WHITE PAPER

Come spezzare la kill chain del ransomware: prevenzione e mitigazione dei rischi

con Akamai Guardicore Segmentation per minimizzare l'impatto del ransomware

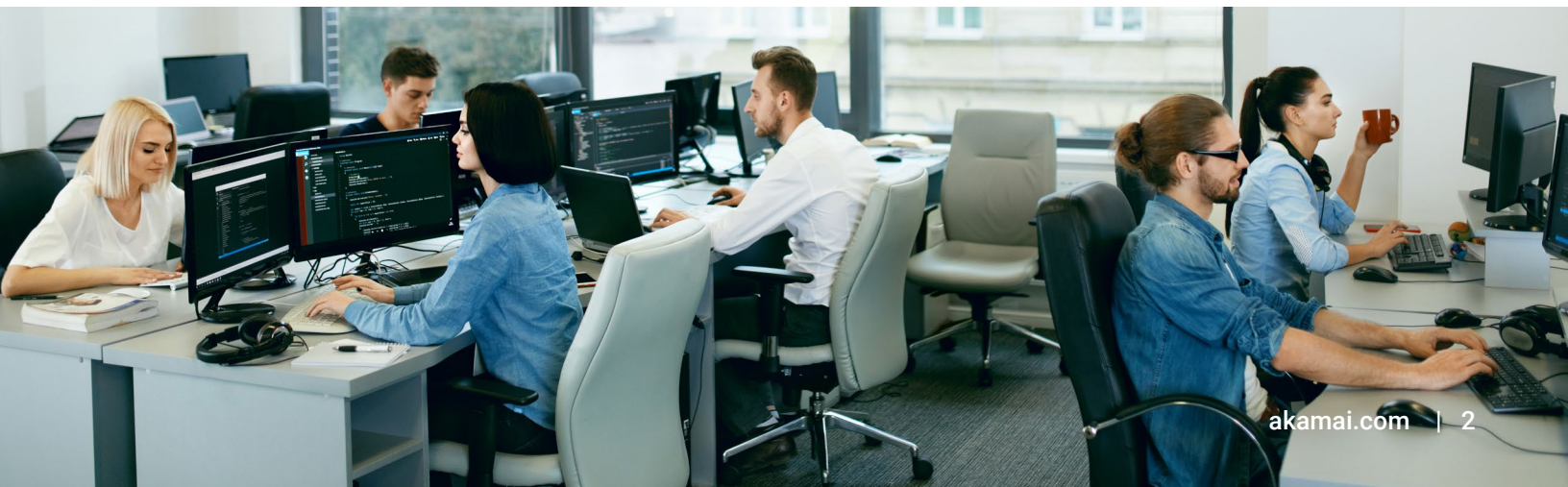
Panoramica

Il ransomware, un tempo semplicemente un fastidioso malware usato dai criminali informatici per limitare l'accesso a file e dati tramite la crittografia, si è trasformato in qualcosa di molto peggiore. La perdita definitiva di dati è un danno scioccante, ma oggi i criminali informatici e gli autori di attacchi governativi sono talmente sofisticati da usare i ransomware per penetrare e paralizzare aziende, governi federali, infrastrutture globali e organizzazioni sanitarie.

Nel 2017, il cryptoworm WannaCry, che ha colpito 230.000 computer in tutto il mondo, sfruttando una vulnerabilità di Microsoft Windows, ha messo in evidenza le minacce rappresentate dal ransomware. Da allora, i criminali sono diventati solo più sofisticati e gli attacchi più invasivi, inclusa la comparsa del RaaS (Ransomware-as-a-Service), in cui gli hacker vendono i loro servizi. Il rapporto di Akamai sulle minacce ransomware nella prima metà del 2022 ha valutato lo schema degli attacchi di Conti, un famigerato gruppo RaaS che è stato rilevato per la prima volta nel 2020 e sembra avere sede in Russia. L'analisi allude alla necessità di adottare solidi sistemi di protezione contro il movimento laterale e al ruolo fondamentale che questi sistemi possono svolgere nella difesa dal ransomware. Inoltre, il rapporto ha rivelato che la stragrande maggioranza di vittime del gruppo Conti era costituita da aziende con un fatturato di 10-250 milioni di dollari USA.

