
NUTANIX
YOUR ENTERPRISE CLOUD
STAI MODERNIZZANDO LA TUA INFRASTRUTTURA?
Ecco perché
adottare un approccio
INCENTRATO SULLA
SICUREZZA

Indice

INTRODUZIONE:

LA SICUREZZA È UN PROBLEMA DI TUTTI

"Nel 2017 il numero di attacchi informatici è raddoppiato, rendendolo l'anno peggiore di sempre per quanto riguarda le violazioni dei dati e gli incidenti informatici in tutto il mondo. Dal momento che la maggior parte degli incidenti non vengono segnalati, Online Trust Alliance stima che il loro numero effettivo potrebbe superare i 350 000".

Fonte: "Rapporto sugli incidenti informatici e sulle tendenze relative alle violazioni", Online Trust Alliance, 25 gennaio 2018.

Il continuo aumento del numero di attacchi informatici e violazioni dei dati non fa più notizia. Più di tre quarti delle organizzazioni sono state vittima di uno o più attacchi informatici riusciti.

E per quanto riguarda la tua azienda? Fino a che punto la stai proteggendo dalle minacce?

Non smettere di leggere solo perché la tua posizione lavorativa non ha a che fare con la sicurezza. Preoccuparsi delle minacce informatiche non è un compito esclusivo del responsabile della sicurezza informatica e del team di sicurezza: la cybersecurity è una responsabilità di tutti, inclusi i consulenti e i responsabili delle decisioni per l'infrastruttura IT.

Perché? Continua a leggere per scoprire come e perché la scelta dell'infrastruttura influisce sulla capacità di proteggere la tua azienda dalle minacce informatiche. Scoprirai come un'infrastruttura che mette la sicurezza al primo posto può migliorare il tuo livello di sicurezza per proteggere più efficacemente la tua azienda dagli attacchi dei cybercriminali di oggi.

[1] "Rapporto 2018 sulla difesa dalle minacce informatiche", CyberEdge Group, 2018.

LA TUA ORGANIZZAZIONE SARÀ LA PROSSIMA?

77%

DELLE ORGANIZZAZIONI HA SUBITO UNO O PIÙ ATTACCHI INFORMATICI RIUSCITI

Fonte: "Rapporto 2018 sulla difesa dalle minacce informatiche", CyberEdge Group, 2018.

45%

DI AUMENTO DELLE VIOLAZIONI DEI DATI SEGNALATE NEL 2017 RISPETTO AL 2016

Fonte: "Resoconto annuale di fine anno sulla violazione dei dati per il 2017", Identity Theft Resource Center, 2018

14 · 712

VULNERABILITÀ ED ESPOSIZIONI COMUNI (COMMON VULNERABILITIES AND EXPOSURES O CVE) PUBBLICATE DA MITRE NEL 2017

Fonte: "Dizionario delle vulnerabilità ed esposizioni comuni", The MITRE Corporation

$3,86

MILIONI È IL COSTO TOTALE MEDIO DI UNA VIOLAZIONE DEI DATI

Fonte: "Studio 2018 sul costo di una violazione dei dati: panoramica globale", Ponemon Institute LLC, sponsorizzato da IBM Security, luglio 2018.

UN'INFRASTRUTTURA COMPLESSA MOLTIPLICA I PROBLEMI DI SICUREZZA

L'EVOLUZIONE DELLE APPLICAZIONI E DELL'INFRASTRUTTURA – DA LEGACY A VIRTUALIZZATE A NATIVE DEL CLOUD – HA CREATO ULTERIORI LIVELLI DI COMPLESSITÀ E DI RISCHIO.
ECCO PERCHÉ:

DECINE DI VENDOR

Per molte aziende l'infrastruttura di datacenter include uno o più stack tecnologici composti da diverse soluzioni di elaborazione, virtualizzazione, storage e networking. Gli stack a loro volta spesso includono prodotti di vendor differenti.

DECINE DI APPROCCI

Ognuno di questi vendor ha una visione ristretta e frammentata dello stack infrastrutturale – e una visione della sicurezza ancora più ristretta. Un vendor di storage solitamente si concentra sulla sicurezza della propria soluzione di storage, ma non su quella dell'intera infrastruttura. Un vendor di virtualizzazione si concentra solo sulla sicurezza della propria soluzione di virtualizzazione, e così via...

