
NUTANIX
YOUR ENTERPRISE CLOUD
SICUREZZA
incentrata
sulle
applicazioni

Indice

Figura 1
Fonte https://www.breachlevelindex.com/. Il numero di violazioni della sicurezza aumenta ogni mese. I criminali informatici stanno prendendo di mira dati preziosi con attacchi sofisticati progettati per superare i controlli basati sul perimetro. Una volta all'interno della rete aziendale, gli aggressori sono liberi di spostarsi da un sistema all'altro alla ricerca di informazioni sensibili o collegate all'identità personale. Queste violazioni possono passare inosservate per settimane o addirittura mesi.

Lo stato della sicurezza del data center

Lo stato della sicurezza al giorno d'oggi può essere riassunto con un **più**. Più violazioni della sicurezza. Minacce più sofisticate. Più rischio informatico. Più tecnologie business-critical. Più requisiti normativi. Più crescita. Più complessità. E nessuno di questi problemi sembra destinato a diminuire.

Nel frattempo, il data center continua a evolversi a un ritmo sempre più rapido mentre le organizzazioni IT lottano per adempiere alla propria missione e rispondere alle esigenze aziendali in altrettanto rapida evoluzione. L'adozione del Software-as-a-Service, dell'infrastruttura basata su cloud e della virtualizzazione aumenta la complessità del datacenter ma appiattisce l'architettura IT, rendendo più semplice per gli aggressori spostarsi lateralmente in questi pool di risorse e più difficile per i team IT sapere dove posizionare i controlli di sicurezza.

Gli approcci alla sicurezza faticano a tenere il passo coi rapidi cambiamenti che stiamo vivendo. Le organizzazioni continuano a utilizzare metodi più tradizionali di protezione dell'ambiente IT con particolare attenzione all'infrastruttura, per esempio implementando la segmentazione della rete tramite firewall perimetrali. La sicurezza basata sul perimetro protegge tradizionalmente l'ambiente solo dalle minacce esterne, e può essere difficile sfruttarla per limitare il traffico interno o prevenire attacchi a diffusione laterale.

È tempo di un nuovo approccio che consideri la necessità delle organizzazioni di proteggere il traffico che ha luogo dietro il firewall perimetrale con una tecnica in grado di offrire di più: più agilità. Più flessibilità. Più sicurezza. Più protezione. Questo è esattamente ciò che le organizzazioni IT ottengono quando adottano un approccio alla sicurezza incentrato sulle applicazioni grazie alla microsegmentazione.

"I dati sono una risorsa pervasiva che travalica i confini tradizionali on-prem e nei servizi cloud. Ogni azienda ha bisogno di una strategia di sicurezza incentrata sui dati che dia priorità ai dataset per mitigare i crescenti rischi aziendali causati dalle leggi sulla protezione dei dati e sulla privacy, dall'hacking, dalle frodi e dal ransomware".

- Gartner - Hype Cycle for threat-gacing Technologies, 2018

Policy di sicurezza basate sulle applicazioni

L'architettura delle applicazioni è cambiata radicalmente negli ultimi cinque-dieci anni. Le applicazioni si sono evolute, passando dall'esecuzione su un singolo server a una raccolta astratta di macchine virtuali (VM) e servizi di distribuzione delle applicazioni quali SaaS, microservizi e container. Per complicare ulteriormente le cose, tali servizi e VM potrebbero non essere tutti eseguiti dalla stessa posizione. Gli approcci tradizionali richiedono principalmente che le policy siano scritte in termini di rete (per esempio, un indirizzo IP), e nel datacenter dinamico di oggi questo tipo di requisito rende la gestione delle policy un processo ricorrente e problematico.

La buona notizia è che il predominio della virtualizzazione nei datacenter e nel cloud potrebbe essere d'aiuto. Per sua natura, una piattaforma di virtualizzazione comprende tutte le macchine virtuali e il modo in cui sono connesse alla rete indipendentemente da eventuali modifiche alla distribuzione o alle configurazioni. Quando sfrutti quella conoscenza della rete, la policy di sicurezza diventa qualcosa che può essere automatizzato, e il passaggio alla definizione della sicurezza in termini di applicazione anziché di endpoint di rete ha senso. È qui che entrano in gioco la microsegmentazione e la policy incentrata sulle app.

