Segmentazione basata sul software

Un approccio dall'interno verso l'esterno per ottenere una solida struttura di sicurezza

SOMMARIO

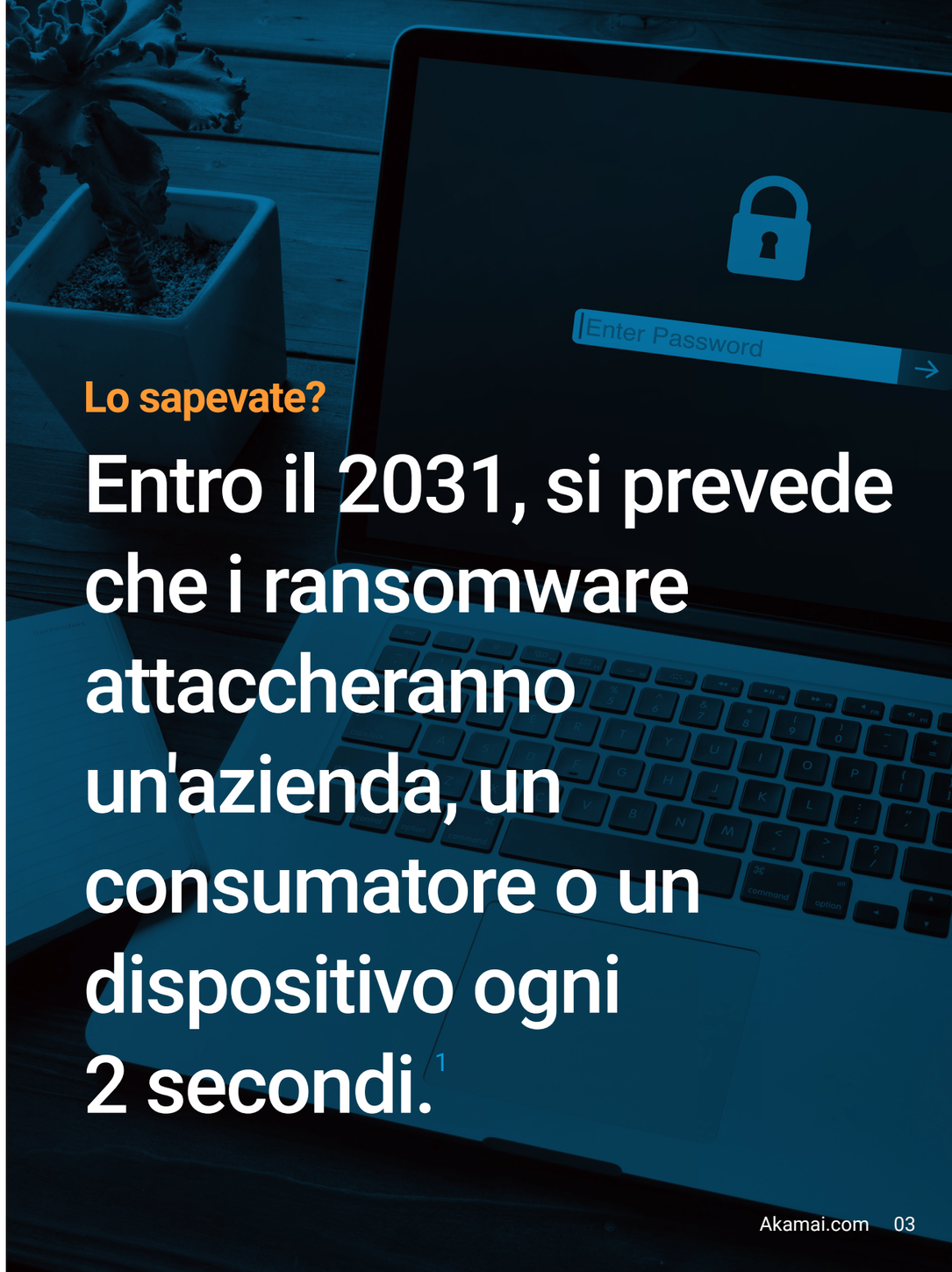
Superamento dei firewall tradizionali

Lo sappiamo. Siete stanchi dei vecchi firewall on-premise. Gli ambienti IT e i requisiti di sicurezza si sono evoluti anni luce rispetto a quello per cui erano stati originariamente creati. E anche il panorama della sicurezza informatica si è evoluto: i metodi di attacco sono diventati più sofisticati e i criminali informatici sono sempre di più. Un'architettura di appliance vecchia di decenni semplicemente non è in grado di resistere ai più recenti malware, attacchi botnet, schemi di phishing, social engineering ed estorsioni di dati.

Ma, nonostante la miriade di problemi che presentano, sono ad esempio costosi, immobili e privi di visibilità, solo per citarne alcuni, la realtà è che i firewall legacy non scompariranno presto. Essi svolgono un'importante funzione nel perimetro che gestisce il traffico nord-sud e forniscono una solida struttura di protezione per l'organizzazione.

Ma i firewall non possono gestire il traffico est-ovest nei data center locali e nel cloud.

Questo è un compito che deve svolgere la segmentazione basata su software.



Lo sapevate?

Entro il 2031, si prevede che i ransomware attaccheranno un'azienda, un consumatore o un dispositivo ogni 2 secondi.[1]

Risolto!

3 problemi con i firewall legacy

1. Il problema: **Mancanza di visibilità**

   La mancanza di visibilità nel flusso di dati rende difficile l'implementazione e il mantenimento delle regole. Per questo motivo, i firewall hanno spesso set di regole estremamente lunghi e hanno molte regole eccessivamente permissive o addirittura non necessarie.

La soluzione

Cercate soluzioni che integrino una mappa visiva, una classificazione delle risorse e una mappatura delle dipendenze delle applicazioni con la creazione e la gestione delle policy.

Risolto!

3 problemi con i firewall legacy

2. Il problema: i firewall hanno una manutenzione complessa

