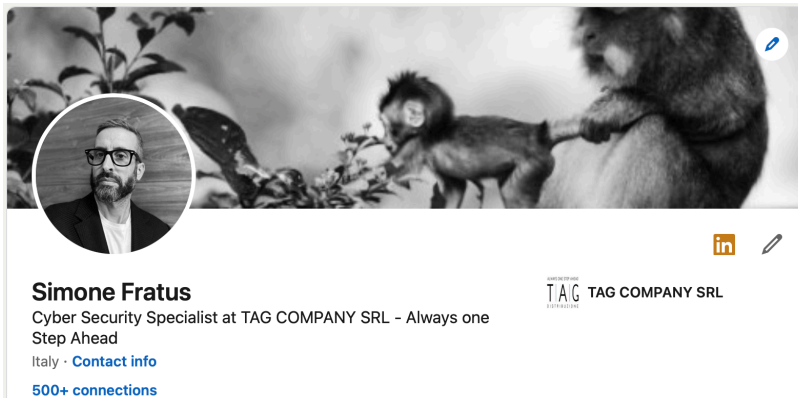




Simone Fratus

Cyber Security Specialist at TAG COMPANY SRL - Always one Step Ahead

Italy · [Contact info](#)

500+ connections

TAG COMPANY SRL

in

Simone Fratus
Cybersecurity Specialist
simone@tagdistribuzione.com

ALWAYS ONE STEP AHEAD

T | A | G

D I S T R I B U Z I O N E



ALWAYS ONE STEP AHEAD

T | A | G

DISTRIBUZIONE

INNOVATIVA CYBERSECURITY ISRAELIANA

SOLUZIONI INNOVATIVE ISRAELIANE

Management israeliano con forti legami nel mondo della cyber-security in Israele.

Selezione e test di **soluzioni innovative**.

Supporto ed **affiancamento dei clienti** per incontri di approfondimento. Il nostro approccio è consulenziale.

Prodotti e servizi di consulenza di **Cyber-Intelligence** nel DarkWeb.

ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

ALWAYS ONE STEP AHEAD

Why?

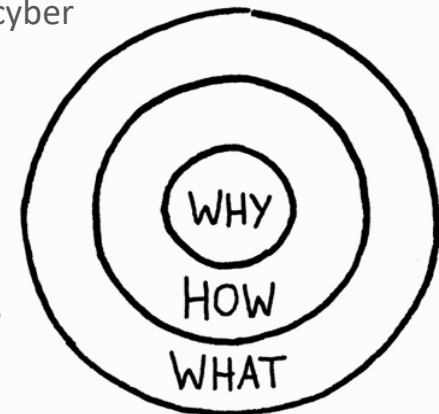
Tutto ciò che facciamo è mettere in discussione lo status quo.
Crediamo nel pensare diversamente, pensare “fuori dalla scatola”

How?

Il modo in cui sfidiamo lo status quo è di evidenziare in anticipo che cyber security vuole dire pensare “fuori dalla scatola”, pensare come un attaccante, non restare fermi negli schemi tradizionali.

What?

Siamo forti di una notevole esperienza tecnica dove abbiamo fatto crescere la consapevolezza parlando di CyberSecurity. Portiamo delle innovative soluzioni che hanno un filo logico nella applicazione della strategia aziendale di cyber security.



ALWAYS ONE STEP AHEAD

T | A | G
DISTRIBUZIONE

THE BEGINNING

Dear ladies and respected gentlemen



ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

25 GENNAIO 2020

ALWAYS ONE STEP AHEAD
T | A | G
D I S T R I B U Z I O N E

CHI SIAMO SOLUTION NEWS EVENTI AREA PARTNER CONTATTI

COSA ASPETTARSI NEL 2020? LA US HOMELAND SECURITY DICE UN ATTACCO CYBER SPROPOSITATO



Jeanette Manfra, responsabile della "US Homeland Security Cybersecurity and Infrastructure Security Agency" si dimette ed ammette che attualmente nulla possono fare contro quello che sembra un imminente e spropositato attacco cyber che avverrà nel 2020.