DECINE DI FALLE NELLA SICUREZZA

Questo ambiente complesso genera silos infrastrutturali che scaricano sulla tua azienda la responsabilità di risolvere le falle di sicurezza e le incompatibilità che sorgono tra i vari vendor di componenti. L'onere di garantire una sicurezza infrastrutturale adeguata diventa troppo impegnativo da gestire per la maggior parte delle aziende: semplicemente non ci sono abbastanza esperti di cybersecurity disponibili per aggiornare costantemente il software, correggere le vulnerabilità, confermare le configurazioni di sicurezza ed eseguire altre attività correlate nella complessa infrastruttura IT.

Gli attuali sforzi in termini di cybersecurity non sono sufficienti
L'89% degli intervistati nell'ambito di un sondaggio globale afferma che il proprio livello di cybersecurity non soddisfa pienamente le necessità dell'organizzazione di appartenenza.
Fonte: "La cybersecurity ritrovata: prepararsi ad affrontare gli attacchi informatici", EY, 2017.

QUALE PERIMETRO? PERCHÉ I MODELLI DI SICUREZZA DEVONO EVOLVERSI

Quando il data center era ben definito, statico e costituito principalmente da hardware fisico, la protezione perimetrale era un approccio sensato per proteggere l'azienda dagli attacchi informatici. Tuttavia la virtualizzazione, il cloud computing, i dispositivi mobili e l'Internet of Things hanno tutti contribuito alla dissoluzione del perimetro.

Oggi gran parte del traffico si muove lateralmente all'interno del data center rispetto al traffico in entrata e in uscita dalla rete esterna. Le comunicazioni interne tra macchine virtuali e applicazioni sono spesso invisibili per le soluzioni di sicurezza tradizionali come i firewall. Una volta che i cybercriminali si infiltrano nella rete possono dunque insediarsi e muoversi lateralmente senza essere rilevati.

INFRASTRUTTURA COMPLESSA + APPROCCI TRADIZIONALI ALLA SICUREZZA = AUMENTO DEI RISCHI

- **Falle di sicurezza:** i prodotti infrastrutturali aggiuntivi e le operazioni manuali per implementarli e mantenerli aumentano la complessità senza risolvere tutte le falle nella sicurezza.
- **Ritardi nell'aggiornamento del software:** convalidare e mantenere una baseline di sicurezza durante gli aggiornamenti software richiede molto tempo e spesso implica processi manuali soggetti a errori.
- **Mancanza di alternative praticabili:** sebbene le strategie multiprodotto possano mitigare diverse minacce, in gran parte si sono dimostrate troppo complesse e richiedono troppe risorse per essere funzionali in uno stack infrastrutturale multivendor tradizionale.

Gli errori di sicurezza rappresentano un rischio importante
Gli errori di vario tipo sono stati la seconda causa più segnalata di violazione dei dati, dopo le applicazioni web.

Fonte: "Rapporto 2018 sulle indagini relative alla violazione dei dati", Verizon

Per tutti i motivi elencati – ambiente eterogeneo, complessità, falle di sicurezza, dissoluzione dei perimetri, aggiornamenti manuali del software, eccetera - al giorno d'oggi l'approccio di sicurezza più efficace per il data center parte da una piattaforma sviluppata con una filosofia incentrata sulla sicurezza.