I proprietari delle applicazioni e gli amministratori del firewall raramente conoscono le porte IP e i protocolli appropriati che devono comunicare. Quindi, la gestione dei firewall diventa un processo iterativo di risoluzione dei problemi.

La soluzione

Invece di definire le policy sugli "elementi di protezione" della rete fissa come IP e porte, basatele su attributi significativi come il processo utilizzato da un'applicazione, i nomi di dominio completi (FQDN) e l'identità dell'utente. In questo modo, gli attributi rimangono gli stessi e le vostre policy continueranno a funzionare, anche se apportate una modifica al data center o spostate il carico di lavoro nel cloud.

Risolto!

3 problemi con i firewall legacy

3. Il problema: i firewall mancano di agilità

Qualsiasi modifica apportata a un firewall di solito richiede la pianificazione di downtime. Quando il proprietario di un'applicazione deve apportare una modifica, può attendere una settimana o più prima che la modifica venga rivista e implementata durante una finestra di manutenzione.

La soluzione

Le moderne organizzazioni IT sono passate dalle finestre di modifica ai modelli DevOps in cui le applicazioni vengono visualizzate e aggiornate continuamente. Trovate una soluzione tecnologica che possa essere automatizzata utilizzando gli stessi strumenti DevOps che utilizzate per le applicazioni stesse. In questo modo, man mano che le applicazioni si evolvono, l'approccio alla sicurezza si adatta di conseguenza.

Potete portarlo con voi

Parliamo dell'approccio tradizionale. È complicato. E non è adattabile. L'approccio di vecchia scuola alla gestione dei firewall legacy basa la segmentazione sulla posizione e tale posizione non può essere modificata facilmente. Di solito è basato su un indirizzo IP codificato o instradato a un data center. Ciò significa che è necessario spostare fisicamente tutto quello che si desidera proteggere dietro il firewall, un processo che richiede molte risorse, è avverso al rischio e lento. Migrazione nel cloud? Visibilità? Sicurezza adeguata? Dimenticateli.

