SONICWALL

LE CARATTERISTICHE RICHIESTE DAGLI AMMINISTRATORI PER UNA SOLUZIONE DI SICUREZZA DEGLI END POINT

Una nuova prospettiva sulle sfide per la sicurezza degli end point

Abstract

Gli amministratori devono affrontare le sfide poste dai prodotti per la sicurezza degli end point. Questo brief esamina alcune di queste sfide continue, tra cui:

- Manutenzione e applicazione della sicurezza
- Minacce crittografate e avanzate
- Avvisi e remediation

Introduzione

La gestione e la sicurezza degli end point sono fondamentali nell'odierno ambiente in costante evoluzione della criminalità informatica. Gli utenti finali si connettono continuamente all'interno e all'esterno della rete con i propri dispositivi end point. Al tempo stesso, questi end point costituiscono il campo di battaglia del panorama delle attuali minacce. Sempre più spesso, le minacce crittografate riescono a raggiungere gli endpoint senza controllo, il ransomware è in aumento e il furto di credenziali procede silenziosamente. Tuttavia, la sempre crescente minaccia posta dal ransomware e gli altri attacchi basati su malware hanno dimostrato che le soluzioni di sicurezza dei client non possono essere misurate solo in base alla compliance degli end point.

Le sfide della sicurezza degli end point

I prodotti per la sicurezza degli end point sono sul mercato da anni, ma gli amministratori hanno difficoltà a:

- Mantenere aggiornati i prodotti per la sicurezza
- Applicare policy e compliance
- Ottenere rapporti
- Minacce provenienti da canali crittografati
- Comprendere gli avvisi e i passaggi di remediation
- Gestire le licenze
- Fermare le minacce avanzate come il ransomware

Mantenere aggiornati i prodotti per la sicurezza

Gli amministratori devono assicurarsi che gli end point gestiti eseguano la versione corretta dei componenti del software di sicurezza installati, come richiesto dalla policy di compliance.

Per contrastare gli attacchi emergenti, gli amministratori della sicurezza della rete necessitano di end point gestiti per valutare la situazione in cui si trova la sicurezza e per segnalarne lo stato in modo continuo.

Alcuni amministratori hanno la necessità di fermare il traffico est-ovest che attraversa i propri data center, che spesso può costituire la maggior parte del traffico che passa per gli switch. Inoltre devono poter disporre della possibilità di mettere in quarantena un dispositivo in locale, nel caso in cui esca dalla compliance o venga infettato. In questi casi, il firewall deve bloccare l'accesso a Internet ed escludere il dispositivo dalla LAN, limitando quindi i percorsi di rete alle stesse posizioni di quarantena messe in atto dal firewall.

Inoltre, gli amministratori della sicurezza devono garantire che tutti i dati scambiati tra il client unificato e la console di gestione centralizzata non possano essere manomessi durante il transito, al fine di garantire l'integrità dei dati.

Applicare policy e compliance

Se lo stato degli end point li pone al di fuori della policy, gli amministratori devono essere in grado di impedire al dispositivo end point di utilizzare i servizi UTM per far passare il traffico attraverso il firewall. Inoltre, anche gli utenti finali svolgono un ruolo importante nella sicurezza degli end point, svolgendo il loro lavoro su laptop aziendali e altri end point. Gli utenti devono sapere immediatamente se sono stati rilevati eventuali software o comportamenti maligni, in modo che possano intervenire o aprire un ticket, se necessario.

Ottenere rapporti

In alcuni casi, gli amministratori possono gestire più firewall, ma i loro utenti sono configurati in un unico pool, e devono essere in grado di ottenere un Single Sign-On (SSO) da qualsiasi amministratore firewall o console di gestione della sicurezza per gestire le policy dei client. Al tempo stesso, i regolamenti di compliance impongono spesso che tutti i ruoli amministrativi rispettino il principio del privilegio minimo, in modo che la gestione unificata dei client disponga di un adeguato controllo degli accessi basato sui ruoli per l'accesso privilegiato. Ad esempio, il sistema potrebbe limitarsi a due ruoli, uno con accesso in lettura/scrittura e l'altro in sola lettura.