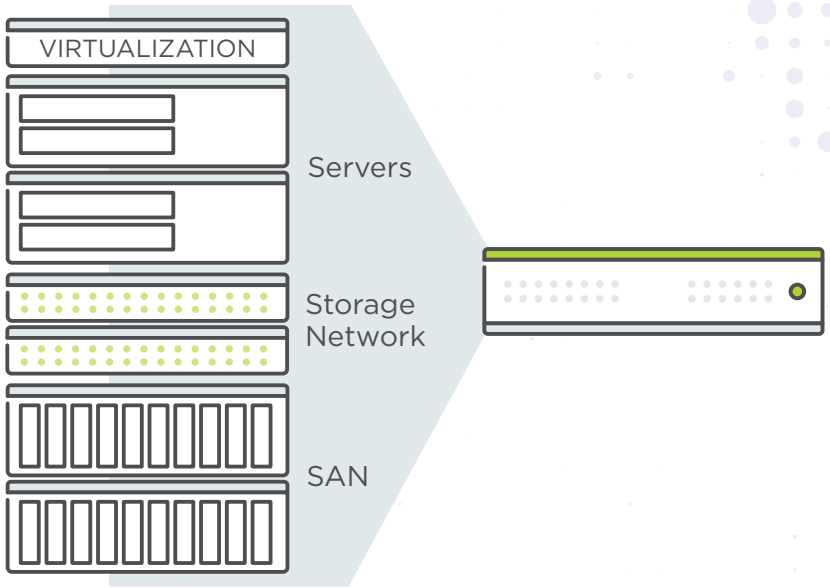
Com'è una piattaforma infrastrutturale incentrata sulla sicurezza?
È una singola piattaforma integralmente testata che mette al centro la sicurezza e la semplicità. Grazie alla combinazione di storage, elaborazione e networking questo tipo di piattaforma è in grado di migliorare la sicurezza e il controllo attraverso:

- Best practice e standard di sicurezza incorporati nell'infrastruttura definita dal software durante l'intero ciclo di vita dello sviluppo
- Funzionalità integrate per la sicurezza e la conformità, che includono il controllo degli accessi in base al ruolo, l'autenticazione a più fattori, la crittografia e altre funzionalità
- Automazione e self-healing per mantenere le configurazioni baseline di sicurezza senza bisogno di interventi manuali
- Un approccio incentrato sulle applicazioni per una maggiore protezione dalle minacce
- Integrazione e supporto di soluzioni di sicurezza di terze parti per una difesa approfondita e un approccio olistico alla sicurezza

Un'infrastruttura che semplifica le operazioni e la sicurezza
Un'infrastruttura iperconvergente (HCI) è definita dal software, non dipende da hardware proprietari e combina storage, elaborazione e networking in un unico sistema per:

- Semplificare notevolmente le operazioni e la sicurezza
- Ridurre il costo totale di proprietà (TCO)
- Accelerare l'agilità e il time to value
- Offrire maggiore scalabilità e prestazioni migliori

LE ORGANIZZAZIONI HANNO BISOGNO DI UN APPROCCIO MIGLIORE ALLA CYBERSECURITY



REQUISITO #1:

CICLO DI VITA DELLO SVILUPPO SOFTWARE 'A PROVA DI BOMBA'

Una singola piattaforma costruita con un approccio incentrato sulla sicurezza può colmare le falle create dalla complessità dei silos infrastrutturali. Per questa ragione le considerazioni sulla sicurezza devono diventare una componente centrale di ogni fase del ciclo di vita dell'infrastruttura – dallo sviluppo e implementazione del prodotto fino al monitoraggio e alla risoluzione dei problemi di routine – e coprire l'intero stack infrastrutturale, inclusi storage, virtualizzazione e gestione.

Se un vendor utilizza un solido ciclo di vita dello sviluppo della sicurezza, quest'ultima viene incorporata nello sviluppo del prodotto fin dall'inizio, evitando difficili compromessi futuri tra sicurezza e prestazioni o funzioni. I team di ricerca e sviluppo, ad esempio, lavorano insieme per comprendere appieno tutto il codice della piattaforma, sia che sia sviluppato in-house o ereditato da dipendenze.

I test per le Common Vulnerabilities and Exposures (CVE) dovrebbero far parte del processo di QA del prodotto. Il vendor dovrebbe pianificare aggiornamenti regolari per affrontare le CVE note per cicli di rilascio minori, così da ridurre al minimo i rischi zero-day senza rallentare l'evoluzione del prodotto.

REQUISITO #2:

BEST PRACTICE E FUNZIONALITÀ DI SICUREZZA INTEGRATE

La sicurezza a livello di infrastruttura con una piattaforma rinforzata aiuta a proteggerti da vari tipi di attacchi informatici, tra cui le violazioni dei dati, gli accessi non autorizzati e altre minacce.

1 **Protezione per i dati a riposo:**
Proteggi da furti o perdite i dati sensibili di utenti e applicazioni con funzionalità di crittografia automatica o crittografia software che soddisfano i requisiti di conformità normativa per il tuo settore, inclusi HIPAA, PCI DSS e altri.

