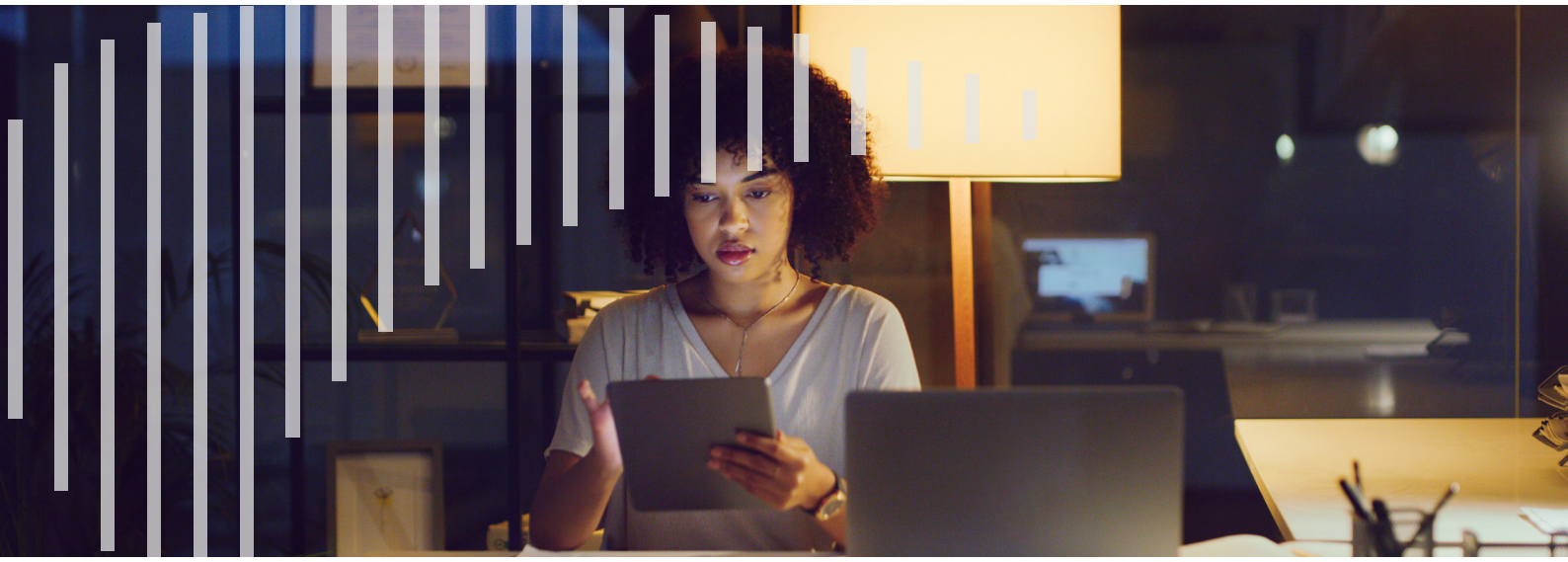

NOTA SINTETICA

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 documento esamina alcune di queste sfide continue, tra cui:

- Manutenzione e applicazione della sicurezza
- Minacce crittografate e avanzate
- Gestione degli avvisi e procedure di risoluzione
- Creazione di policy e manutenzione
- Visibilità sullo stato dei tenant
- Vulnerabilità non corrette da patch

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 per le attuali minacce. Sempre più spesso le minacce crittografate riescono a raggiungere gli endpoint in modo incontrollato, il ransomware è in aumento e il furto di credenziali procede silenziosamente. La crescente minaccia posta dal ransomware e da altri attacchi basati su malware ha dimostrato che l'efficacia delle soluzioni di sicurezza dei client non è misurabile solo in termini di compliance degli end point.

Queste sfide si aggravano quando si tratta di gestire più tenant, sia all'interno di un'unica azienda che per diversi clienti. Ciò richiede spesso policy e configurazioni diverse basate su gruppi di utenti, dispositivi e posizione.

Le sfide della sicurezza degli end point

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

- mantenere aggiornati i prodotti per la sicurezza
- applicare policy e misure di compliance Web
- creare report e gestire gli accessi
- rilevare le minacce provenienti da canali crittografati
- capire gli allarmi e le procedure di risoluzione
- gestire le licenze
- fermare le minacce avanzate come il ransomware
- sapere dove si nascondono le vulnerabilità critiche
- conoscere lo stato dei tenant e gestire policy globali

Mantenere aggiornati i prodotti per la sicurezza

Gli amministratori devono assicurarsi che sugli endpoint gestiti sia installata la versione corretta dei componenti del software di sicurezza in uso, come previsto dalla policy di conformità.

Per contrastare gli attacchi emergenti, gli amministratori della sicurezza di rete necessitano di end point gestiti per valutare costantemente il livello di sicurezza e ottenere aggiornamenti sul loro 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 non sia più conforme 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, per assicurare l'integrità dei dati, i responsabili 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.