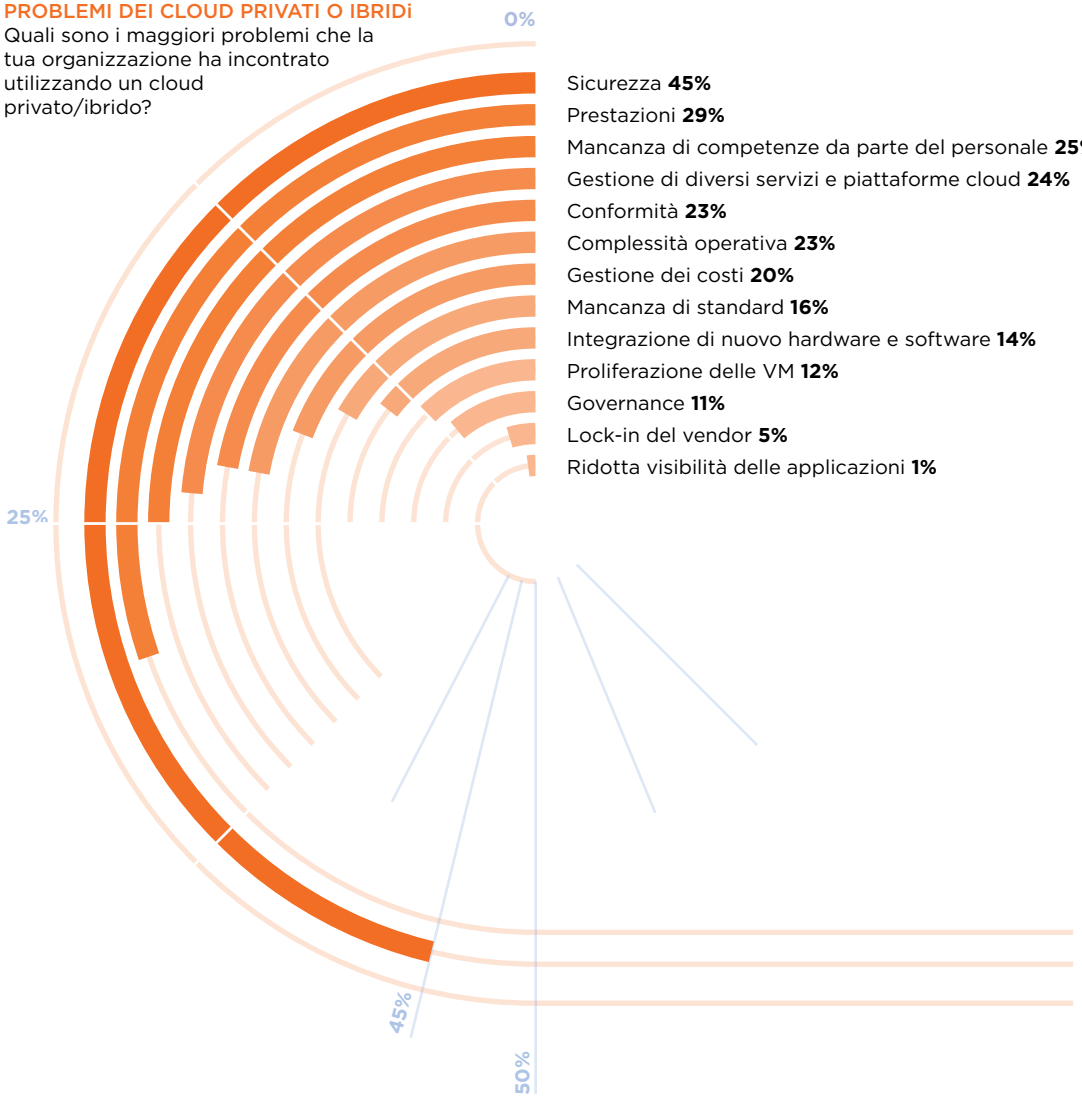
Quando diciamo "incentrata sulle app" intendiamo spostare l'attenzione dalle singole VM e dalla loro identità di rete alle applicazioni stesse. Questa segmentazione basata sull'applicazione scardina la policy dalla rete, semplificando l'amministrazione e la gestione delle policy. I criteri di sicurezza sono associati a gruppi logici o categorie di macchine virtuali, utilizzati per definire applicazioni e livelli di applicazioni (server web, database, livelli intermedi), o gruppi di isolamento (collaudo e sviluppo vs produzione). Dopo che l'applicazione è stata assegnata a un gruppo o una categoria, la policy associata segue la VM ovunque. Il layer di virtualizzazione rileva le modifiche alla rete e aggiorna le regole di conseguenza. I criteri, inoltre, vengono applicati automaticamente quando viene eseguito il provisioning delle macchine virtuali e quando viene modificata la configurazione di rete, lo stato dell'alimentazione, o quando avviene una migrazione, eliminando in questo modo l'onere del change management.

La sicurezza incentrata sulle app offre alle organizzazioni IT un nuovo approccio alla gestione delle policy di sicurezza, e in questo modo aiuta ad affrontare molte delle difficoltà che le organizzazioni IT incontrano al giorno d'oggi. Il resto di questo eBook esamina queste difficoltà e il modo in cui la sicurezza incentrata sulle app può affrontarle per permettere un ambiente applicativo più sicuro.

PROBLEMA:

Le organizzazioni affrontano rischi crescenti in fatto di sicurezza informatica

PROBLEMI DEI CLOUD PRIVATI O IBRIDI
Quali sono i maggiori problemi che la tua organizzazione ha incontrato utilizzando un cloud privato/ibrido?



- Sicurezza **45%**
- Prestazioni **29%**
- Mancanza di competenze da parte del personale **25%**
- Gestione di diversi servizi e piattaforme cloud **24%**
- Conformità **23%**
- Complessità operativa **23%**
- Gestione dei costi **20%**
- Mancanza di standard **16%**
- Integrazione di nuovo hardware e software **14%**
- Proliferazione delle VM **12%**
- Governance **11%**
- Lock-in del vendor **5%**
- Ridotta visibilità delle applicazioni **1%**

I criminali sanno che i grandi data center aziendali contengono informazioni preziose. Ciò ha dato origine ad attacchi più frequenti e altamente mirati su quei dati. Quando viene impiegata una tecnica di sicurezza perimetrale o anche una basata su zone più ristrette, un malintenzionato deve solo sconfiggere alcuni "muri di sicurezza" prima di potersi muovere liberamente alla ricerca di ulteriori obiettivi. In poche parole, l'approccio alla sicurezza basato sul perimetro è obsoleto e non può impedire i movimenti laterali di un attacco informatico. Non solo la sicurezza perimetrale non riesce a bloccare le minacce avanzate che si diffondono da un sistema all'altro, ma non riesce nemmeno ad adattarsi facilmente per proteggere gli ambienti IT dinamici di oggi. Le organizzazioni hanno bisogno di un modo per proteggere le applicazioni e prevenire la propagazione delle minacce di rete garantendo al contempo la capacità di distribuire, migrare e gestire le applicazioni alla velocità necessaria per le aziende.

