, sono in larga parte questi.

Il caso italiano: che cosa chiede

davvero il regolamento ACN

Il regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione è stato adottato dall'Agenzia per la cybersicurezza nazionale con decreto direttoriale n. 21007/24 del 27 giugno 2024 e si applica dal 1° agosto 2024. Non impone il confidential computing. Impone però obblighi che presuppongono esattamente ciò che DDRop mette in discussione.

Per i dati e i servizi critici, l'allegato 3 chiede al punto 11_C un meccanismo di cifratura in cui l'amministrazione genera in autonomia almeno la chiave principale. Il modulo hardware di sicurezza che la custodisce può stare presso l'amministrazione stessa, presso il fornitore in modalità dedicata o presso una terza parte scelta dall'amministrazione.

Per il livello più alto di qualificazione l'allegato 4 alza l'asticella. Il punto 18_SS chiede un meccanismo che consenta all'amministrazione di generare e gestire in autonomia tutte le chiavi. Il punto 19_SS chiede di garantire l'accesso esclusivo dell'amministrazione alle chiavi e ai propri dati in chiaro.

Qui sta il nodo. La gestione autonoma delle chiavi protegge il dato a riposo e in transito, non il dato in elaborazione: per essere elaborato, il dato viene decifrato nella memoria del fornitore. In quel momento l'accesso esclusivo ai dati in chiaro dipende da come la piattaforma isola la memoria. Il confidential computing è la risposta tecnica abituale a quel problema, e DDRop mostra che la risposta ha un limite dichiarato dai produttori stessi.

Il regolamento contiene altri due elementi che il caso rende attuali. Per i dati e i servizi strategici, il punto 15_S dell'allegato 3 obbliga il fornitore a segnalare ad ACN e all'amministrazione ogni richiesta di accesso a dati o metadati proveniente da entità extra-UE. L'accesso può essere

concesso solo dopo un’autorizzazione esplicita dell’amministrazione. Sempre per il livello più alto, il fornitore deve rendere disponibili due cose: la metodologia di verifica del personale con accesso privilegiato e l’elenco dei dipendenti che ne dispongono. Da quell’elenco l’amministrazione può chiedere unilateralmente la rimozione di una o più persone.

Sono obblighi costruiti attorno all’accesso logico e alle persone. DDRop riguarda l’accesso fisico ai moduli di memoria, che nessuna di queste clausole intercetta.

Un ultimo riferimento chiude il cerchio. L’articolo 22, comma 5 riguarda i trasferimenti di dati personali fuori dallo Spazio economico europeo. In quei casi i responsabili del trattamento seguono le istruzioni dell’amministrazione e mettono a disposizione ogni informazione necessaria a valutare l’effettività delle misure adottate ai sensi del capo V del GDPR. È la cerniera fra il regolamento ACN e la valutazione descritta dalle raccomandazioni del Comitato europeo. Dopo il 14 settembre, l’informazione necessaria comprende anche il modello di minaccia coperto dalla piattaforma.

Cinque domande da porre al fornitore

Anche questa sezione è una proposta della redazione, non una prescrizione normativa.

Quali tecnologie di confidential computing sono attive sui nodi che ospitano il servizio, e in quale modalità di integrità? La distinzione fra integrità logica e integrità crittografica su TDX cambia il quadro. La modalità crittografica avrebbe impedito i primi due casi di studio, ma non la falsificazione della misura di avvio sulla macchina dell’attaccante. I ricercatori precisano di non aver potuto verificare quest’ultimo punto in laboratorio, perché il loro

sistema non supportava quella modalità.

Quali controlli esistono sull'accesso fisico ai rack e sulla catena di custodia dei moduli di memoria, e come vengono registrati? Sono le pratiche di difesa in profondità che Intel raccomanda nel proprio annuncio. Sono anche il livello su cui si sposta la protezione quando la cifratura della memoria non basta.

Quali interfacce di gestione della memoria restano attive? SEV-SNP prevede una politica che disabilita lo spostamento delle pagine dell'ospite. TDX non offre un'opzione equivalente, e l'interfaccia di gestione delle tabelle sicure è necessaria al funzionamento.

Come intende il fornitore dare seguito agli obblighi di trasparenza sui trasferimenti fuori dallo Spazio economico europeo? Se deve fornire ogni informazione utile a valutare l'effettività delle misure, il modello di minaccia della piattaforma rientra in quelle informazioni.

Che cosa afferma esattamente la documentazione contrattuale e di conformità già consegnata? Se un documento sostiene che il fornitore non può tecnicamente accedere ai dati, vale la pena verificare che l'affermazione sia circoscritta al modello di minaccia effettivamente coperto.

