NTT DATA
Trusted Global Innovator

Zero Trust Identity

Che cos'è e come implementarlo in 3 step fondamentali

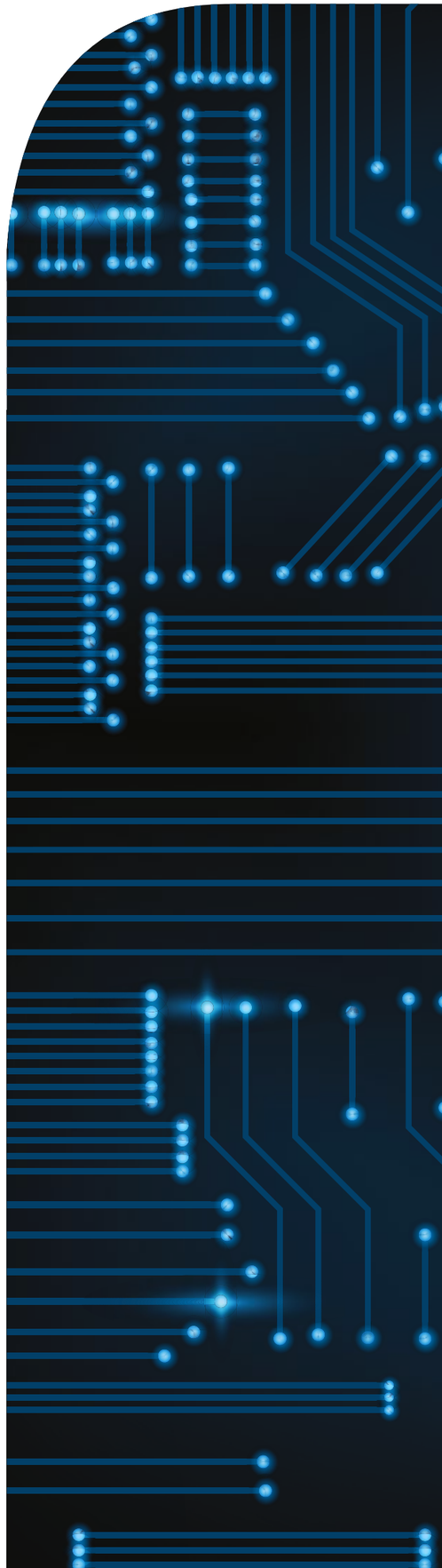
WHITE PAPER / ZERO TRUST

Indice dei contenuti

Abstract

La sicurezza Zero Trust non è un termine o un concetto nuovo. Esiste da tempo e si riferisce a concetti di sicurezza e a un modello di minacce che presuppone non tanto che gli attori, i sistemi o i servizi che operano all'interno del perimetro di sicurezza debbano essere automaticamente affidabili, quanto invece la verifica di tutto ciò che cerca di connettersi prima ancora di concederne l'accesso.

L'avvento "forzato" dello smart working e del lavoro a distanza degli ultimi anni hanno reso prioritarie la comprensione e l'adozione di questo modello di sicurezza per qualsiasi organizzazione che voglia mitigare i rischi legati alla cybersecurity.



Introduzione

L'emergenza della pandemia Covid-19 prima e le tensioni geopolitiche in atto poi hanno contribuito a diffondere il lavoro a distanza e lo smart working anche tra utenti con poca o nessuna formazione in termini di cybersecurity dando il via a una rapida e improvvisa Digital Transformation.

Le forme di lavoro da remoto, nonostante siano alleati efficaci per garantire la continuità aziendale, ampliano la portata delle attività che hanno per oggetto la gestione dei dati, oltre che informazioni e comunicazioni aziendali, costringendo così le aziende stesse e i propri dipendenti a raddoppiare gli sforzi per proteggerle. L'obiettivo è quindi quello di mantenere la riservatezza, l'integrità e la disponibilità di tali dati, affrontando sfide di complessità sempre più ardue.

Il vecchio concetto di perimetro aziendale fisico e ben delineato è stato scardinato dalle circostanze ed esigenze storiche citate. Per decenni, i controlli di sicurezza sono stati costruiti intorno alla protezione di un singolo e massiccio perimetro aziendale fisico. Tuttavia, come si è visto, l'operatività aziendale non è più vincolata alle mura di un ufficio, ma sta sempre più diventando un sistema sinergico di appaltatori, partner, fornitori, sviluppatori, canali di distribuzione e altri soggetti terzi che le aziende utilizzano per supportare le proprie iniziative.