Di certo coincidenze come queste fanno riflettere. La numero 2 degli Stati Uniti per quanto riguarda la cyber sicurezza nazionale si dimette dal suo ruolo conquistato con tanta fatica e lavoro di molti anni, ed inoltre cita che fonti di

T | A | G
ALWAYS ONE STEP AHEAD

Search...

Articoli recenti

Ecco perchè servono soluzioni innovative

600.000€ di sanzione per mancata gestione privilegi minimi

Lo Smart-Working e le numerose opportunità di violazione

LOCKBIT è il nuovo ransomware a noleggio

UNICREDIT DI NUOVO SOTTO
ATTACCO: DATI IN VENDITA NEI
FORUM DEL CYBER-CRIME

ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

26 FEBBRAIO 2020

ALWAYS ONE STEP AHEAD
T | A | G
D I S T R I B U Z I O N E

CHI SIAMO SOLUTION · NEWS EVENTI Restricted content CONTATTI

IL CORONAVIRUS, LE VPN AZIENDALI E LA MIA PREVISIONE CHE SPERO NON SI AVVERI



TUTTI I RISCHI DELLA VPN AZIENDALE

In questi giorni dove il Coronavirus tiene banco in tutti i media italiani le preoccupazioni sono già tante. Probabilmente il tema è troppo spettacolarizzato dalla "solita stampa" italiana che butta sul tavolo numeri confusi e senza un criterio serio di paragone che aiuterebbe a capire. Faccio un esempio semplice: si dice che in Italia i casi positivi al tampone sono 150 circa mentre in Germania 18. Non si dice invece che l'Italia ha fatto più di 6000 tamponi mentre la Germania solo 600 e la Francia 400. Non si dice che dei 150 positivi italiani solo circa 20 presentano sintomi mentre gli altri sono asintomatici, il che vuol dire che se non avessero fatto il tampone non avrebbe probabilmente mai saputo di essere positivi perchè non si sono ammalati. Quindi, se la Germania avesse fatto lo stesso numero di tamponi dell'Italia

T | A | G
ALWAYS ONE STEP AHEAD

Search...

Articoli recenti

Tag Distribuzione partner dell'Associazione Bullismo No Grazie

Identity Management e Zero Trust: cosa significa sicurezza al giorno d'oggi

Si prevede un aumento di 4 volte degli attacchi alla catena di approvvigionamento

I costi ransomware aumentano esponenzialmente

Perché implementare Zero Trust è più importante che mai

ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

List of haked company



ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

ZERO TRUST

WORLD
ECONOMIC
FORUM
COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

The Cybersecurity Guide for Leaders in Today's Digital World

October 2019



This guide is intended for senior executives who are responsible for setting and implementing the strategy and governance of cybersecurity and resilience in their organization. Cybersecurity is everyone's responsibility in an organization, not solely of the Chief Information Security Officer. It is essential that key stakeholders in the C-Suite, such as Chief Information Officers, Chief Technology Officers, Chief Digital Officers, Chief Financial Officers and other company executive officers understand their responsibilities as it relates to cybersecurity.

10 Tenets for Leaders

Tenet 1
Think Like a
Business Leader



Tenet 2
Foster Internal
and External
Partnerships



Tenet 3
Build and
Practice Strong
Cyber Hygiene



Tenet 4
Protect Access to
Mission-Critical
Assets



Tenet 5
Protect Your
Email Domain
Against Phishing



Tenet 6
Apply a Zero-Trust
Approach to
Securing Your
Supply Chain



Tenet 7
Prevent, Monitor
and Respond to
Cyber Threats



Tenet 8
Develop
and Practice
Comprehensive
Crisis Management
Plan



Tenet 9
Build a Robust
Disaster-Recovery
Plan for
Cyberattacks



Tenet 10
Create a Culture
of Cybersecurity



ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

ZERO TRUST

NIST

Search NIST



Menu

PUBLICATIONS

Zero Trust Architecture

Published: August 11, 2020

Author(s)

Scott W. Rose, Oliver Borchert, Stuart Mitchell, Sean Connelly

Abstract

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprises overall information technology security posture.