> **La microsegmentazione riduce la fiducia implicita nella rete consentendo solo la connettività esplicitamente definita dalle policy, applicando, di conseguenza, l'accesso del privilegio minimo alle applicazioni per il traffico tra computer.**
>
> **- Forrester, Le best practice per la microsegmentazione Zero Trust, 27 giugno 2022**

Ciò indica chiaramente che sono a rischio le organizzazioni di tutte le dimensioni a causa di una combinazione di tecnologie obsolete, strategie di difesa "adeguate" incentrate esclusivamente sui perimetri e sugli endpoint, mancanza di formazione (e scarsi protocolli di sicurezza) e assenza di una soluzione nota. In realtà, nel rapporto sul mercato dei ransomware 2023 di Cybersecurity Ventures, si prevede che, entro il 2031, i ransomware attaccheranno un'azienda, un consumatore o un dispositivo ogni due secondi.



Tutto dipende dal movimento laterale

Un attacco ransomware inizia con una violazione, spesso perpetrata tramite un'e-mail di phishing, una vulnerabilità nel perimetro di rete o attacchi di forza bruta, che creano delle falle, distraendo, al contempo, i sistemi di difesa dall'intento effettivo dell'autore dell'attacco. Una volta penetrato nel dispositivo o nell'applicazione, il malware procede con l'escalation dei privilegi e un movimento laterale attraverso la rete e più endpoint, al fine di massimizzare l'infezione e i punti di crittografia. In genere, i criminali si impossessano di un controller di dominio, compromettono le credenziali, quindi riescono ad individuare e crittografare il backup per impedire all'operatore di ripristinare i servizi bloccati.

Il movimento laterale è fondamentale per il successo di un attacco. Se il malware non riesce ad espandersi oltre il punto di approdo, è inutile, pertanto, la prevenzione dal movimento laterale è essenziale. Le funzionalità di visibilità e segmentazione presenti in una soluzioni come Akamai Guardicore Segmentation consentono di impostare rapidamente le policy necessarie per prevenire e contenere una violazione iniziale. Inoltre, gli utenti vengono avvisati in caso di movimenti laterali e altri comportamenti sospetti in modo da rilevare tempestivamente il malware per poter reagire immediatamente.

Parte 1. Come spezzare la kill chain del ransomware: prevenzione e mitigazione dei rischi

Il ransomware non si diffonde violando un singolo computer o dispositivo. I criminali informatici utilizzano il ransomware per crittografare il maggior numero possibile di sistemi su una rete per assicurarsi il pagamento del riscatto.

Poiché il ransomware è un attacco composito, l'implementazione di più livelli di difesa può aiutare a prevenire danni estesi, la perdita di dati e i problemi di downtime. Il primo livello di difesa consiste nel tentare di prevenire l'infezione iniziale del ransomware.

La kill chain del ransomware

1. **Accesso iniziale**
   Phishing (spear) o servizi vulnerabili
2. **Movimento laterale**
   Diffusione sulla rete per il massimo impatto
3. **Esfiltrazione**
   Individuazione e furto di informazioni utili
4. **Crittografia**
   PKI con crittografia per prevenire le violazioni
5. **Richiesta di riscatto**
   Sfondo, e-mail, file . txt sul riscatto, ecc.
6. **Impatto**
   Dati, finanziario, ecc.

Prevenzione dell'infezione iniziale

Le prime aree vulnerabili per qualsiasi rete sono i punti di contatto con Internet. Sebbene molti attacchi ransomware siano basati sullo spear phishing, nulla impedisce loro di violare i servizi esposti a Internet.

Grazie alle funzioni di visibilità presenti in Akamai Guardicore Segmentation, potrete monitorare i servizi esposti a Internet e limitarne l'esposizione tramite apposite policy per:

- Servizi di accesso remoto (RDP, SSH, TeamViewer, AnyDesk, VPN)
- Servizi potenzialmente vulnerabili (Apache, IIS, Nginx)
- Computer potenzialmente vulnerabili (rilevati i computer con un sistema operativo senza patch tramite la funzione aggiuntiva Insight)
- Servizi esposti indesiderati (database, controller di dominio, server web interni o file server)

Come spezzare la kill chain con la segmentazione

È inevitabile che una rete venga violata a un certo punto. Ciò potrebbe accadere a causa dello spear phishing, di un errore umano o di un server su cui viene eseguito un servizio vulnerabile che non è stato mitigato correttamente. Ecco perché è fondamentale disporre di adeguate strategie di mitigazione del rischio.