Le contromisure valutate dai ricercatori

Gli autori esaminano tre direzioni, e nessuna risolve il problema.

La prima è rilevare l'interposer misurando i tempi di addestramento della memoria all'avvio. Funziona in via di principio, perché l'esperimento mostra un aumento misurabile del ritardo sullo slot interposto. L'adozione richiederebbe però una validazione estesa su schede madri, controllori e

implementazioni di firmware diverse. Un modulo malevolo potrebbe inoltre integrare gli interruttori a bordo, riducendo il ritardo osservabile.

La seconda è una verifica durante il funzionamento: scrivere una sequenza nota in un'area riservata di ogni modulo e rileggerla. È un'euristica, aggirabile da un interposer che scarti le scritture in modo più selettivo.

La terza è l'irrobustimento del software, cioè disattivare le interfacce non necessarie e rileggere per controllo dopo le operazioni critiche. Nessuna di queste misure introduce la freschezza. Gli autori sono espliciti: una correzione duratura richiede motori di cifratura della memoria che offrano insieme integrità e freschezza, quindi una modifica dell'hardware.

Intel, dal canto suo, lavora su cinque fronti elencati nell'intervento di marzo: endorsement di proprietà della piattaforma, riduzione della superficie d'attacco delle enclave, attestazione radicata nell'hardware, ricerca sul rilevamento delle manomissioni fisiche e nuova generazione di cifratura della memoria.

L'ultimo fronte è quello che tocca DDRop. La spinta, dichiara Intel, viene dalla scala dell'intelligenza artificiale confidenziale, che sta mettendo sotto pressione i limiti della cifratura basata su AES e il suo modello di costo. La direzione allo studio è una costruzione basata su ASCON, con blocchi più grandi e versionamento opzionale delle linee di cache, presentata come resistenza più forte alla manomissione fisica e agli attacchi di replay. Lo studio osserva però che non è chiaro se quel disegno neutralizzerebbe la soppressione delle scritture.

In sintesi

DDRop non è una vulnerabilità da correggere con un aggiornamento. È la conferma sperimentale di un compromesso di

progetto noto, portata al livello di costo e di praticabilità che rende il discorso concreto. La risposta dei due produttori conferma che quel compromesso è voluto.

Per chi scrive valutazioni d’impatto, contratti e dichiarazioni di conformità la conseguenza è più semplice di quanto appaia. Le affermazioni sul confidential computing vanno formulate indicando il modello di minaccia coperto, non come garanzie assolute.

https://www.ictsecuritymagazine.com/notizie/ddrop-confidential-computing-intel/

Creative Photo Illustration with an iPhone with Russell Preston Brown

Great photo illustrations still start with great photographs, and you don’t need a studio full of gear to create them.

In his new class, **Adobe**’s **Russell Preston Brown** starts with an iPhone, one continuous light, and a tripod to photograph model and professional bubbleologist **Kirk Marsh**. Russell shows you how to shoot 48-megapixel raw on the iPhone and create split, Rembrandt, loop, and butterfly lighting using just that single light.

Then the fun really starts.

Russell takes the photographs into **Lightroom** and **Photoshop**, where he uses Adobe Firefly and Generative Fill to build on what he captured in camera. You’ll see how he adds lighting that wasn’t there during the shoot and creates elements for

the scene without changing his original subject.

It’s a great example of how a strong photograph and a little imagination can become something completely different. Watch Russell tell you more about it below, and then check it out. *You can watch two lessons from the course for free.*

▶️ Watch it today!

https://layersmagazine.com/creative-photo-illustration-iphone-russell-brown.html

---

Mark Weinstein Joins Target as CMO and Guest Experience Officer



The future of brands gets decided here. Join the industry’s top marketers at Brandweek for the ideas, insights, and connections shaping what’s next. **Get your ticket.**

Mark Weinstein needs to find a Target-red necktie after being named CMO and guest experience officer for the retailer.

Tasked with elevating the consumer experience and boosting the brand’s growth strategy, Weinstein will report directly to Target CEO Michael Fiddelke.

“Mark has a proven ability to understand what consumers value and turn those insights into brand connections that feel relevant and personal,” Fiddelke said in a statement. “His leadership will help us elevate the guest experience across every interaction with Target.”

The news comes days after Weinstein stepped down as chief marketing officer and head of luxury brands at Hilton, where

he had spent the last 16 years overseeing all 28 brands.

Recommended videos
https://www.adweek.com/brand-marketing/mark-weinstein-joins-target-cmo-guest-experience-officer/

Consigli utili per dormire: quali abitudini aiutano davvero il sonno

Una notte difficile non equivale a insonnia cronica. Per capire se esiste un problema ricorrente, conta soprattutto ciò che accade nel tempo: gli orari, il tempo trascorso svegli a letto, i risvegli, le condizioni della camera e le abitudini della serata.