SOLUZIONE:

La microsegmentazione riduce il rischio

"La natura sempre più dinamica dei carichi di lavoro dei data center rende complessa, se non impossibile, l'applicazione delle strategie di segmentazione tradizionali. Inoltre il passaggio alle architetture di microservizi per applicazioni ha anche aumentato la quantità di traffico da server a server e complicato ulteriormente la capacità dei firewall fissi tradizionali di fornire questa segmentazione".

- Gartner - Hype Cycle for Threat-Facing Technologies, 2018

La microsegmentazione, a volte chiamata firewall da server a server ("East-West"), è la creazione di policy di rete granulari tra applicazioni e servizi. L'implementazione della microsegmentazione è una parte fondamentale di una strategia di difesa approfondita contro le attuali minacce dei data center, in grado di offrire il livello di difesa più avanzato oltre i tradizionali firewall perimetrali. La microsegmentazione essenzialmente riduce il perimetro di sicurezza a un recinto attorno a ciascun servizio o macchina virtuale. La recinzione può consentire solo la comunicazione necessaria tra i tier di applicazione o altri confini logici, rendendo così molto difficile la diffusione delle minacce informatiche da un sistema all'altro. Perciò la compromissione di un piccolo perimetro non espone automaticamente altri obiettivi.

Incentrare la microsegmentazione sulle applicazioni semplifica ulteriormente le operazioni di sicurezza grazie alla capacità di definire policy di alto livello senza bisogno di dettagli sull'infrastruttura sottostante o sugli identificatori di rete. La policy si concentra sui tier o sui gruppi di applicazioni e su quali tipi di comunicazione sono consentiti. Questa è una distinzione importante, in quanto separa la policy e i gruppi da identificatori di rete più dinamici quali gli indirizzi IP. Ciò riduce significativamente la complessità tipica della gestione delle policy. La responsabilità di comprendere la connettività dell'infrastruttura o della rete passa dagli esseri umani autori delle policy alla piattaforma di virtualizzazione, che conosce sempre le informazioni necessarie per aggiornare di conseguenza le policy in modo automatico.

In teoria gli autori delle policy dovrebbero incorporare la policy di sicurezza a livello di applicazione senza alcuna modifica alla configurazione di rete esistente, senza complicare le cose e consentendo ad amministratori e architetti di concentrarsi sulle necessità aziendali o delle app, non sull'infrastruttura di rete. L'eliminazione della dipendenza o dell'impatto sulla rete fisica esistente elimina anche la necessità di modificare o rielaborare il progetto fisico. Di conseguenza il tempo necessario per implementare le policy di sicurezza si riduce drasticamente.

PROBLEMA:

Mancanza di comprensione delle applicazioni e di conoscenza del dominio

"La visibilità è la chiave per difendere qualsiasi risorsa preziosa. Non si può proteggere l'invisibile. Maggiore è la visibilità che si ha della rete dell'ecosistema aziendale, migliori sono le possibilità di individuare rapidamente i segni rivelatori di una violazione in corso e di fermarla. Oggi molte aziende non riescono a rilevare una violazione in corso per settimane, persino mesi, e sono incapaci di limitare il danno".

- Forrester, The Eight Business And Security Benefits Of Zero Trust

La virtualizzazione del data center, le architetture di rete e le applicazioni che supportano sono complesse. Non è più possibile comprendere facilmente come le applicazioni vengono distribuite o come comunicano semplicemente facendo due passi nel data center e tracciando i cavi. Le moderne applicazioni possono comprendere più server fisici e macchine virtuali. In alcuni casi le applicazioni potrebbero non essere in esecuzione nel proprio datacenter. Di conseguenza, le organizzazioni non hanno idea di come i sistemi e l'hardware si connettano fisicamente o attraverso una rete. I problemi dovuti a una mancanza di visibilità vengono alla luce quando si considerano gli approcci tradizionali alla creazione delle policy: blacklisting e whitelisting. Quando si utilizza l'approccio di blacklist, l'autore della policy consente la maggior parte delle comunicazioni (default allow) e tenta di bloccare il traffico pericoloso o indesiderato. Questo approccio è semplicemente poco pratico, dato il volume di nuovi attacchi che bombardano giornalmente le reti dei data center.

Un approccio migliore alla gestione delle policy è quello del whitelisting. Chi scrive le policy blocca tutto il traffico (default deny) e quindi crea policy per consentire le comunicazioni richieste tra utente e applicazione. Nel moderno data center, tuttavia, il whitelisting è un compito arduo. Perché sia efficace, i proprietari delle applicazioni devono avere un'idea molto chiara delle comunicazioni delle loro applicazioni. Con l'avvento delle architetture di servizio e dei microservizi, questa conoscenza può essere divisa tra più team, rendendo molto più difficile l'implementazione di questo tipo di di soluzione.