Quando un computer viene violato, è necessario limitare la propagazione all'interno della vostra rete. Potete eseguire questa operazione in tre modi:

1. La segmentazione tramite l'isolamento delle applicazioni

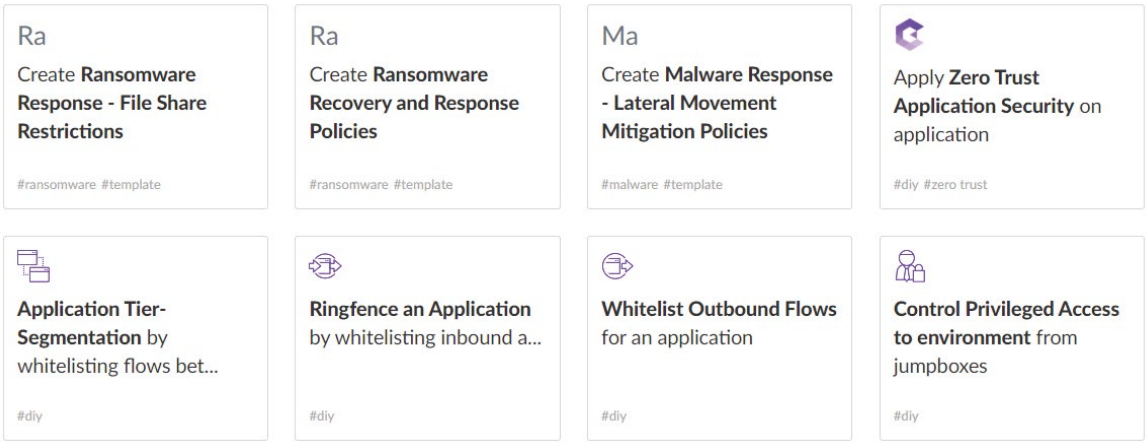
Separate la rete in segmenti operativi, in base all'applicazione, all'utilizzo o all'ambiente, e non consentite a tali segmenti di connettersi tra uno e l'altro o al loro interno se non è necessario.

Ecco di seguito quattro linee guida da considerare:

- Bloccate qualsiasi comunicazione tra laptop/workstation.
- Bloccate la comunicazione dai processi in esecuzione con "potenti" privilegi di utenti di dominio, come gli amministratori.
- Limitate gli utenti che possono eseguire i processi sui vostri server.
- Limitate l'accesso da laptop/workstation a server di data center e istanze cloud.

Akamai Guardicore facilita la protezione della rete dai ransomware. Con i modelli predefiniti, potete mitigare gli attacchi impostando apposite policy in tre semplici passaggi:

1. **Selezionate il vostro obiettivo,** ad esempio delimitare un'applicazione critica, creare policy di mitigazione del ransomware o proteggere una directory attiva.
2. **Identificate le risorse rilevanti da proteggere,** come le risorse delle applicazioni di e-commerce che state cercando di delimitare, tutti i carichi di lavoro di Active Directory nel data center o gli endpoint da proteggere dalla diffusione del ransomware. Questo passaggio, in molti casi, viene eseguito automaticamente dall'etichettatura IA di Akamai.
3. **Proteggete le risorse creando apposite policy.** L'IA di Akamai Guardicore Segmentation suggerisce e consiglia automaticamente le policy basate sul traffico reale nell'ambiente e apprende i modelli di comunicazione delle applicazioni tramite centinaia di reti.

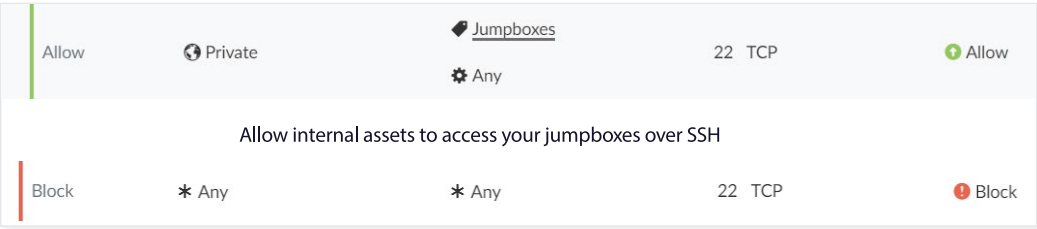


Esempio: Modelli di Akamai Guardicore Segmentation

2. Prevenzione del movimento laterale con regole di restrizione del protocollo

Esistono linee guida generali per protocolli e comportamenti specifici. Alcuni protocolli vanno accuratamente limitati visto il loro uso intrinseco nelle normali operazioni quotidiane. Akamai Guardicore Segmentation crea una visualizzazione di tutto il traffico per creare le regole più accurate per il vostro ambiente basate su protocolli ad alto rischio, come WinRM, SMB, RPC, RDP e SSH.