Osservare questi elementi evita di attribuire subito la colpa a un singolo fattore. Permette invece di individuare gli ostacoli che si ripetono e di sperimentare cambiamenti mirati. Le regole di igiene del sonno possono creare condizioni più favorevoli, ma non costituiscono una terapia individuale e non bastano a stabilire la causa di una difficoltà persistente.

Partire da un registro semplice del sonno

Per alcuni giorni può essere utile annotare l’ora in cui ci si corica, quella approssimativa dell’addormentamento, gli eventuali risvegli e l’orario del risveglio definitivo. Nello stesso registro trovano posto le circostanze potenzialmente rilevanti: uso di schermi prima di dormire, consumo serale di

caffeina o alcol, rumori, luce, caldo e attività svolte nell’ultima parte della giornata.

Non serve ottenere misurazioni perfette. Lo scopo è riconoscere una sequenza: per esempio, capire se le notti peggiori coincidono spesso con orari molto variabili oppure con una camera troppo calda. Una coincidenza non prova da sola un rapporto di causa ed effetto, ma indica da quale cambiamento conviene iniziare.

È preferibile non modificare tutto contemporaneamente. Se si anticipa l’orario, si eliminano gli schermi, si cambia alimentazione e si interviene sulla camera nella stessa sera, un eventuale miglioramento non dirà quale scelta abbia inciso davvero.

La regolarità viene prima della ricerca dell’orario perfetto

Andare a letto e alzarsi a orari regolari, anche nei fine settimana e nei giorni liberi, è una delle raccomandazioni ricorrenti per l’igiene del sonno. Non garantisce di addormentarsi subito, ma offre al riposo una struttura quotidiana più coerente.

Il registro aiuta a valutare quanto gli orari reali si discostino da quelli desiderati. Se la variazione è frequente, la prima prova può consistere nel rendere più costanti sia il momento di coricarsi sia quello del risveglio. L’esito va giudicato su una serie di notti, non sulla prima: anche un’abitudine appropriata può essere seguita da una notte poco soddisfacente.

Il letto dovrebbe rimanere associato principalmente al sonno e all’attività sessuale. Quando l’addormentamento non arriva dopo un certo periodo, le raccomandazioni disponibili suggeriscono di alzarsi, dedicarsi in un ambiente poco

illuminato a qualcosa di tranquillo e tornare a letto quando ricompare la sonnolenza. Le fonti indicano tempi diversi, quindi non è utile trasformare questa indicazione in un conto alla rovescia rigido.

Ridurre luce e attività stimolanti prima di coricarsi

Nelle ore che precedono il sonno conviene abbassare progressivamente il livello degli stimoli. La luce intensa e la luce blu degli schermi possono ostacolare il riposo, così come le attività che mantengono alta l'attivazione. Non esiste però un unico intervallo di astensione dagli schermi adatto a chiunque.

Una prova realistica può partire dalla sostituzione dell'ultima parte della serata con attività più calme, come leggere, fare un bagno o praticare esercizi respiratori. Anche in questo caso è il confronto fra più serate simili a mostrare se il cambiamento è plausibilmente utile.

Il punto non è introdurre una cerimonia elaborata, ma creare un passaggio riconoscibile fra veglia e riposo. Una routine troppo difficile da mantenere rischia di essere abbandonata; una sequenza breve e ripetibile è più facile da valutare nel tempo.

Controllare le condizioni della camera

Una camera buia, silenziosa, confortevole e non eccessivamente calda offre condizioni più adatte al sonno. Tende pesanti o una mascherina possono limitare la luce; tappi auricolari, ventilatori o rumore bianco possono invece attenuare i disturbi sonori, a seconda delle necessità individuali.

Non occorre inseguire una temperatura numerica universale. È più utile verificare se durante la notte si avverte caldo o freddo eccessivo e intervenire di conseguenza. Quando il problema riguarda tutta l'abitazione, possono essere utili anche accorgimenti per gestire il caldo in casa prima che la temperatura della camera diventi un ostacolo al riposo.

Per capire quale elemento pesa di più, conviene separare le prove. Se luce e rumore sono già ben controllati ma i risvegli coincidono con notti particolarmente calde, si può intervenire prima sulla temperatura. Se invece l'ambiente è confortevole ma entra luce al mattino presto, la priorità cambia.