Questa forza lavoro così diversificata e distribuita fa sì che i metodi di protezione perimetrale diventino sempre più inefficaci con il passare del tempo, impedendo ai sistemi di sicurezza aziendali di raggiungere il loro intento principale, che è quello di proteggere i sistemi critici, i dati e gli utenti che permettono alle aziende di operare con successo. Nel momento in cui questo perimetro aziendale viene violato, attraverso ad esempio un attacco di phishing o a causa di un sistema senza patch e protezione, un attore malevolo può muoversi liberamente attraverso tutti i livelli di sicurezza e sistemi, dove i dati sono contenuti e possono essere compromessi.

Smart working, lavoro da remoto, connessioni VPN, utilizzo di dispositivi personali e diversificazione della forza lavoro sono solo alcuni dei driver che portano le aziende ad una sempre più necessaria protezione del perimetro aziendale, non più inteso come perimetro ristretto ma come un ecosistema di dispositivi e utenti distribuiti che rendono l'azienda iperconnessa e iperestesa e costantemente a rischio di minacce, sia interne che esterne.

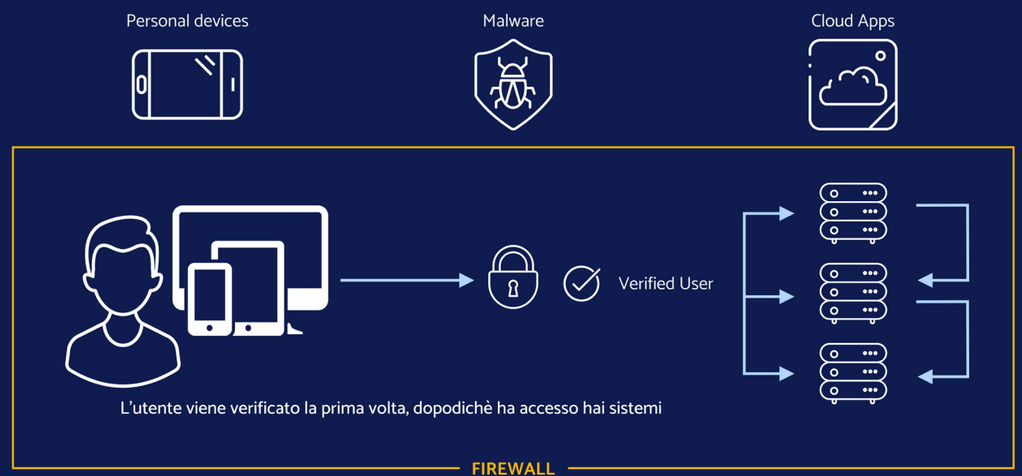
"Hic sunt leones". Una frase ricorrente nelle carte geografiche più antiche per segnalare la presenza di creature amene e mostri. Analogamente l'approccio Zero Trust in ambito cybersecurity ruota attorno all'idea che un'organizzazione non deve fidarsi a priori degli agenti all'interno o all'esterno dei propri confini ("never trust"), bensì verificare tutto ciò che si presenta e cerca di connettersi ai propri sistemi prima di concedere l'accesso ("always verify"). In altre parole una specie di diffidenza positiva che ci faccia procedere sempre con la dovuta prudenza.

Cos’è lo Zero Trust e come si differenzia da un approccio tradizionale

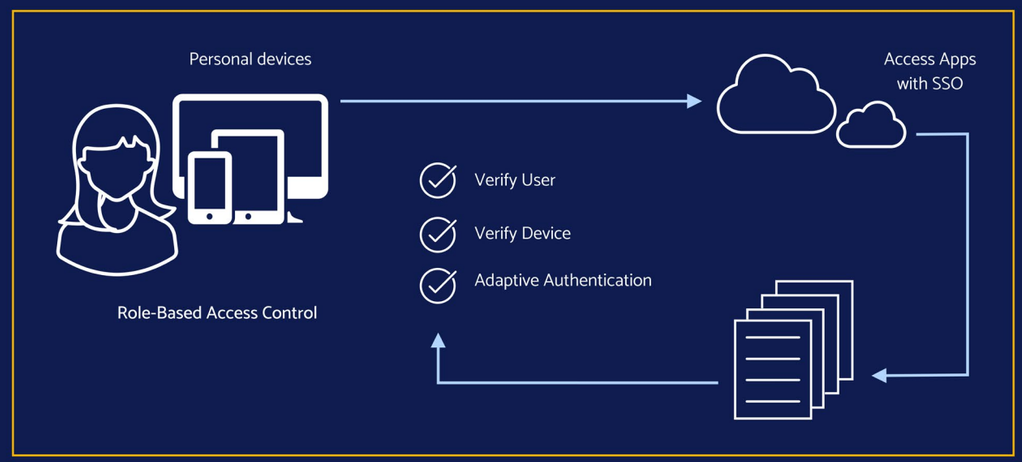
Il termine Zero Trust diventa popolare nel mondo della Cyber Security dopo le analisi portate avanti dai ricercatori di Forrester Research nel 2010, che lo definiscono come un modello alternativo per la gestione della sicurezza IT.