SOLUZIONE:

Portare visibilità e contesto alla creazione delle policy

"La visibilità è importante per creare un livello generale di sicurezza che sia solido. Investire in soluzioni di visibilità e scoperta è un'opportunità per ridurre i rischi legati alla sicurezza informatica. Tuttavia oltre la metà degli intervistati (55%) afferma che le proprie organizzazioni non comprano questo tipo di soluzioni. Inoltre la mancanza di visibilità su dati, applicazioni e piattaforme è il motivo per cui molte aziende sono preoccupate per la sicurezza dei cloud sia pubblici che privati".

- Ponemon, Separating the Truths from the Myths in Cybersecurity, 2018

Fai luce sui misteri della creazione delle policy di rete. Consenti ai proprietari delle policy di visualizzare le interazioni discrete tra diverse entità all'interno dell'applicazione, permettendo loro di capire esattamente come ogni parte di un'applicazione comunica con le altre. Chiunque dovrebbe essere in grado di osservare la visualizzazione e capire quali VM e servizi sono coinvolti nella consegna di un'applicazione e quale infrastruttura fisica viene utilizzata per eseguire quei server. Una volta capito questo, gli autori delle policy possono essere certi di implementare le migliori policy per quelle specifiche applicazioni e quei servizi.

La visibilità completa elimina le supposizioni dalla scrittura delle policy. La creazione di criteri per il traffico consentito diventa un processo semplice e ripetibile. Assicura l'applicazione delle policy appropriate e riduce gli errori che potrebbero influire sulla disponibilità o sulla sicurezza delle applicazioni. Il rilevamento automatico delle comunicazioni tra VM e la visualizzazione del traffico e delle relazioni delle applicazioni riducono la necessità di conoscere il dominio dell'applicazione. Gli autori delle policy possono crearne automaticamente in base alla visualizzazione in tempo reale delle comunicazioni tra applicazioni e VM senza una vasta conoscenza del dominio dell'applicazione. Infine, la visibilità facilita la risoluzione dei problemi e la risposta agli incidenti poiché le organizzazioni IT possono vedere la causa principale dei problemi di prestazioni e disponibilità.

PROBLEMA:

Soddisfare gli standard e i requisiti di conformità alle normative

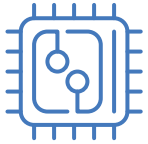
I 5 PIÙ IMPORTANTI SETTORI INDUSTRIALI CHE SUBISCONO VIOLAZIONI DEI DATI

Studio sul costo della violazione dei dati nel 2018: Panoramica globale, Ponemon Institute LLC, sponsorizzato da IBM Security, luglio 2018

Servizi finanziari

Produzione industriale

Servizi



Tecnologia

Vendita al dettaglio

Le organizzazioni IT devono far fronte a un elenco sempre crescente di conformità e standard normativi, tra cui l'Health Insurance Portability and Accountability Act (HIPAA), il Sarbanes-Oxley Act (SOX), il Regolamento generale sulla protezione dei dati dell'Unione europea (GDPR) e il Payment Card Industry Data Security Standard (PCI-DSS). La mancata osservanza degli standard necessari e dei requisiti di conformità normativa può comportare multe salate, azioni legali o interruzioni delle attività di audit governativi. A complicare ulteriormente le cose, la spesa delle pratiche di sicurezza obbligatorie da parte della attività di conformità normativa possono apparire in contraddizione con gli obiettivi aziendali o con la necessità di ridurre i costi e aumentare l'efficienza e i profitti.

Gli autori delle policy sono chiamati a implementare controlli laddove i requisiti di conformità lo impongono, nel modo meno complesso e più efficiente possibile. Se vi si aggiunge la complessità di molte applicazioni moderne, questo passaggio può diventare un problema difficile da risolvere. Per esempio, se uno standard impone l'implementazione di controlli per i sistemi di produzione che contengono dati dei clienti ma non devono essere applicati a server di test/sviluppo, chi scrive le policy dovrebbe avere la possibilità di fare esattamente questo, e basta. Una pratica comune per rispondere all'esigenza di questo tipo di segmentazione è quella di creare delle "isole" di infrastrutture dedicate in base a specifiche aree di conformità. Questa segmentazione può ridurre l'ambito dei controlli di sicurezza, ma non aiuta a contenere i costi né a ridurre i carichi di gestione. Le moderne infrastrutture on-prem possono essere progettate per raggiungere analoghe economie di scala rispetto alle offerte di cloud pubblico; l'introduzione della segmentazione fisica elimina questi vantaggi.