Ad esempio, mentre il protocollo SSH è utile per l'amministrazione remota e serve a rendere sicuri altri protocolli (come sFTP), è anche uno strumento utilizzato dai criminali per la violazione dei computer e la propagazione nella rete. È consigliabile limitare il più possibile il protocollo SSH a livello di rete creando jumpbox per gli utenti autorizzati.



Regole create in Akamai Guardicore Segmentation

3. Protezione dei backup e dei servizi di dati critici

Per massimizzare i danni, gli attacchi ransomware, di solito, prendono di mira i server di backup dell'organizzazione per crittografare i dati archiviati e non risparmiano i servizi di dati e i file server.

L'utilizzo di Akamai Guardicore Segmentation consente non solo di limitare l'accesso a server di backup, database e file server, ma anche di ridurre l'accesso esterno ad aree specifiche della rete. Per ridurre al minimo la comunicazione da e verso i server di backup critici, potete utilizzare Akamai Guardicore Segmentation per delimitare le applicazioni e bloccare la comunicazione da e verso un'applicazione fino ai livelli di processo e utente. Limitare l'esposizione dei servizi di dati solo al minimo operativo consente di ridurre il fattore di rischio per tali servizi e mitigare l'esposizione al ransomware e i percorsi di propagazione.

Parte 2. Rilevamento e risposta al ransomware

Per contrastare le minacce informatiche, come il ransomware, è fondamentale adottare un avanzato livello di pianificazione e vigilanza. Se si reagisce rapidamente ad una violazione, è possibile ridurre al minimo i danni alla rete. Akamai Guardicore Segmentation include funzionalità che possono aiutarvi sia con il rilevamento che con la risposta alle minacce.

Rilevamento delle minacce con Akamai Guardicore Segmentation

Tra i tipi di incidenti, figurano i seguenti:

- **Frode**: rileva e intercetta tentativi di movimento laterale sospetti e li reindirizza ad honeypot dinamici per consentire di monitorare e analizzare le loro azioni. Vengono forniti dati dettagliati sulle attività dannose e sulla successiva fase di attacco del criminale informatico.
- **Scansioni di rete**: i criminali informatici raccolgono le informazioni una volta penetrati all'interno della rete, utilizzando le scansioni di rete come metodo di ricognizione per rilevare porte o servizi aperti in ascolto da parte di altri server. Akamai Guardicore Segmentation rileva automaticamente le scansioni di rete e avvisa immediatamente gli utenti.
- **Rilevamento basato su policy**: l'adozione di policy di sicurezza a livello di rete e processi consente il riconoscimento immediato delle comunicazioni non autorizzate e del traffico non conforme.

Akamai Guardicore Segmentation presenta la funzione Insight

Akamai Guardicore Segmentation può fornire visibilità sulle singole risorse sfruttando una funzione aggiuntiva basata su OSquery. Utilizzando il modello di query fornito, la soluzione riesce a rilevare rapidamente attività anomale, come la copia shadow del volume, l'azione di pre-crittografia più comune del ransomware. Inoltre, la soluzione è in grado di rilevare i trojan utilizzati per distribuire il ransomware mediante la ricerca di una comune tecnica di hollowing che nasconde il malware in svchost.exe, un processo legittimo di Windows.

Ricerca delle minacce gestita

Il servizio gestito di ricerca delle minacce di Akamai Hunt avvisa gli utenti di qualsiasi comportamento anomalo rilevato all'interno della loro rete tramite tecniche come l'analisi delle connessioni Internet in entrata e in uscita e del relativo GeoIP associato, la ricerca di nuovi file eseguibili con una crescente presenza sulla rete, che può indicare la propagazione, e l'analisi delle connessioni delle risorse alla ricerca di indicazioni di movimento laterale tramite anomalie nel numero dei router adiacenti.

Risposta immediata

Dopo aver rilevato nella rete una minaccia, come un ransomware, potete implementare rapidamente appropriate misure di mitigazione tramite l'adozione di policy a livello di processi e utenti per impedire e isolare attivamente il verificarsi di attività dannose.

Visibilità incrementale delle infezioni

A partire da un primo indizio o segnale di compromissione (IOC), potete iniziare a cercare ulteriori indicatori, come modelli di comunicazione, processi, porte utilizzate, risorse infette e altro ancora. Akamai Guardicore Segmentation può aiutarvi ad individuare tutte le risorse che presentano questo indicatore (tutte le risorse che comunicano con C2, tutte le risorse che comunicano ad una porta univoca o tutte le risorse che eseguono un processo dannoso). Inoltre, con una mappa visiva del vostro ambiente, potete cercare altre similitudini tra computer infetti o tracce di propagazione.