In un ambiente d’ufficio **tradizionale**, la maggior parte delle architetture di sicurezza si basano sul concetto di sicurezza perimetrale che applica certe policy ed è gestita e amministrata all’interno del perimetro aziendale. In poche parole se un utente dispone delle corrette credenziali può accedere a qualsiasi sito, applicazione o dispositivo richiesto anche con movimenti laterali.

Il Trust, e quindi l’approvazione ad operare, si basa sul luogo (che può essere interno o esterno da perimetro) da cui proviene la richiesta stessa di accesso. Se un utente si trova già all’interno del perimetro e quindi ha già passato i controlli di sicurezza presenti ai confini della rete aziendale, allora può muoversi liberamente all’interno della rete senza che vengano effettuati ulteriori controlli circa la sua identità o i suoi privilegi di accesso.



Con un approccio Zero Trust, gli utenti e i loro dispositivi sono verificati al momento dell’autenticazione e durante ogni richiesta di accesso all’applicazione, indipendentemente dal luogo o dalla rete utilizzata.



L'Ecosistema Zero Trust

Un approccio di tipo Zero Trust non dovrebbe essere applicato ad un perimetro limitato, ma al contrario dovrebbe estendersi a tutto il patrimonio digitale dell'azienda e servire come una filosofia di sicurezza integrata e come una strategia *end-to-end*. L'Ecosistema Zero Trust è, quindi, un concetto trasversale a più ambiti ognuno dei quali contribuisce, con i propri controlli e le proprie soluzioni/tecnologie, a raggiungere un livello di maturità sempre più avanzato. Tali controlli non possono dipendere da un singolo attributo per determinare il livello di fiducia; invece, devono continuamente costruire quella fiducia con l'utente ponendo domande come: "Chi sei", "da dove vieni", "cosa stai cercando di fare", "quando stai cercando di farlo". Queste verifiche spaziano inevitabilmente per tutti gli ambiti del panorama digitale in ottica cybersecurity:

- **Identity**: *Secure and Trusted Identity*
  Solo gli utenti autorizzati e i device protetti possono accedere a dati e applicazioni.

- **Network**: *Connect securely from anywhere*
  micro segmentazione e cifratura E2E per impedire l'accesso non autorizzato di device e utenti.

- **Data**: *Be in control of your data*
  I dati devono essere protetti all'interno dell'organizzazione, in transito e quando sono scaricati.

- **Infrastructure**: *Control of your environment*
  aumentare il livello di protezione valutando versioni, configurazioni e usare la telemetria per rilevare attacchi e anomalie.

- **Threat Protection**: *Help stop attacks with integrated and automated security*
  L'intelligenza artificiale può ad esempio essere implementata per automatizzare alcuni processi come il rilevamento delle anomalie e la visibilità dei dati end-to-end.

Zero Trust Identity

I più recenti *framework* e le *best practice* del settore Zero Trust sono tutti allineati su un dato di fatto: l'identità è il nuovo perimetro. È fondamentale garantire che tutti gli utenti che ogni giorno richiedono migliaia di accessi siano effettivamente chi dicono di essere. Mentre le aziende continuano a costruire e perfezionare i loro ambienti di lavoro dinamici e ibridi, hanno sempre più bisogno di un approccio alla sicurezza incentrato sull'identità e sulla gestione efficace degli accessi.

Così facendo le organizzazioni sono in grado di garantire che le persone giuste abbiano il giusto livello di accesso, alle risorse giuste, nel giusto contesto e che l'accesso sia valutato continuamente, il tutto senza aggiungere attrito per l'utente, per il quale i controlli dovrebbero essere trasparenti e veloci.