SOLUZIONE:

Semplificare la conformità alle regole

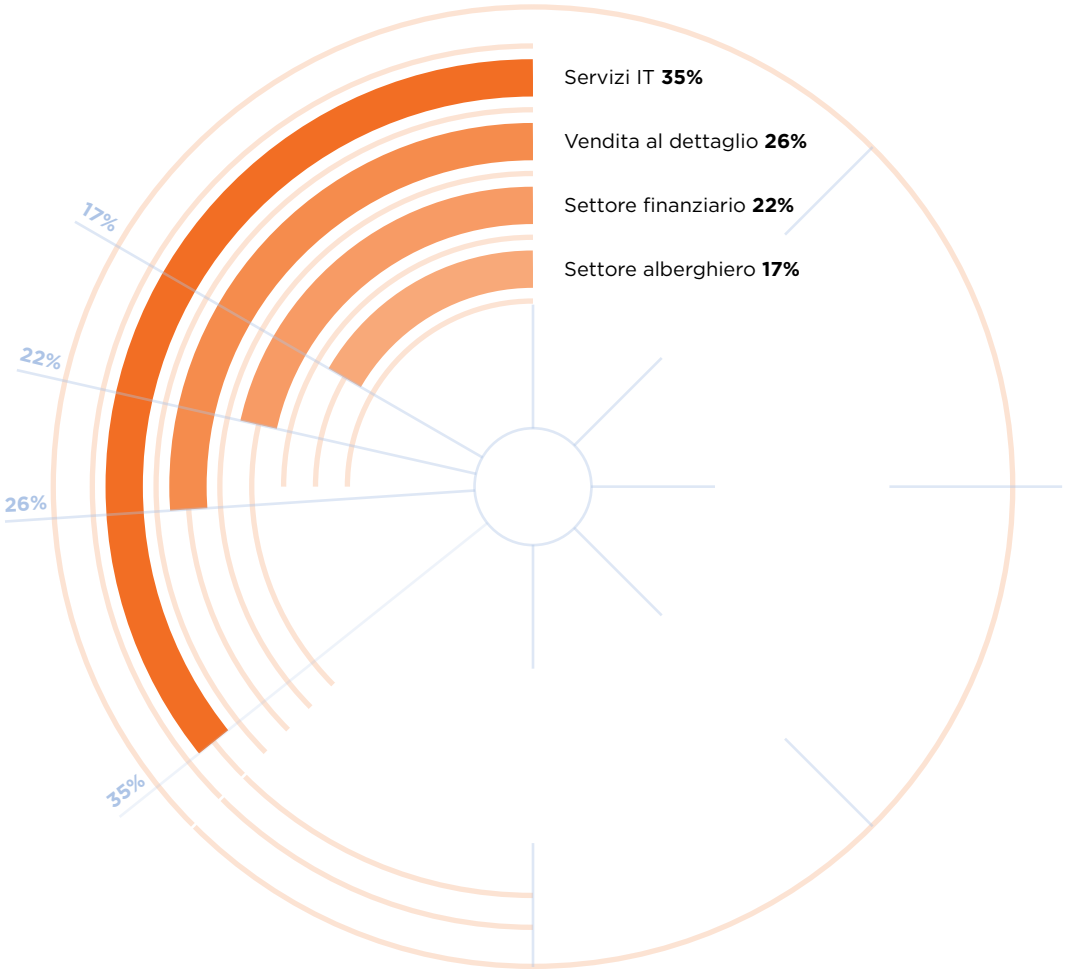


Figura 2
Verizon, Rapporto sulla sicurezza dei pagamenti 2018, https://www.verizonenterprise.com/verizon-insights-lab/payment-security/2018/

La cosa fondamentale in questo caso è passare dai controlli fisici o basati sull'infrastruttura all'utilizzo di policy a livello di applicazione o VM basate su controlli software.

La granularità della sicurezza basata sulle app e definita dal software consente agli autori delle policy di applicare facilmente i controlli di sicurezza in modo estremamente mirato — solo dove sono necessari per soddisfare i requisiti normativi. La granularità può essere a livello di macchina virtuale o comprendere una segmentazione a livello di applicazione. Essendo definiti dal software, questi confini possono essere facilmente ampliati e ridotti, consentendo ai carichi di lavoro regolamentati e non regolamentati di mescolarsi più facilmente utilizzando un'infrastruttura condivisa. Non è necessario creare costose infrastrutture dedicate solo ai fini della conformità alle regole.

Un approccio globale e olistico semplifica anche la gestione della conformità e l'auditing. Si ha la possibilità di astrarre la policy dai dettagli di implementazione dell'infrastruttura, permettendo di semplificare la gestione, l'auditing e la ripetibilità. Anziché esaminare individualmente server e servizi, la policy può essere più completa a livello di applicazione; tutti i servizi membri o VM in un'applicazione sono quindi soggetti alla stessa policy di conformità. Poiché i nuovi servizi o componenti vengono identificati come membri del gruppo di applicazioni, possono essere facilmente aggiunti alla policy generale.

PROBLEMA:

Raggiungere l'agilità in tutta l'organizzazione IT

"Le organizzazioni non possono gestire la complessità sempre crescente tramite processi manuali. La natura della tecnologia, e in particolare della tecnologia basata sul software, implica che una maggiore scalabilità e flessibilità portano naturalmente a una maggiore complessità. Diventa estremamente facile far girare istanze di sistema nel cloud, per esempio, quando è possibile farlo attraverso alcune chiamate API anziché tramite il racking e lo stacking dell'hardware fisico. Mentre la tecnologia scala, tuttavia, la capacità di gestirla attraverso processi manuali non fa altrettanto".