Lasciate i firewall legacy dove si trovano. Fate un respiro profondo e adottate qualcosa di innovativo. La segmentazione basata su software può essere facilmente implementata insieme ai firewall esistenti ed è adattabile. Con la segmentazione basata su software, potete effettivamente apportare modifiche all'ambiente, al data center e alla rete e impostare criteri in base a ciò che osservate. E il carico di lavoro e le policy possono essere visualizzati ovunque: nel cloud, nel data center, ovunque. Inoltre, potete applicare e adattare la vostra policy di sicurezza senza apportare modifiche alla rete e senza downtime del sistema.

Rivelate i vostri segmenti interni

Vi fidereste di qualcosa che non potete effettivamente vedere? Crediamo di no. Ma è esattamente ciò che succede quando stabilite policy di sicurezza dietro un firewall. Non potete effettivamente vedere cosa c'è dentro. È come guardare un edificio senza riuscire a vedere le persone all'interno.

La segmentazione basata sul software non si basa sul caso. Separa gli elementi offrendovi una consapevolezza totale di tutte le attività in cui sono coinvolti i carichi di lavoro. Una volta consapevoli delle risorse presenti all'interno del vostro ambiente, potete formulare un piano e suddividere i segmenti in qualcosa di significativo ed efficace in base agli specifici casi di utilizzo.

Sicurezza oltre il perimetro

I firewall legacy semplicemente non sono stati creati per il cambiamento. Sebbene servano a uno scopo importante a livello perimetrale, come la protezione DDoS e il filtraggio e l'ispezione del traffico, la sicurezza all'interno della rete è difficile da realizzare con i firewall. Perché? Sono stati implementati come punti di strozzatura naturali, il che significa che ogni sforzo di segmentazione comporta blocchi operativi, come la necessità di modificare e rimuovere reti e applicazioni. Ciò è impegnativo e richiede molte risorse.

La segmentazione basata su software può aiutarvi a superare queste sfide operative e consentirvi di continuare le vostre pratiche di sicurezza oltre gli endpoint e i perimetri. Innanzitutto, prevede un approccio firewall distribuito (rispetto a un punto di strozzatura). In secondo luogo, è incentrata sul carico di lavoro, il che significa che può raccogliere dati dal sistema host e quindi applicarli alla classificazione delle risorse e adottare a un approccio più granulare alle regole, come i contenuti e le policy a livello di processo. Nel complesso, la segmentazione basata sul software è un modo più adattabile e granulare per proteggere le risorse critiche all'interno della rete e richiede meno sforzi e risorse rispetto ai firewall.

4 nozioni di base sulla segmentazione

La segmentazione è più importante che mai. Le superfici di attacco sono più ampie. Gli attacchi sofisticati, come il ransomware, si spostano lateralmente dopo una violazione e bisogna pensare alle dipendenze delle applicazioni oltre il perimetro. Ma la segmentazione non è un approccio unico.

Ecco uno sguardo a quattro tipi comuni di segmentazione, in che modo si differenziano e perché sono necessari.

1. Segmentazione dell'ambiente

Separa i sistemi in diversi ambienti di sviluppo, come sviluppo, controllo qualità, staging e produzione. Questa è una versione ampia della segmentazione in cui l'obiettivo finale è separare i sistemi in ambienti diversi per garantire che l'accesso sia limitato solo agli utenti e alle applicazioni necessari. Molte iniziative di conformità richiedono la garanzia che i sistemi non di produzione non possano accedere ai sistemi di produzione.

2. Segmentazione della rete

È una pratica architettonica per suddividere una rete in più sottoreti, ciascuna delle quali è il proprio segmento di rete più piccolo. La segmentazione della rete offre agli operatori IT uno strumento per controllare meglio il traffico di rete, aumentare le performance e migliorare la sicurezza.

3. Microsegmentazione

È una forma più granulare di segmentazione utilizzata per isolare i carichi di lavoro l'uno dall'altro e proteggerli individualmente. Ciò include la possibilità di impostare regole di segmentazione per elementi come processi, contenitori, utenti, nomi di dominio e dispositivi. Questo approccio è superiore nel controllo del traffico est-ovest e nella protezione contro il movimento laterale.