Questo può essere fatto implementando da una parte una soluzione di Identity e Access Management, e dall'altra implementando un'architettura Zero Trust che pone l'identità al suo centro.

Da dove partire per applicare un approccio Zero Trust Identity

Possiamo identificare 3 step fondamentali per iniziare ad applicare il concetto di Zero Trust Identity in un ambiente reale:

1. Least Privilege e applicazione del need to know

Il concetto di *Least Privilege* è legato allo Zero Trust più di quanto si possa pensare. Per semplificare, si pensi al controllo degli accessi fisici negli uffici: diversi livelli di utenti hanno diversi diritti di accesso, e per ottenere l'accesso a certe aree è necessario spesso fare richiesta ed essere approvati.

Nell'ambito della sicurezza cyber, si utilizza la stessa logica: applicazione del *Role-Based Access Control* (RBAC) per garantire accesso granulare alle risorse privilegiate.

In sostanza, il principio del Least Privilege significa che agli utenti dovrebbe essere consentito di accedere solo alle risorse ed eseguire solo le funzioni necessarie per il loro lavoro. L'accesso ad applicazioni, sistemi, dati e processi dovrebbe essere basato sul Least Privilege per ridurre al minimo l'esposizione ad aree sensibili della rete.
Un problema comune è che a troppi utenti vengono concessi troppi privilegi per facilitare l'utilizzo di sistemi e la consultazione di documenti, ma se le loro credenziali vengono compromesse, allora l'intera organizzazione sarà a rischio. In un ambiente Zero Trust, ad esempio, solo pochi amministratori dispongono di privilegi a livello di dominio e queste credenziali sono strettamente controllate e protette.

2. Micro-segmentazione della rete

Una "zona a traffico limitato" con una rete che permetta il collegamento sicuro delle postazioni di lavoro alla LAN aziendale solo a una selezione di servizi e dati accessibili e visibili solo agli utenti remoti consente di creare zone di sicurezza multiple, stabilire politiche granulari di sicurezza e di controllo degli accessi e isolare specifici workload. La **micro-segmentazione** della rete riduce la superficie di attacco e aiuta a prevenire che gli *hacker* o gli *insider* malintenzionati si spostino lateralmente attraverso la rete per accedere a sistemi e dati sensibili.

Data la natura dinamica della rete, un approccio alla segmentazione software-based è fondamentale.
La segmentazione software-based permette di aggiornare e applicare le policy senza riconfigurazioni manuali dell'hardware - i segmenti sono separati e creati dinamicamente, gestiti centralmente e applicati automaticamente in tutta la rete. Gli utenti sono assegnati a gruppi di policy in modo da poter essere identificati più facilmente e garantire le autorizzazioni appropriate. L'implementazione di un modello Zero Trust Network semplifica i controlli di compliance utilizzando policy granulari per l'accesso ai sistemi e ai dati regolamentati.

3. Context Authentication e Policy Dinamiche

Chi aprirebbe la porta senza guardare prima dallo spioncino e chiedere “Chi è?”.

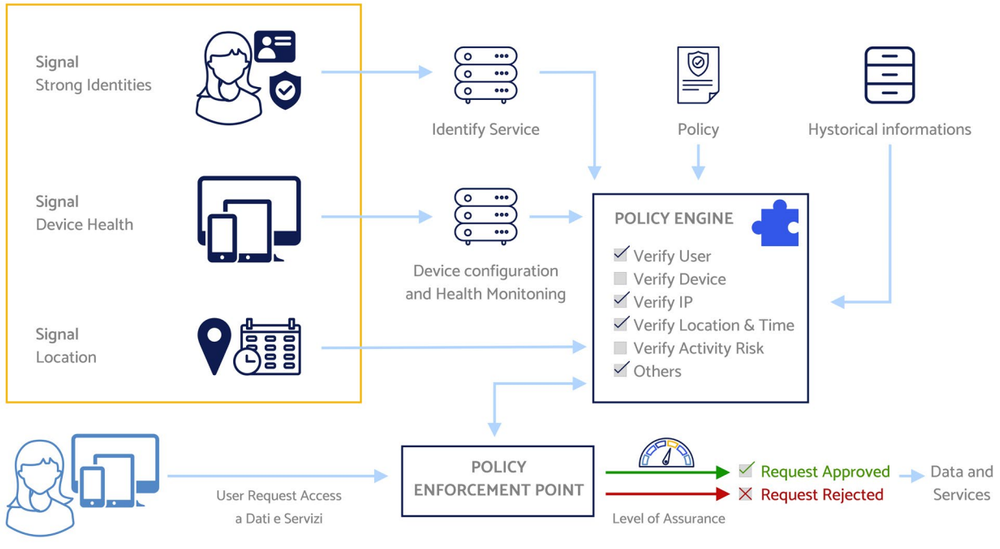
Identificare e raccogliere informazioni delle risorse che interagiscono con i sistemi aziendali al fine di instaurare con questi un rapporto di “fiducia” è un altro passo per raggiungere un livello di maturità in termini di sicurezza Zero Trust. La stratificazione delle policy di accesso basate sul contesto, ovvero applicare la cosiddetta Context Authentication. Questo significa raccogliere segnali su:

- **l’utente**
  chi è; se si trova in un gruppo di utenti a rischio
- **contesto dell’applicazione**
  qual è l’applicazione a cui l’utente sta cercando di accedere
- **contesto del dispositivo**
  tenendo presente che il BYOD è una pratica sempre più diffusa (riconosciamo il dispositivo; qual è la sua Security Posture)
- **la posizione**
- **la rete**
  sono in una rete aziendale conosciuta; stanno cercando di nascondere il loro indirizzo IP.

e applicare politiche di accesso basate su queste informazioni. Ciò significa che l’autenticazione non avviene più non avviene più solo al gate principale, ma avviene continuamente durante l’esperienza dell’utente attraverso una valutazione adattiva e risk-based per identificare le potenziali minacce.

- **Policy Dinamiche**: La policy è un insieme di regole di accesso assegnate a un soggetto, a una risorsa o a un’applicazione. È opportuno stabilire i criteri in base alle esigenze dell’azienda e alla quantità di rischio che si intende accettare. Una policy dinamica può includere livelli di rischio costantemente monitorati di utenti, dispositivi e attributi comportamentali.
  I motori di policy risk-based considerano il livello di fiducia degli utenti e dei dispositivi, regolando dinamicamente le policy di accesso in risposta. Per esempio, un utente che cerca di accedere per la prima volta a un servizio con dati sensibili, al di fuori del normale orario di lavoro potrebbe essergli richiesto di presentare un ulteriore fattore di autenticazione (MFA).
- **Behavioral Analysis**: Il comportamento degli utenti e la salute dei servizi o dei dispositivi sono indicatori importanti quando si cerca di stabilire la fiducia nella sicurezza dei sistemi. Analizzare continuamente i segnali di utenti e dispositivi, per valutarne l’affidabilità è importante per misurarne il comportamento e permette di verificare la genuinità e garantire il Trust. Tali segnali possono poi confluire in un motore di policy per decidere se concedere o meno un accesso. Per facilitare queste valutazioni è bene avere più fonti dati, individuati precedentemente con una fase di Asset Discovery.

- **Monitoraggio e Informazioni Storiche**:
  Monitorare continuamente i segnali di utenti e dispositivi, per valutarne l’affidabilità e memorizzare i comportamenti e le informazioni permette di verificare la genuinità dei dispositivi e degli utenti e il fatto che non siano stati compromessi.
- **Mobile Device Management**: Dal punto di vista della gestione dei dispositivi aziendali e personali (BYOD), il concetto fondamentale è che i dispositivi non devono essere affidabili di default, anche se sono collegati a una rete aziendale gestita come la LAN aziendale sebbene sia stati precedentemente verificati.
  Gli strumenti MDM possono impostare i criteri di accesso degli utenti su una serie di dispositivi, ma da soli non sono sufficienti per garantire una sicurezza mobile efficace.
  L’adozione di un’architettura Zero-Trust è un passo fondamentale per le aziende in un ambiente mobile e basato sul Cloud, dove i confini tradizionali della rete sono stati cancellati. Una piattaforma centralizzata di sicurezza end-to-end che al contempo cifra i dati sia in transito che sul dispositivo, autentica e controlla l’accesso degli utenti, fornisce una gamma completa di protezioni contro malware, phishing e altri attacchi e applica criteri di sicurezza mobile può contribuire a rendere lo Zero Trust una realtà per qualsiasi organizzazione.