- Forrester, Reduce Risk And Improve Security Through Infrastructure Automation

L'IT è passato dallo svolgere sostanzialmente una attività di back office a essere la chiave delle strategie competitive di molte aziende. Le aziende devono muoversi rapidamente per essere competitive: ciò significa che l'IT deve muoversi ancora più velocemente. La natura dinamica delle applicazioni odierne complica ulteriormente le cose. Lo scale-up o lo scale-down in base alle esigenze aziendali e la possibilità di espandersi rapidamente su infrastrutture di cloud pubblico qualora la domanda superi la capacità in locale è una caratteristica delle applicazioni moderne. Il cloud computing e la virtualizzazione in una certa misura sono stati d'aiuto, consentendo l'automazione di molte attività comuni.

I proprietari delle applicazioni possono eseguire il provisioning di nuove macchine virtuali e servizi con un click. Ma mentre l'automazione semplifica le operazioni sia on-prem che nel cloud, deve estendersi a tutte le discipline delle operazioni del datacenter: infrastruttura, applicazioni, networking e sicurezza. In molti casi la rete e la sicurezza sono state escluse dalle operazioni di automazione e rientrano nell'ambito delle attività lente da svolgere manualmente. L'intervento manuale per modificare una policy di sicurezza o una configurazione di dispositivi fisici comporta il rallentamento esasperato del deployment di applicazioni (provisioning di macchine virtuali, collegamento di storage, distribuzione di software applicativo, connessione in rete, ecc.), che di solito è invece un'operazione automatizzata.

Il processo manuale di configurazione delle porte di uno switch di rete o l'applicazione di criteri di sicurezza statici crea un collo di bottiglia ogni volta che si verifica un cambiamento nell'ambiente, con una maggiore probabilità di errore. L'IT non può permettersi che la rete e la sicurezza costituiscano un collo di bottiglia. Anche rete e sicurezza devono essere automatizzate e diventare una casella da spuntare, non una matassa da districare.

SOLUZIONE:

Automatizzare le operazioni di rete e di sicurezza

I processi convalidati per le modifiche alla policy o alla configurazione dell'applicazione devono essere codificati e automatizzati. La maggior parte delle tecnologie di sicurezza tradizionali è in grado di automatizzare le modifiche alla configurazione, ma poiché questi controlli di sicurezza sono applicati a un macrolivello anziché a livello di applicazione/VM, può essere difficile comprendere quale sia l'impatto di una modifica apportata a un'entità su un'altra che si trova in un ambiente condiviso. Quando le modifiche su infrastruttura, sistemi operativi o altro vengono apportate in assenza dell'impatto sulle applicazioni che si basano su tali elementi, possono verificarsi problemi. Un'automazione efficace richiede anche una nuova attenzione all'applicazione e alle tecnologie di sicurezza che hanno la capacità di applicare controlli allo stesso livello. Ancora una volta, la conoscenza approfondita dell'applicazione o la visibilità completa non sono solo fondamentali per la creazione di policy a livello di applicazione, ma anche per la capacità di automatizzare l'applicazione e per la gestione di tali policy.

LA COMPLESSITÀ CRESCENTE RENDE NECESSARIO L'USO DELL'AUTOMAZIONE

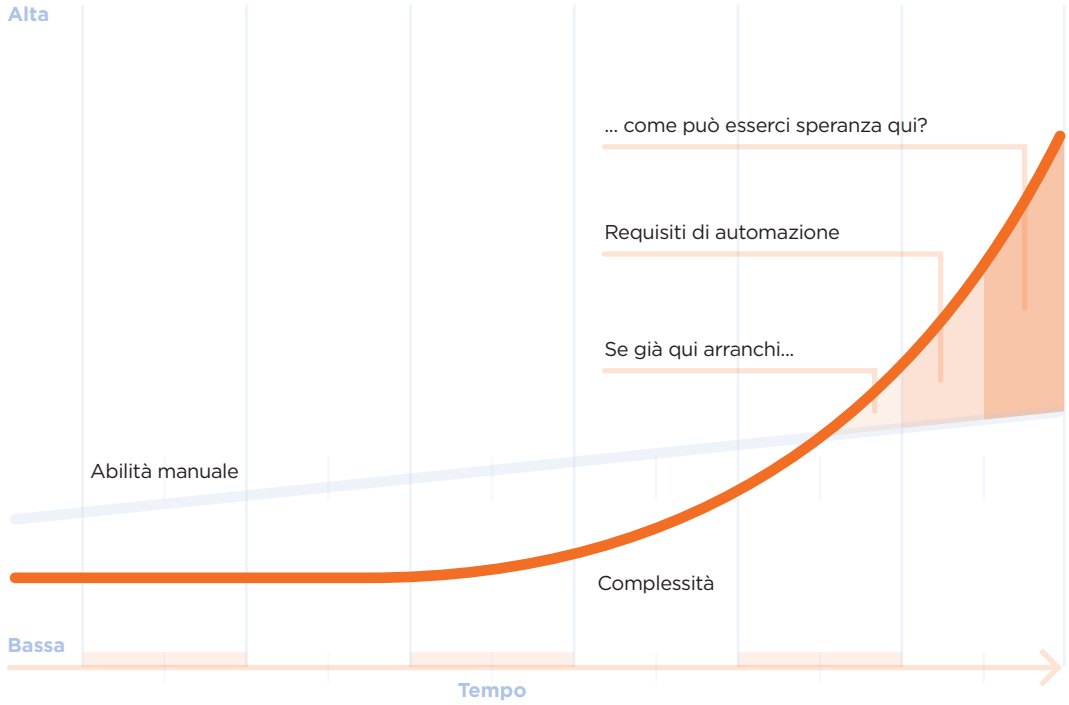
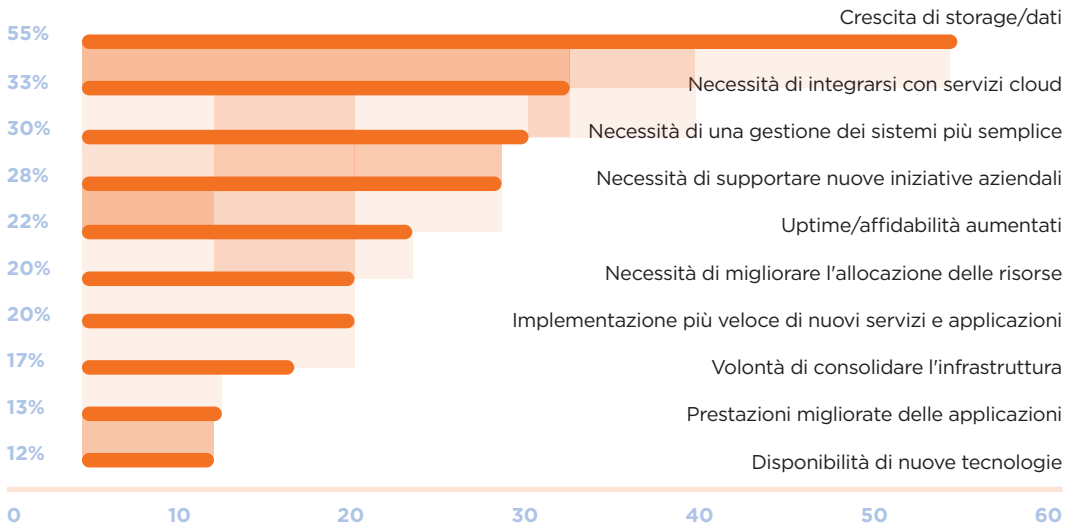