2 **Controllo degli accessi in base al ruolo:**
Limita l'accesso all'infrastruttura e ai dati sensibili utilizzando il controllo degli accessi in base al ruolo, in modo da ridurre il rischio di accessi non autorizzati e soddisfare i requisiti normativi.

3 **Meccanismi di identità e autenticazione:**
impedisci il furto di account e mitiga il rischio che le credenziali vengano compromesse utilizzando meccanismi di autenticazione SAML 2.0 per il single sign-on e l'autenticazione multifattore degli amministratori di sistema. Secondo Neil MacDonald, vicepresidente di Gartner, "come minimo i responsabili della sicurezza informatica dovrebbero rendere obbligatoria l'autenticazione multifattore (MFA) per tutti gli amministratori".[1]

Gli aggressori sono alle porte

Il 73% degli attacchi informatici è perpetrato da estranei, e la metà delle violazioni è perpetrata da membri di associazioni criminali organizzate.

Fonte: "Rapporto 2018 sulle indagini relative alla violazione dei dati", Verizon

[1] "Top 10 dei progetti di sicurezza di Gartner per il 2018", Gartner, 6 giugno 2018.

REQUISITO #3:

AUTOMAZIONE E SELF-HEALING

Data la natura dinamica e complessa dell'attuale panorama tecnologico, è diventato quasi impossibile realizzare adeguate misure di sicurezza con il solo intervento umano. È per questo che l'automazione è diventata una funzionalità indispensabile affinché la cybersecurity sia efficace.

A livello di infrastruttura l'automazione accelera la convalida e gli aggiornamenti del software, limitando significativamente il rischio di abbassare il livello di sicurezza a causa di errori umani. Grazie alle funzionalità di self-healing e automazione integrate in un'unica piattaforma sicura, il processo di aggiornamento di tutti i software di sistema non comporta disservizi e fatica, evitando così che i team IT rinviino le regolari operazioni di aggiornamento.

Per esempio, un'unica soluzione infrastrutturale sicura dovrebbe includere:

- **Convalida automatica delle baseline di sicurezza:** nell'implementare l'infrastruttura e nel proteggerla continuamente da modifiche accidentali o maligne, le baseline di sicurezza (sviluppate in base agli standard del settore e del Dipartimento della Difesa degli Stati Uniti) aiutano i vendor a consolidare l'infrastruttura "dalla fabbrica". Rendere la baseline compatibile con strumenti di valutazione automatizzati accelera il processo di certificazione.

- **Gestione automatica della configurazione:** automatizza il monitoraggio periodico delle modifiche sconosciute o non autorizzate alle configurazioni e lascia che l'infrastruttura risolva le deviazioni dalla baseline in modo automatico per mantenere la conformità.

- **Automazione della rete:** ottimizza e automatizza le modifiche comuni alla configurazione di rete, come la modifiche della configurazione VLAN o delle policy di bilanciamento del carico, in base agli eventi del ciclo di vita delle applicazioni per le macchine virtuali.

Test di adeguatezza alla sicurezza informatica? Fallimentari.
Un sondaggio globale condotto da Forrester Consulting ha valutato le aziende partecipanti in base alla loro prontezza in fatto di cybersecurity (qualità della strategia ed esecuzione) e ha scoperto che il 73% dei partecipanti sono classificabili come novizi della materia, con ancora molta strada da fare prima di raggiungere i livelli degli esperti di sicurezza informatica.

Fonte: "Rapporto Hiscox 2018 sulla prontezza in fatto di cybersecurity", Hiscox.

[2] "Top 10 dei progetti di sicurezza di Gartner per il 2018", Gartner, 6 giugno 2018.