Parte 3. Disinfezione e ripristino

Quando si dispone di un elenco di tutti i computer e degli indicatori di compromissione, potete iniziare la disinfezione. Dividete i computer in tre gruppi: **Isolati**, **Monitorati** e **Puliti**.

Isolati

- Risorse **infettate** dal malware
- Mantenete tali risorse in **quarantena** fino alla rimozione del malware

Monitorati

- Le risorse potrebbero essere **infette** o meno
- **Monitorate** finché non siete sicuri che il malware sia stato **rimosso**

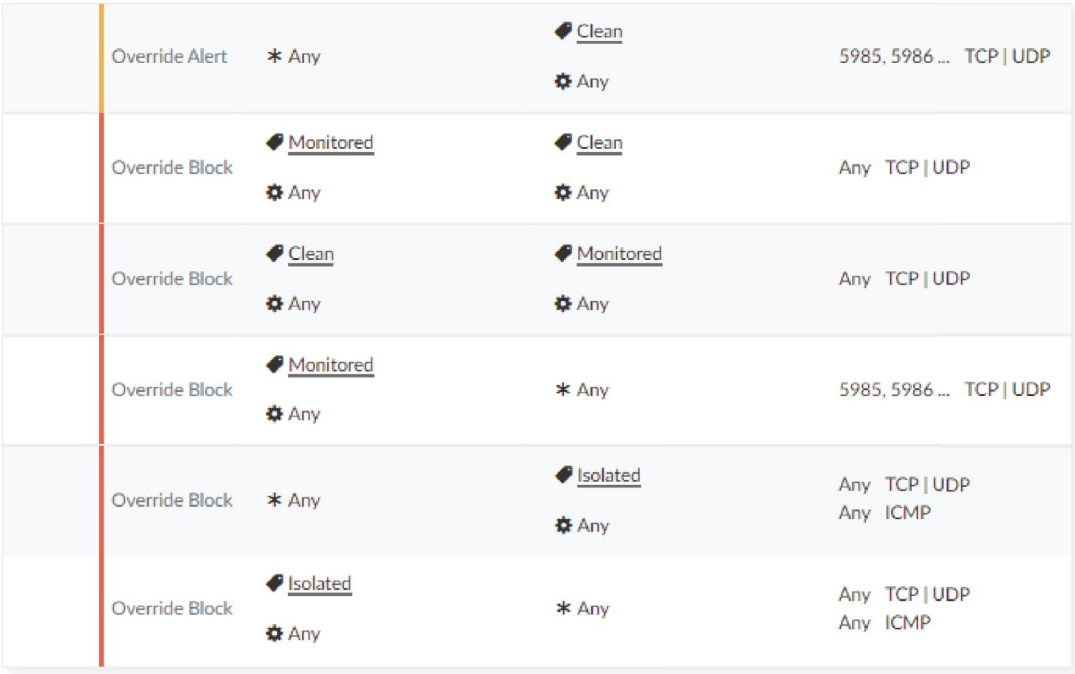
Puliti

- Le risorse sono state verificate come **non infette** e possono **funzionare normalmente**

Linee guida di segmentazione per il ripristino

Dopo aver impostato i tre gruppi, potete iniziare ad aggiungere policy appropriate per segmentare la vostra rete creando quattro livelli di comunicazione:

- **Bloccate** tutte le comunicazioni in entrata e in uscita da computer **isolati**.
- **Bloccate** la comunicazione del protocollo di gestione remota da e verso i computer **monitorati**.
- **Inviate avvisi** relativamente a qualsiasi comunicazione del protocollo di gestione remota ai computer **puliti**.
- **Bloccate** tutte le comunicazioni tra i gruppi.