4. Segmentazione basata sull'identità

Si espande oltre la capacità della microsegmentazione di proteggere un singolo endpoint, dispositivo, carico di lavoro o container abilitando regole dinamiche che valutano l'identità, ad esempio l'utente, il dispositivo o il contesto, nel decidere se consentire la comunicazione. Le policy di segmentazione basate sull'identità possono essere basate su impostazioni granulari, non solo IP o porta, come tag, tipo di sistema operativo o caratteristiche dell'applicazione.

Mito o realtà: 5 miti sulla segmentazione sfatati

Mito numero 1

I progetti di segmentazione sono troppo difficili e richiedono troppo tempo per essere completati.

Realtà: Iniziare con la visibilità e una chiara comprensione di ciò che sta accadendo all'interno del proprio ambiente riduce il completamento della segmentazione da mesi a settimane o addirittura giorni. Le moderne tecnologie di segmentazione possono anche utilizzare l'IA per accelerare ulteriormente il processo.

Mito numero 2

I progetti di segmentazione richiedono modifiche all'infrastruttura di rete e downtime.

Realtà: La segmentazione basata sul software separa la sicurezza dall'infrastruttura, quindi la segmentazione può essere eseguita indipendentemente dall'infrastruttura sottostante senza modifiche o downtime.

Mito numero 3

La segmentazione blocca il traffico legittimo nella rete.

Realtà: La visualizzazione dell'ambiente e l'utilizzo di policy di segmentazione basate sul software consentono di vedere l'effetto che queste policy avranno sulle attività aziendali prima dell'attivazione dell'applicazione in tempo reale.

Mito numero 4

La segmentazione inibisce l'accesso degli utenti e introduce una latenza non necessaria.

Realtà: L'utilizzo di policy di segmentazione distribuite basate sul software invece di forzare tutto il traffico attraverso specifici punti di strozzatura del firewall elimina i colli di bottiglia della rete. E policy più precise che tengono conto dell'applicazione e dell'identità riducono il rischio di problemi di accesso accidentale degli utenti.

Mito numero 5

Non posso utilizzare gli stessi strumenti di segmentazione nel cloud che utilizzo on-premise.

Realtà: Se si separano le policy di segmentazione dall'infrastruttura, le stesse policy utilizzate nel data center possono funzionare anche nel cloud.