Maturity Model

Un approccio di tipo Zero Trust non dovrebbe essere applicato ad un perimetro limitato, ma al contrario dovrebbe estendersi a tutto il patrimonio digitale dell'azienda e servire come una filosofia di sicurezza integrata e come una strategia *end-to-end*. L'Ecosistema Zero Trust è, quindi, un concetto trasversale a più ambiti ognuno dei quali contribuisce, con i propri controlli e le proprie soluzioni/tecnologie, a raggiungere un livello di maturità sempre più avanzato. Tali controlli non possono dipendere da un singolo attributo per determinare il livello di fiducia; invece, devono continuamente costruire quella fiducia con l'utente ponendo domande come: "Chi sei", "da dove vieni", "cosa stai cercando di fare", "quando stai cercando di farlo". Queste verifiche spaziano inevitabilmente per tutti gli ambiti del panorama digitale in ottica cybersecurity:

Livello di maturità

Tradizionale

- Utilizzo di Identity Provider di tipo on-prem
- Non è presente un sistema di federazione SSO tra le applicazioni on-prem e Cloud
- Percezione molto limitata dei rischi

Avanzato

- Federazione tra i sistemi on prem e Cloud
- Applicazione di policy di Conditional Access
- Possibilità di analisi per migliorare la visibilità sui rischi connessi alla gestione delle identità e degli accessi

Ottimale

- Passwordless authentication è abilitata
- Analisi real-time dei comportamenti degli utenti per determinare il livello di rischio e garantire una protezione costante

Conclusioni

La dematerializzazione del perimetro aziendale a cui abbiamo assistito negli ultimi tempi ha indotto le organizzazioni di ogni settore ad adeguarsi con sistemi di Identity and Access Management e Governance che consentano di centralizzare in un'unica soluzione la gestione delle identità digitali durante tutto il loro ciclo di vita nonché il controllo degli accessi ai sistemi.

A supporto delle esigenze emerse per la gestione degli accessi da remoto, il modello Zero Trust consente di passare al setaccio tutti gli agenti - umani e non - che si presentano ancor prima di effettuare l'accesso e di storicizzarne le informazioni al fine di valutarne di continuo i comportamenti.

Visti gli scenari geopolitici recenti e i requisiti di compliance alle normative in materia, fare di necessità virtù sta spronando sempre più le aziende a rivedere la propria posture in ambito di cybersecurity e a correre ai ripari prima che sia troppo tardi.

Lo Zero Trust model rappresenta una svolta nell'approccio alla sicurezza proponendosi come modello strategico che ruota intorno alla protezione delle identità digitali delle aziende.

Key takeway

1 Lo Zero Trust è un modello strategico di sicurezza basato sull'idea che tutti gli agenti, sia interni che esterni al perimetro di rete di un'organizzazione, non possano essere ritenuti affidabili di default.

2 Rispetto ad un approccio tradizionale alla security costruito su un'infrastruttura on-premise, lo Zero Trust si adatta ad un contesto dove il perimetro aziendale è sempre più esteso e frammentato e i sistemi comunicano tra loro in modo più complesso.

3 La gestione delle identità in ottica Zero Trust contribuisce a rafforzare la protezione degli asset aziendali attraverso l'applicazione del Least Privilege e del principio del need to know, la micro-segmentazione della rete, l'autenticazione basata sul contesto e la creazione di policy dinamiche.

4 Lo Zero Trust, quindi, rappresenta un'opportunità per gestire le identità digitali delle aziende che hanno la necessità di innalzare il livello di Security Posture per adeguarsi alle minacce crescenti.

NTT DATA
Trusted Global Innovator

Jessica Naso
IAM Process Specialist

Digital Identity Protection

Giulia Tonussi
Consultant

Cyber Security Strategy & Governance

Carlo Mancini
Manager

Digital Identity Protection Lead

NTT DATA aiuta le organizzazioni a orientarsi nella rapida evoluzione delle tecnologie, a rispondere alle crescenti aspettative dei clienti e, attraverso l'innovazione e la profonda esperienza nel settore, mette a disposizione le competenze e le risorse per guidare lo sviluppo digitale. Offriamo consulenza in ogni fase di progetto, da una prima fase di strategia e concept, passando dagli impatti sui processi, per arrivare all'implementazione finale. Advisory, Design, Tecnologia e Operation sono solo alcune delle nostre aree di competenza. NTT DATA ha sede a Tokyo con oltre 123.000 professionisti in oltre 50 Paesi in tutto il mondo. www.nttdata.com/it

© 2022 NTT DATA, Inc. All rights reserved

NTT DATA