Figura 3
Forrester, Reduce Risk And Improve Security Through Infrastructure Automation, 22 giugno 2018

PROBLEMA:

La complessità dei datacenter porta alla complessità delle policy

COSA STA GUIDANDO IL CAMBIAMENTO DELL'INFRASTRUTTURA IT
Quali sono i tre fattori che determinano il cambiamento maggiore nell'ambiente dell'infrastruttura IT della tua organizzazione?



Nota: sono consentite massimo tre risposte.
Dati: Sondaggio Interop ITX su 200 utenti di cloud computing che utilizzano o intendono utilizzare IaaS, dicembre 2017

La progettazione semplice di un data center e di una applicazione, documentabile con qualche diagramma e un foglio di calcolo, è scomparsa molto tempo fa. I data center stanno diventando sempre più complessi con l'aumentare del numero di fattori che intervengono nella loro creazione e crescita. La complessità è guidata sia dalle tendenze del business, come il mobile computing e dall'analisi dei big data, sia dalle tendenze dell'IT che fanno aumentano ulteriormente la complessità, inclusi virtualizzazione, container, cloud computing, ecc. Tutta questa complessità ha un impatto su efficienza, costi, disponibilità e affidabilità del servizio e, naturalmente, sulla sicurezza.

L'ambito dell'IT era tradizionalmente definito dalle risorse presenti in un data center. Quelle pareti fisiche, insieme a una semplice segmentazione funzionale o per dipartimenti, costituivano un insieme di perimetri facilmente definibili che potevano essere protetti da dispositivi fisici di rete. Questo metodo di implementazione dei dispositivi di sicurezza fisica per creare recinti protettivi attorno a grandi gruppi di risorse IT non è più efficace o pratico in questo ambiente. Imporrebbe l'uso di molti più dispositivi con configurazioni complesse. Sebbene possa essere possibile realizzarlo, sarebbe finanziariamente insostenibile.

La gestione delle policy di rete tradizionali è un compito estremamente complesso perché il gran numero di regole aumenta significativamente la possibilità di una configurazione errata. Inoltre, a causa delle regole scritte a livello di indirizzo di rete, le policy possono diventare rapidamente incomprensibili.

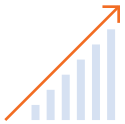
Mentre continua la corsa verso le operazioni ibride e multi-cloud, questo problema di complessità si moltiplica. Gli amministratori sono oberati da policy conflittuali tra cloud pubblico, cloud privato ospitato, data center on-prem ecc., tutte estremamente soggette a errori che portano a vulnerabilità della rete.

SOLUZIONE:

Sfrutta la virtualizzazione e la categorizzazione per ridurre la complessità delle policy

LA COMPLESSITÀ DEL SETTORE E DELLE OPERAZIONI IT È UN RISCHIO SIGNIFICATIVO PER LA SICUREZZA

83%
lamenta una complessità eccessiva



78%
rapida crescita delle risorse di **dati per sito**

76%
integrazione di terze parti nelle reti interne e nelle applicazioni

Ponemon Institute, La necessità di una nuova architettura di sicurezza IT: studio globale, 2017 (The Need for a New IT Security Architecture: Global Study, 2017)

La policy deve essere semplice. A renderla complessa è la necessità di enumerare gli identificatori di rete dei componenti dell'applicazione. In teoria, essere in grado di astrarre quei componenti semplificherà notevolmente il linguaggio delle policy. Questa astrazione trasforma la policy da incentrata sulla rete a incentrata sull'applicazione, per concentrarsi non sulla rete dinamica, ma sulla definizione più statica di ciò che serve a un'applicazione per funzionare. Pensa a tutti gli indirizzi IP e ai dettagli dell'infrastruttura che non confonderanno più la definizione della policy. Le policy diventano leggibili con meno necessità di aggiornamenti a causa di modifiche alla rete o alla posizione. La virtualizzazione consente di compilare dinamicamente gran parte di queste informazioni di rete, semplificando la policy di rete alla sola richiesta dei dettagli per la comunicazione consentita o non consentita tra componenti dell'applicazione o entità esterne.