Caffeina, nicotina e alcol: osservare l'effetto della sera

Caffeina, nicotina e alcol assunti durante la serata possono interferire con il sonno. Caffeina e nicotina hanno un'azione stimolante, mentre l'alcol può favorire i risvegli notturni. Le indicazioni disponibili non fissano quantità e orari identici per tutti, perciò il registro personale resta utile per individuare consumi ricorrenti nelle serate peggiori.

La prova più leggibile consiste nel limitare un fattore alla volta, mantenendo per quanto possibile stabili gli altri. Se si sospetta la caffeina serale, per esempio, è meglio non accompagnare lo stesso esperimento con una modifica radicale di tutti gli orari e dell'ambiente. Il risultato sarà più facile da interpretare.

Come capire se un cambiamento sta funzionando

Un miglioramento reale non coincide soltanto con l'impressione lasciata da una singola mattina. Nel registro si possono confrontare alcuni segnali concreti: maggiore facilità ad

addormentarsi, meno tempo trascorso svegli a letto, risvegli meno disturbanti e migliore funzionamento durante il giorno.

Se una modifica non produce differenze riconoscibili dopo una prova sufficientemente ripetuta, si può passare alla leva successiva indicata dagli appunti. Un ordine ragionevole è partire dal problema più frequente: prima gli orari, se sono molto variabili; poi luce e attività serali, se il periodo prima di dormire è molto stimolante; quindi ambiente e sostanze serali, quando emergono associazioni ricorrenti.

Questo metodo non trasforma il diario in uno strumento diagnostico. Serve a rendere più chiaro ciò che accade e a portare informazioni ordinate anche a un eventuale colloquio con un professionista.

Quando è opportuno chiedere aiuto

Le abitudini non spiegano ogni forma di insonnia. Se la difficoltà persiste o incide sulla vita quotidiana, aumentare la rigidità della routine potrebbe non essere sufficiente. Humanitas indica come opportuno rivolgersi al medico quando il problema compromette la qualità della vita, per esempio con sonnolenza diurna, stanchezza, irritabilità oppure difficoltà di concentrazione e memoria.

Il medico può valutare il quadro complessivo e stabilire se sia indicato un approfondimento o il ricorso a un centro del sonno. La frequenza dei disturbi, la loro durata e le conseguenze diurne hanno più valore di una singola notte negativa.

Il monitoraggio può continuare con poche annotazioni essenziali: orari, ostacolo principale, cambiamento sperimentato e qualità della giornata successiva. È questo confronto ordinato, più della ricerca di una regola perfetta, a mostrare quali abitudini producono un miglioramento riconoscibile e quali difficoltà richiedono invece una

valutazione.

L’articolo Consigli utili per dormire: quali abitudini aiutano davvero il sonno proviene da Il Kim Magazine.

https://www.ilkim.it/consigli-utili-per-dormire-quali-abitudini-aiutano-davvero-il-sonno/

Week of Aug 31 Cable News Ratings: Fox News & MS NOW Record Gains in Demo

CNN was the only network to register across-the-board declines week over week. https://www.adweek.com/tvnewser/week-of-aug-31-2026-cable-news-ratings/

One Year Post-American Eagle Scandal, Sydney Sweeney Sparks Ire by Going Naked for Novig

The ad has received backlash for reversing years of gains for female athletes https://www.adweek.com/brand-marketing/one-year-post-american-

eagle-scandal-sydney-sweeney-sparks-ire-by-going-naked-for-novig/

Kate McKinnon Is an Evil CEO in Sequel to Zoom's Bowen Yang-Led Brand Reset

The SNL alum fronts the next phase of the company's largest global campaign ever
https://www.adweek.com/brand-marketing/kate-mckinnon-is-an-evil-ceo-in-sequel-to-zooms-bowen-yang-led-brand-reset/

Samsung Taps Couples Therapy's Dr. Orna Guralnik to Ease Phone Switching Fears

Samsung enlists Couples Therapy's Dr. Orna Guralnik and a group of famous duos to address the emotional barriers of phone switching.
https://www.adweek.com/creativity/samsung-taps-couples-therapys-dr-orna-guralnik-to-ease-phone-switching-fears/

Sonos’ New Brand Story Aims to Win Back Trust Two Years After Botched App Update

First campaign under new CMO Colleen DeCourcy is the most significant repositioning in Sonos’ history. https://www.adweek.com/creativity/sonos-new-brand-story-aims-to-win-back-trust-two-years-after-botched-app-update/

Liz Rutgersson Named CEO of Stagwell’s Assembly to Build ‘Agency for the Future’

Rutgersson previously held the title of CEO at Dentsu’s iProspect
https://www.adweek.com/agencies/liz-rutgersson-named-ceo-of-stagwells-assembly-to-build-agency-for-the-future/