Applicare policy e misure di compliance Web

Se lo stato di un end point non è conforme alle 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 hanno 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 vengono rilevati eventuali software o comportamenti dannosi, in modo da poter intervenire o richiedere assistenza in caso di necessità.

Per il personale che lavora fuori dall'ufficio è possibile applicare le policy aziendali sull'utilizzo del Web mediante un filtro web o di contenuti integrato nella soluzione di sicurezza. È inoltre essenziale bloccare l'accesso a siti dannosi noti ed eventualmente bloccare siti web che comportano una perdita di produttività come pure materiale per adulti. Se gli utenti scaricano video attraverso i server aziendali tramite la VPN, può essere opportuno limitare la larghezza di banda per i siti web ad alto consumo di dati.

Creare report e gestire gli accessi

In alcuni casi gli amministratori possono gestire diversi firewall, ma i loro utenti sono configurati in un unico pool, quindi devono essere in grado di ottenere un single sign-on (SSO) dall'amministratore di ogni firewall o console di gestione della sicurezza per gestire le policy dei client. Al tempo stesso, le normative di conformità impongono spesso che tutti i ruoli degli amministratori rispettino il principio del privilegio minimo, per cui la gestione unificata dei client dovrebbe disporre 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 l'ispezione deep packet del traffico SSL/TLS (DPI-SSL). Tuttavia, senza un'installazione capillare di certificati SSL/TLS affidabili su tutti gli endpoint, questa soluzione non è facilmente applicabile senza pregiudicare l'esperienza dell'utente e la sicurezza. È quindi necessario un meccanismo di base per distribuire e gestire i certificati e il modo in cui i browser possono ritenerli affidabili.

Capire gli allarmi e le procedure di risoluzione

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

Per rimediare rapidamente a qualsiasi problema di compliance con le policy aziendali, sia per gli utenti finali che per l'IT può essere utile fornire agli utenti 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, questo utente deve anche ricevere indicazioni sulle azioni da adottare per ripristinare la conformità.

Gestione delle licenze

Gli amministratori devono assicurarsi che ogni software di sicurezza degli end point acquistato venga automaticamente aggiornato dalla loro interfaccia di gestione, in modo che tutti gli end point dispongano di una licenza corretta. 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.

Alcuni amministratori devono redigere periodicamente dei 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 rispetto 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 ridefinite le tecniche di evasione, evidenziando la necessità di un approccio diverso per la protezione degli endpoint. Tale approccio deve non soltanto fornire motori avanzati per il rilevamento delle minacce, ma anche supportare una strategia di difesa degli end point su più livelli, inclusa l'integrazione con un ambiente sandbox.

Una delle principali limitazioni delle attuali soluzioni dedicate (note come enforced AV client) sta nel fatto che lo sviluppo è specifico per un determinato fornitore e viene quindi integrato nei suoi prodotti. Gli amministratori necessitano di un modello più aperto, che consenta un'installazione relativamente rapida di moduli di sicurezza aggiuntivi se richiesto dall'azienda o dal settore.

Non sapere dove si nascondono le vulnerabilità critiche

Con la forte crescita delle applicazioni aziendali è aumentato in modo esponenziale anche il rischio di vulnerabilità delle applicazioni. Nel solo 2019 è stato rilevato un gran numero di vulnerabilità con punteggi CVSS critici superiori a 9.0, causando violazioni e numerosi problemi agli amministratori IT. Le aziende hanno bisogno di un metodo per quantificare e classificare le vulnerabilità, in modo da poter creare un piano per l'applicazione di patch o la disinstallazione di applicazioni a rischio.

Conoscere lo stato dei tenant e gestire policy globali

Molte grandi organizzazioni hanno la necessità di gestire un gran numero di endpoint oppure la sicurezza degli endpoint in diverse regioni, gruppi di utenti o tipi di dispositivi – o entrambi i casi. La loro probabilità di successo dipende dalla rapidità con cui riescono a creare un nuovo tenant e dalla

capacità di monitorare lo stato di salute dei tenant mediante un pannello di controllo globale. In queste situazioni, gli amministratori devono avere la possibilità di modificare rapidamente una policy globale per diversi tenant e gruppi. Per gli MSSP e gli MSP è inoltre importante poter creare delle policy personalizzate per i tenant che non sono interessati da modifiche alle policy globali. La funzione di gestione dovrebbe fornire loro statistiche di alto livello su infezioni e vulnerabilità, senza la necessità di analizzare in dettaglio ogni singolo tenant.

Conclusioni

A causa del crescente utilizzo degli end point come vettori di attacchi informatici, i professionisti della sicurezza devono adottare misure per proteggere i dispositivi end point. Inoltre, con la diffusione del telelavoro, si riscontra un estremo bisogno di fornire una protezione coerente per qualsiasi client ovunque si trovi.

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

Per saperne di più. Leggete il nostro documento "Sicurezza degli endpoint su misura per le aziende" oppure visitate il sito www.sonicwall.com/capture-client.

SonicWall

SonicWall fornisce soluzioni di cybersecurity illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni, visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

ExecBrief-WhatAdminNeed-A4-VG-3575