Questo metodo incentrato sulle app fornisce un modello di policy semplice e intuitivo ideale per i team di virtualizzazione e i proprietari di applicazioni. Le complessità della rete vengono rimosse dal linguaggio delle policy, riducendo la necessità di conoscenza del dominio dell'applicazione. Al contrario, i criteri vengono mappati tramite il tipo di applicazione, la zona di isolamento o altre categorie che diventano i blocchi di costruzione delle policy di sicurezza. Una volta definiti i criteri, l'applicazione e l'esecuzione possono essere gestite contrassegnando le VM o i servizi da includere. Il semplice processo di aggiunta o rimozione dei tag per includere o escludere una VM dalla policy semplifica notevolmente l'applicazione e le attività quotidiane di amministrazione IT.

Conclusione

Il data center di oggi è ormai troppo grande, sotto svariati aspetti, per il tradizionale firewall perimetrale, aumentando così il rischio di una violazione della sicurezza. I controlli di sicurezza devono evolversi per lavorare nell'ambiente IT moderno: un ambiente caratterizzato da rapida crescita, cambiamenti e complessità. Le organizzazioni necessitano di controlli di sicurezza che offrano una protezione granulare capace di andare oltre la tradizionale sicurezza perimetrale per prevenire la diffusione di minacce e proteggere le risorse IT ovunque si trovino.

Con l'enorme aumento dei dati di alto valore archiviati nei data center aziendali, gli attacchi alla sicurezza sono diventati più sofisticati. Recenti violazioni raccontate sui media mostrano come piccole vulnerabilità siano state utilizzate come punto di accesso, diffondendo successivamente un malware sofisticato in tutto il data center. In parte questo genere di situazione può essere attribuita a un progetto antiquato basato sul perimetro. Nella progettazione legacy la segmentazione viene eseguita su una macro-scala che in genere si esaurisce con il datacenter: vale a dire che, una volta che tale difesa viene sconfitta, il malware è libero di diffondersi.

La soluzione è nota da tempo: è la **microsegmentazione**.
La microsegmentazione sposta la sicurezza dal perimetro alla VM o all'applicazione con controlli granulari che limitano la comunicazione CC al minimo richiesto per far funzionare le applicazioni. In un ambiente microsegmentato, la diffusione del malware è notevolmente ridotta se non completamente bloccata.

A impedire un uso diffuso della microsegmentazione sono stati la complessità e i costi di implementazione. Le applicazioni moderne sono complesse; si estendono su più server, sfruttando microservizi e persino servizi condivisi basati su cloud. Il sovraccarico dato dal comprendere, elencare e mantenere la policy per migliaia di end point si è rivelato in moltissimi casi troppo complesso per essere gestito. Con la virtualizzazione moderna e il livello di contesto e visibilità disponibili ora è possibile implementare con successo una strategia di microsegmentazione.

La risposta è la sicurezza incentrata sull'app di Nutanix Flow.

- Aumentare la sicurezza delle applicazioni tramite microsegmentazione
- Isolare gli ambienti senza complessità fisica della rete
- Garantire la conformità alle normative
- Integrare facilmente funzioni di rete aggiuntive di terze parti

Nutanix Flow semplifica la gestione della rete e delle policy con particolare attenzione alle applicazioni, consentendo di governare le applicazioni e gli ambienti indipendentemente dall'infrastruttura fisica. Completamente integrato nella piattaforma Nutanix, Flow offre potenti funzionalità di rete e di microsegmentazione con un'interfaccia di gestione e creazione di policy che consente ai team IT di visualizzare facilmente, ottimizzare e proteggere le applicazioni aziendali più complesse. Per ulteriori informazioni su Nutanix Flow o per visualizzare una demo personalizzata dal vivo con un consulente, visita https://www.nutanix.com/products/flow/.

Riguardo a Nutanix
Nutanix è leader globale nel software cloud e nelle soluzioni di infrastruttura iperconvergente che rende l'infrastruttura invisibile in modo da permettere all'IT di concentrarsi sulle applicazioni e sui servizi ad alto valore aggiunto per la propria attività. Le aziende di tutto il mondo usano Nutanix Enterprise Cloud OS per portare la gestione one-click e la mobilità delle applicazioni su cloud edge pubblici, privati e distribuiti in modo che possano eseguire qualsiasi applicazione su qualsiasi scala con un total cost of ownership (TCO) decisamente inferiore. Il risultato sono organizzazioni in grado di fornire rapidamente un ambiente IT on-demand ad alte prestazioni, offrendo ai proprietari di applicazioni una vera esperienza di tipo cloud.

Scopri di più su **www.nutanix.it** o seguici su Twitter **@nutanix**.

NUTANIX™
YOUR ENTERPRISE CLOUD