REQUISITO #4:

SICUREZZA INCENTRATA SULLE APPLICAZIONI

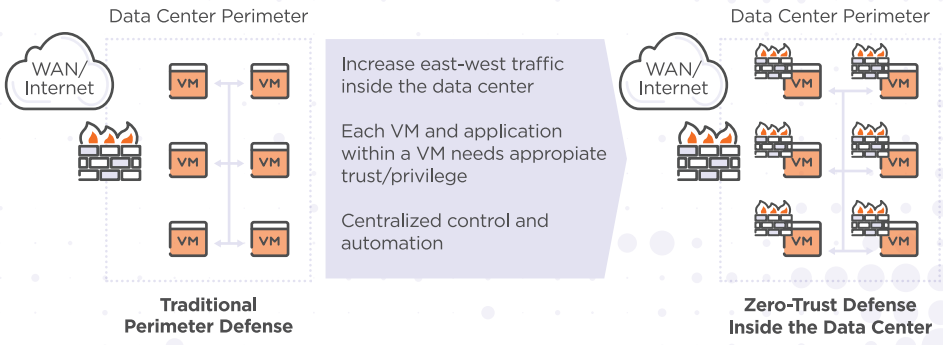
Storicamente l'implementazione della microsegmentazione è sempre stata un'operazione complessa che richiede l'analisi manuale del traffico laterale del data center, la comprensione contestuale di ciascuna applicazione e una lunga mappatura dei flussi di lavoro dell'applicazione per identificare i raggruppamenti logici per la segmentazione. Nonostante i chiari vantaggi di questa best practice per la sicurezza, i problemi causati dall'implementazione della microsegmentazione ne hanno limitato l'impatto e la portata.

La sicurezza incentrata sulle applicazioni in un'unica piattaforma rafforzata riduce in modo significativo la complessità derivante dall'utilizzo della microsegmentazione per proteggersi dalle minacce interne ed esterne non rilevate dai prodotti di sicurezza incentrati sul perimetro. Ecco come:

- **Visualizzazione:** mostrando il traffico, le prestazioni e la disponibilità delle applicazioni hai la completa visibilità e comprensione del comportamento del carico di lavoro, il che ti permette di identificare rapidamente le connessioni logiche e di impostare le policy appropriate in base alle applicazioni.

- **Raggruppamento:** la classificazione delle macchine virtuali e delle applicazioni in base ai casi d'uso, alle esigenze di conformità o alla sensibilità dei dati, anziché in base a identificatori di rete dinamici come gli indirizzi IP, semplifica il processo di protezione e isolamento dei carichi di lavoro e dei dati sensibili.

- **Policy granulare:** i controlli granulari delle policy ti consentono di definire applicazioni multitier e di limitare o consentire il traffico interno in entrata e in uscita dai tier dell'applicazione.



Il modello Zero Trust e la microsegmentazione

Zero Trust è un concetto di sicurezza sviluppato da John Kindervag, ex analista principale presso Forrester Research. L'idea è incentrata sulla convinzione che le organizzazioni non dovrebbero fidarsi automaticamente di tutto ciò che si trova dentro o fuori i propri perimetri: al contrario, dovrebbero invece sottoporre a verifica qualsiasi cosa cerchi di connettersi ai loro sistemi prima di concedere l'accesso.

Una delle funzionalità abilitanti del modello Zero Trust è la microsegmentazione, un modo per creare zone sicure per isolare le applicazioni e i carichi di lavoro e proteggerli individualmente. Applicando le regole della segmentazione al carico di lavoro o all'applicazione, l'IT può ridurre il rischio che un aggressore passi da un carico di lavoro o da un'applicazione compromessa all'altra.

REQUISITO #5:

DIFESA IN PROFONDITÀ TRAMITE I PARTNER DELL'ECOSISTEMA

Ovviamente le misure di sicurezza non dovrebbero limitarsi al livello infrastrutturale. Per evitare falle in questo senso, le singole piattaforme devono integrarsi con soluzioni di sicurezza esterne per creare un approccio olistico e approfondito di difesa.

Ciò richiede che il vendor supporti un solido ecosistema di soluzioni esterne convalidate, come le soluzioni di sicurezza dei dati e degli endpoint. Un modo per integrare la piattaforma infrastrutturale con servizi di terze parti è utilizzare il service chaining delle funzioni di rete.

Cos'è il service chaining? È una funzionalità che ti consente di sfruttare le funzioni di rete virtualizzate di software di terze parti.

Come funziona? I servizi vengono inseriti in linea con il traffico delle macchine virtuali e possono essere facilmente abilitati per tutto il traffico o implementati solo per traffico di rete specifico.

Alcuni esempi? Tra le funzioni di rete comuni che possono essere inserite ci sono: firewall virtuale, rilevamento delle minacce di rete (es. IPS/IDS), monitoraggio delle prestazioni dell'applicazione (APM) o diagnostica generale della rete dell'applicazione.