Akamai

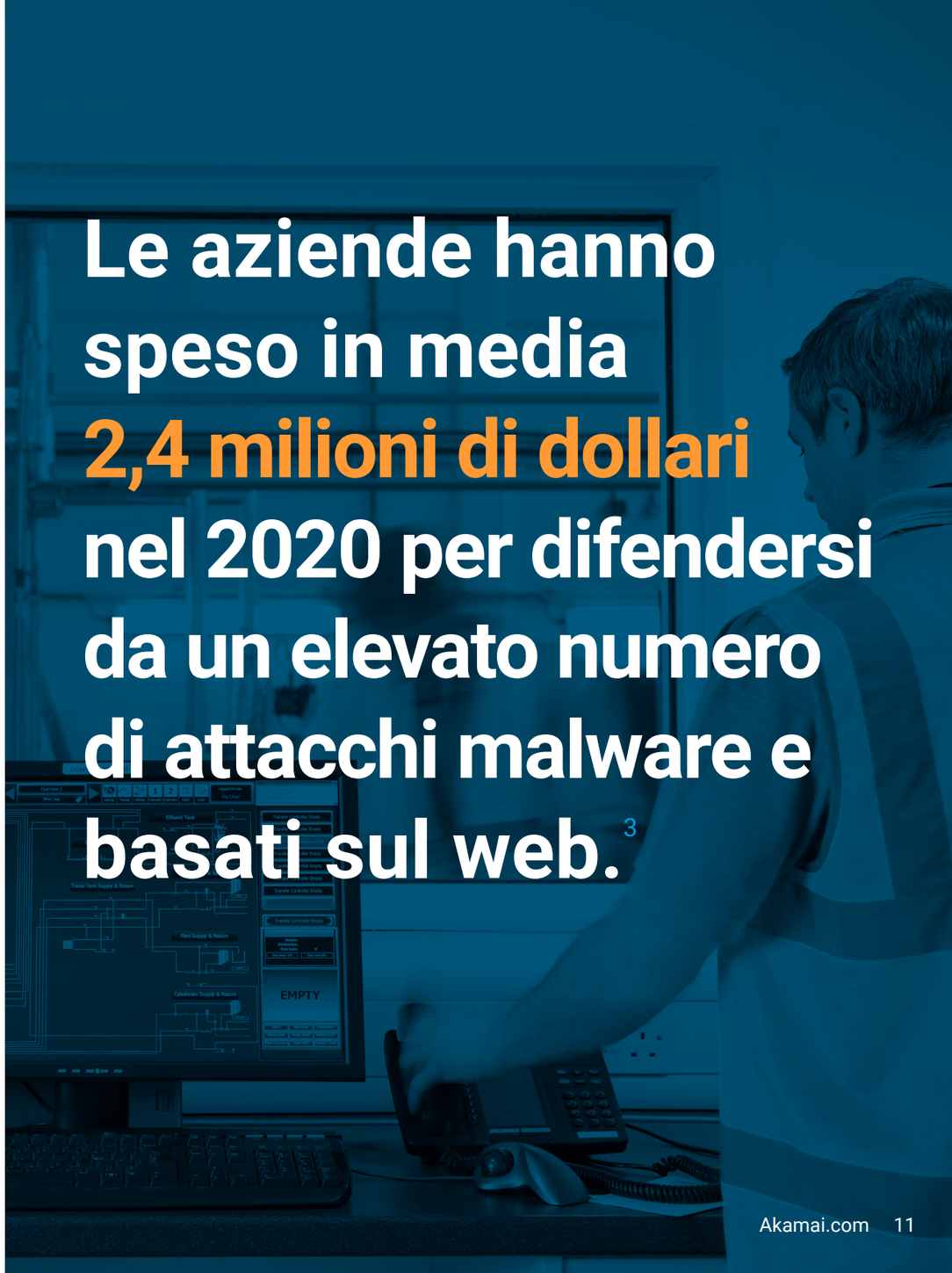
Riduzione dei rischi all'interno

Le violazioni esistono. E possono paralizzare la vostra attività, compromettere i vostri dati, danneggiare il vostro marchio e costarvi milioni.

Pensate ancora che i firewall siano sufficienti? Riflettete. Una volta che un utente malintenzionato ha violato una rete, un ambiente o un data center, utilizzerà il movimento laterale per rubare dati e provocare il caos, come prendere il controllo dei server delle applicazioni o accedere ai server dei database.

In effetti, il 70% di tutti gli attacchi attualmente comporta tentativi di movimento laterale.[2]

Mentre i firewall considerano il movimento laterale come traffico legittimo che si verifica all'interno di una rete, la segmentazione basata sul software lo blocca completamente. Un componente fondamentale per il vostro programma di sicurezza, la segmentazione basata sul software vi consente di limitare il movimento laterale e, in caso di violazione, di rendere più difficile per un utente malintenzionato navigare nell'ambiente. Avete la possibilità di combattere per proteggere i dati e le applicazioni critiche, diminuendo il tempo di permanenza e persino rilevando l'autore dell'attacco. Questo approccio è più scalabile, facile da usare e consente di implementare rapidamente la segmentazione senza apportare modifiche alla rete o ai sistemi.



Il modello Zero Trust non deve essere complicato.

Adottare Zero Trust significa sapere chi fa cosa a chi e come lo fa. In altre parole, si tratta di avere un controllo esplicito sulle attività degli utenti all'interno della vostra rete.