Minacce provenienti da canali crittografati

Con l'aumento del numero di applicazioni Web protette tramite canali crittografati come HTTPS e con il ricorso alla crittografia anche da parte del malware per aggirare l'ispezione basata sulla rete, è diventato indispensabile abilitare la Deep Packet Inspection del traffico SSL/TLS (DPI-SSL). Tuttavia, questa soluzione non è facilmente applicabile senza un'implementazione di massa di certificati SSL/TLS affidabili su tutti gli end point per evitare problematiche che impattano sull'esperienza dell'utente e sulla sicurezza. È quindi necessario un meccanismo di base per distribuire e gestire i certificati e il modo in cui i browser si fidano di essi.

Comprendere gli avvisi e i passaggi di remediation

In genere gli utenti finali sono meno consapevoli dei rischi per la sicurezza rispetto ai professionisti e, in quanto tali, sarebbe necessario che la piattaforma di sicurezza utilizzata sugli end point li avvisi in caso di cambiamento del profilo di rischio mentre si spostano con il proprio laptop in luoghi diversi e consigliando loro come rimanere protetti.

Ad esempio, un client unificato o un software di terze parti potrebbe generare un avviso oppure fornire il reindirizzamento a una fonte esterna, ad esempio una pagina Web.

Per rimediare rapidamente a qualsiasi problema di compliance con le policy aziendali, sia per gli utenti finali che per l'IT può essere utile dare agli utenti finali l'accesso ad informazioni con cui porre rimedio ai problemi in autonomia. Se il dispositivo di un utente non rientra nella policy e l'utente viene messo in quarantena, gli utenti devono avere anche indicazioni sulle azioni da adottare per ripristinare la compliance.

Gestire le licenze

Gli amministratori devono assicurarsi che qualsiasi software di sicurezza degli end point acquistato venga automaticamente aggiornato alla loro interfaccia di gestione, in modo che possano mantenere correttamente la licenza per gli end point. Ad esempio, tutte le informazioni sulle licenze relative a un cliente devono essere monitorate e archiviate a livello centrale. In caso di acquisto di una nuova licenza, è necessario inviare un segnale alla gestione centralizzata dei client unificati per avvisare e autorizzare alla titolarità del software.

Sulla base di una pianificazione periodica, alcuni amministratori hanno la necessità di redigere report di compliance per tutte le licenze di terze parti implementate per pagare i propri partner.

Fermare le minacce avanzate come il ransomware

Gli approcci tradizionali possono talvolta lasciare a desiderare in merito al soddisfacimento dei requisiti amministrativi. L'approccio basato su firme, adottato a lungo dalle tecnologie antivirus tradizionali, ha fallito di fronte al ritmo con cui vengono sviluppati i nuovi malware e alle loro tecniche di evasione, portando alla luce la necessità di un approccio diverso per la protezione dei client. Tale approccio deve non soltanto fornire motori avanzati di rilevamento delle minacce, ma anche supportare una strategia di difesa stratificata sugli end point.

Una delle principali limitazioni delle attuali soluzioni a punto (note come *enforced AV client*) sta nel fatto che lo sviluppo è specifico per una data terza parte ed è stato quindi integrato nelle offerte di tale terza parte. Gli amministratori necessitano di un modello più aperto, che consenta un'aggiunta relativamente rapida di moduli di sicurezza aggiuntivi se richiesto dall'azienda o dal settore.

Conclusione

A causa della crescita nell'utilizzo degli end point come vettori di attacchi informatici, i professionisti della sicurezza devono adottare misure per proteggere i dispositivi end point. Inoltre, con il proliferare del telelavoro, della mobilità e del BYOD, si riscontra un estremo bisogno di fornire una protezione coerente per qualsiasi client ovunque si trovi.

Gli amministratori della sicurezza devono valutare soluzioni per gli end point tenendo conto delle esigenze del mondo reale.

Per saperne di più. Leggete il nostro Brief sulle soluzioni «Sicurezza degli endpoint su misura per le aziende» oppure visitate il sito www.sonicwall.com/capture-client.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul potenziale utilizzo di questo materiale, contattare:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com