I 5 SETTORI CHE SUBISCONO PIÙ VIOLAZIONI DEI DATI

"Studio 2018 sul costo della violazione dei dati: panoramica globale", Ponemon Institute LLC, sponsorizzato da IBM Security, luglio 2018.

PARTI DA UNA CHECKLIST DEDICATA ALLA SICUREZZA PER PRENDERE DECISIONI SULLA TUA INFRASTRUTTURA

È evidente che l'infrastruttura IT giochi un ruolo fondamentale nella cybersecurity. Questa è la ragione per cui ogni decisione sull'infrastruttura deve includere la sicurezza quale principio base non negoziabile e non come qualcosa da considerare solo in un secondo momento, né dovrebbe limitarsi al fatto che un fornitore soddisfi o meno un particolare standard. La posta in gioco è alta e le aziende hanno bisogno di ogni strumento possibile per impedire ai cybercriminali di provocare danni.

Nella scelta di una piattaforma infrastrutturale robusta e rinforzata dal punto di vista della sicurezza, insisti sui punti elencati di seguito:

- ✓ Ciclo di vita dello sviluppo della sicurezza full-stack
- ✓ Piattaforma rinforzata pronta all'uso con best practice di sicurezza integrate
- ✓ Convalida automatizzata e self-healing delle baseline
- ✓ Documentazione di sicurezza dettagliata per auditor e architetti dell'infrastruttura
- ✓ Funzionalità di sicurezza incentrate sull'applicazione
- ✓ Ecosistema di sicurezza robusto e in crescita
- ✓ Progettata per soddisfare le certificazioni e gli standard di sicurezza comuni
  - Certificata per i Common Criteria
  - Moduli di crittografia dei dati con convalida FIPS 140-2
  - Conforme a NIST-SP800-131A
  - Supporto per NSA Suite B
  - Conforme a Section 508 VPAT
  - Conforme a TAA

"I leader aziendali e gli stakeholder senior cominciano finalmente a considerare la sicurezza come qualcosa di molto più importante di un semplice aspetto tattico e tecnico portato avanti nel seminterrato dell'azienda da tipi esageratamente seri e incapaci di sorridere. Chi si occupa di sicurezza deve sfruttare questa tendenza lavorando fianco a fianco con i dirigenti aziendali e mostrando chiaramente il collegamento tra i problemi di sicurezza e le iniziative aziendali che potrebbero esserne vittime".

Peter Firstbrook, vicepresidente per la ricerca presso Gartner, in "Gartner identifica le sei principali tendenze in materia di sicurezza e gestione dei rischi", 3 luglio 2018.

PER SAPERNE DI PIÙ

RENDI LA CYBERSECURITY UNA PARTE FONDAMENTALE DELLA TUA PROSSIMA DECISIONE INFRASTRUTTURALE. SCOPRI DI PIÙ SU COME NUTANIX PUÒ AIUTARTI A MIGLIORARE IL LIVELLO DI SICUREZZA DELLA TUA AZIENDA.

RISORSE AGGIUNTIVE:

- Nutanix Flow - www.nutanix.com/products/flow
- Acropolis Platform Security - www.nutanix.com/products/acropolis/security
- Sicurezza e conformità del cloud - www.nutanix.com/products/beam/cloud-security-compliance

Riguardo a Nutanix

Nutanix è un leader mondiale nel campo delle soluzioni di software cloud e di infrastruttura iperconvergente, che rende l'infrastruttura invisibile in modo da permettere all'IT di concentrarsi sulle applicazioni e sui servizi che alimentano il business. Le aziende di tutto il mondo utilizzano il sistema operativo Nutanix Enterprise Cloud per portare la gestione e la mobilità one-click delle applicazioni su cloud edge pubblici, privati e distribuiti, in modo che possano eseguire qualsiasi applicazione su qualsiasi scala con un costo totale di proprietà (TCO) decisamente inferiore. Il risultato sono organizzazioni in grado di fornire rapidamente un ambiente IT on-demand ad alte prestazioni, offrendo ai proprietari delle applicazioni una vera esperienza di stampo cloud.

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

NUTANIX™
YOUR ENTERPRISE CLOUD