Fornendo a un utente l'accesso completo all'interno della rete, state concedendo automaticamente troppa fiducia e, di conseguenza, mettendo a rischio l'intera organizzazione. In primo luogo, i dipendenti spesso commettono errori, che potrebbero avere gravi implicazioni sulla sicurezza. Alcuni hanno anche cattive intenzioni.

Inoltre, al di fuori delle reti e dei dispositivi VPN, ci sono molti punti di accesso al data center che dovreste considerare. Ad esempio, gli aggressori possono accedere a una rete tramite il server di produzione (come nel caso della violazione di SolarWinds), un'applicazione vulnerabile con connessione a Internet o una VPN vulnerabile. In questo caso, vi fidate di un server solo perché è all'interno della vostra rete, ma in pratica il malintenzionato può accedere a qualsiasi risorsa e spostarsi lateralmente senza limitazioni.

Per attuare il modello Zero Trust nella vostra rete di produzione, dovete bloccare tutte le attività che non sono esplicitamente consentite.

Questa è una funzione che i firewall legacy semplicemente non sono in grado di eseguire a livello granulare, perché richiede l'identificazione di attributi a un livello più profondo degli indirizzi IP e delle porte.

In alternativa, la segmentazione basata sul software consente di vedere effettivamente cosa sta accadendo in dettaglio e creare policy precise e comprensibili che includono l'identità.

Checklist per il modello Zero Trust: 6 modi per ottenere il controllo esplicito

Manteniamola semplice. La fiducia dovrebbe basarsi sulle dimensioni del segmento e più piccolo è il segmento, meglio è quando si tratta di proteggere dati, risorse e applicazioni critici. Ecco sei passaggi per attuare il modello Zero Trust senza la complessità operativa.

1 Identificate i vostri dati sensibili utilizzando etichette di visualizzazione.

2 Mappate i flussi dei vostri dati sensibili utilizzando un flusso automatizzato e la mappatura delle dipendenze.

3 Progettate i vostri micro-perimetri Zero Trust utilizzando gli strumenti giusti per la definizione rapida di qualsiasi policy di segmentazione o microsegmentazione.

4 Monitorate continuamente il vostro ecosistema Zero Trust tramite monitoraggio e analisi in tempo reale.

5 Adottate l'automazione e il coordinamento della sicurezza con le API e le integrazioni tecnologiche.

6 Implementate funzionalità che consentano di contrassegnare come inaffidabile qualcuno o qualcosa in modo tale che, in caso di attacco, possiate contrassegnare come inaffidabile qualsiasi computer con attributi predefiniti, indipendentemente dall'utente o dal segmento.

Akamai

Redditività

A questo punto, probabilmente vi starete chiedendo come potete eliminare le soluzioni di vecchia scuola per rafforzare la vostra strategia di sicurezza all'interno della rete.

Nessun problema.

Lasciate i firewall legacy dove si trovano, sono utili a proteggere il perimetro della rete. Ma i vantaggi si fermano davvero qui.

La risorsa più importante risiede nel cuore della vostra organizzazione, le risorse digitali, i dati e le applicazioni che esistono oltre il perimetro: le fondamenta della vostra infrastruttura aziendale. Spostare la vostra attenzione dall'esterno verso l'interno e implementare la segmentazione basata sul software e una struttura Zero Trust vi fornirà la visibilità e il controllo necessari per rilevare e fermare il movimento laterale, applicare policy granulari e adattabili e bloccare la propagazione degli attacchi informatici, come il ransomware, sulla vostra rete.

Richiedete una demo o richiedete **ulteriori informazioni** su come la segmentazione possa aiutarvi con il ransomware, il modello Zero Trust, la sicurezza nel cloud e molto altro.

1 Cybersecurity Ventures. Rapporto sul mercato dei ransomware nel 2022. Conceal, 2022.

2 Kellerman Tom e Greg Foss. Rapporto sulla risposta agli incidenti a livello globale. VMware Carbon Black, ott. 2020.

3 "Dati e tendenze delle statistiche sulla cybersicurezza nel 2023". PurpleSec, 22 feb. 2023.