	Override Alert	✱ Any	Clean Any	5985, 5986 ... TCP | UDP
	Override Block	Monitored Any	Clean Any	Any TCP | UDP
	Override Block	Clean Any	Monitored Any	Any TCP | UDP
	Override Block	Monitored Any	✱ Any	5985, 5986 ... TCP | UDP
	Override Block	✱ Any	Isolated Any	Any TCP | UDP Any ICMP
	Override Block	Isolated Any	✱ Any	Any TCP | UDP Any ICMP

Regole di blocco e avviso in Akamai Guardicore Segmentation

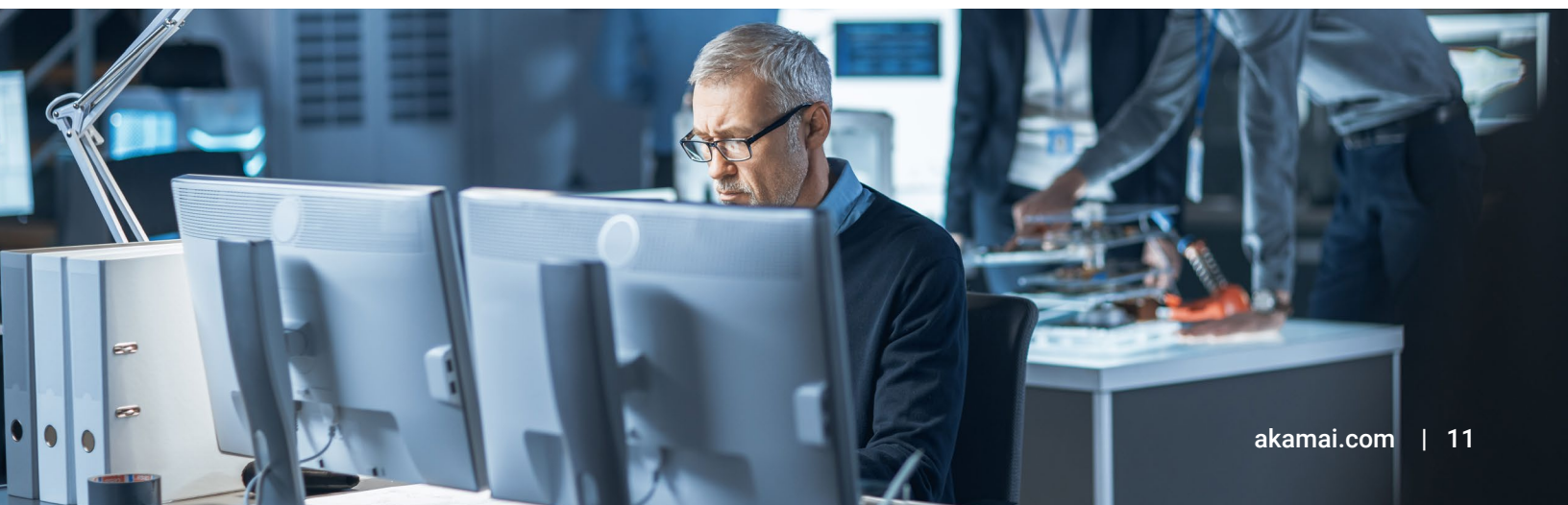
Modello di risposta e ripristino dal ransomware

Il modello delle policy di risposta e ripristino dal ransomware incluso in Akamai Guardicore Segmentation fornisce una policy predefinita di facile utilizzo per limitare l'accesso tramite i gruppi **Isolati**, **Monitorati** e **Puliti**.

Questo modello vi consentirà di mantenere facilmente la continuità operativa dei computer **puliti** senza temere il rischio di venire (re)infettati dai computer **isolati**.

Conclusione

Se vi affidate ancora a un firewall tradizionale o a un sistema di difesa solo del perimetro, non potete impedire al ransomware di diffondersi nella rete e bloccare le applicazioni e le infrastrutture critiche. La realtà è che le violazioni sono inevitabili e dovete tenervi pronti. Akamai Guardicore Segmentation può aiutarvi a rilevare le minacce presenti nel traffico est-ovest del data center e a bloccare il movimento laterale da cui dipende il ransomware per crittografare e prendere in ostaggio le vostre risorse più critiche.



5 passaggi per mitigare l'impatto di un attacco ransomware con Akamai Guardicore Segmentation

Preparazione con l'identificazione di tutte le applicazioni e le risorse in esecuzione nel vostro ambiente IT.

Prevenzione con la creazione di regole tali da bloccare le tecniche di propagazione dei ransomware più comuni.

Rilevamento con l'invio di avvisi nel caso di un tentativo di accesso alle applicazioni e ai backup segmentati.

Risoluzione dei problemi con l'avvio di misure automatiche di contenimento e messa in quarantena delle minacce quando viene rilevato un attacco.

Ripristino con funzionalità di visualizzazione che supportano strategie di ripristino in più fasi.

Bloccate il movimento laterale dei ransomware nella rete. Non ci credete? Scopritelo da soli. akamai.com/guardicore

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 05/23.