Citation: Special Publication (NIST SP) - 800-207

Report Number: 800-207

NIST Pub Series: [Special Publication \(NIST SP\)](#)

Pub Type: NIST Pubs

Download Paper

[DOI Link](#)

ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

ZERO TRUST



SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures

March 17, 2021
Cybersecurity and Infrastructure Security Agency





Search for resources, tools, p

TOPICS ▾ PUBLICATIONS TOOLS NEWS EVENTS

Home > Publications > Threat Landscape for Supply Chain Attacks

Topic

- ^ Threat and Risk Management
 - > Threat Landscape
 - > Threat and Risk Management

Keywords

Threat landscape

Threat Landscape for Supply Chain Attacks

This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021. Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.



Download

PDF document, 4.79 MB

Published July 29, 2021
Language English

ALWAYS ONE STEP AHEAD

T|A|G
DISTRIBUZIONE



ALWAYS ONE STEP AHEAD

 **NSA | CSS** National Security Agency Central Security Service
Defending our Nation. Securing the Future.

Search NSA CSS 

What We Do ▾ News & Features ▾ Resources ▾ Join our Team ▾ D

[HOME](#) > [NEWS & FEATURES](#) > [FEATURE STORIES](#) > [ARTICLE VIEW](#)



[DOWNLOAD HI-RES](#) / [PHOTO DETAILS](#)

NSA Issues Guidance on Zero Trust Security Model

NSA Issues Guidance on Zero Trust Security Model

[PRINT](#) | [E-MAIL](#)



FORT MEADE, Md., Feb. 25, 2021 —

The National Security Agency published a cybersecurity product, “[Embracing a Zero Trust Security Model](#),” on Thursday. This product shows how deploying Zero Trust security principles can better position cybersecurity professionals to secure enterprise networks and sensitive data. To provide NSA’s customers with a foundational understanding of Zero Trust, this product discusses its benefits along with potential challenges, and makes recommendations for implementing Zero Trust within their networks.

The Zero Trust model eliminates trust in any one element, node, or service by assuming that a breach is inevitable or has already occurred. The data-centric security model constantly limits access while also looking for anomalous or malicious activity.

ALWAYS ONE STEP AHEAD
T | A | G
D I S T R I B U Z I O N E

ALWAYS ONE STEP AHEAD

T | A | G
D I S T R I B U Z I O N E

ZERO TRUST - Executive order

 An official website of the United States government [Here's how you know](#) ▼

Moving the U.S. Government Towards Zero Trust Cybersecurity Principles

Executive Order 14028 | WhiteHouse

[Home](#) [Federal Zero Trust Strategy](#) [Zero Trust Maturity Model](#) [Cloud Security Technical Reference Architecture](#)

Welcoming public feedback

The [Office of Management and Budget](#) (OMB) and the [Cybersecurity and Infrastructure Security Agency](#) (CISA) are **seeking public feedback** on strategic and technical guidance documents meant to **move the U.S. government towards a zero trust architecture**.

- Read and comment on OMB's [Federal Zero Trust Strategy](#). The goal of this strategy is to accelerate agencies towards a shared baseline of early zero trust maturity.
- Read and comment on CISA's [Zero Trust Maturity Model](#). The maturity model complements OMB's Federal Zero Trust Strategy, and is designed to provide agencies with a roadmap and resources to achieve an optimal zero trust environment.
- Read and comment on CISA's [Cloud Security Technical Reference Architecture](#), a guide for agencies to leverage when migrating to the cloud securely. The document explains considerations for shared services, cloud migration, and cloud security posture management.



This website is maintained by the [Office of Management and Budget](#) and the [Cybersecurity and Infrastructure Security Agency](#).

This website is [open source](#) and built using the [U.S. Web Design System](#).



[Administration](#) [Priorities](#)

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

ALWAYS ONE STEP AHEAD



Zero Trust ci insegna a **“Non fidarsi mai, verificare sempre”**. Il modello **Zero Trust** presume la violazione e verifica per ogni richiesta come se provenisse da una rete aperta, invece di presumere che tutto dietro il firewall aziendale sia sicuro. Ogni richiesta di accesso è completamente autenticata, autorizzata e crittografata prima di concedere l'accesso.

Zero Trust si basa su tre semplici principi:

- **Verificare esplicitamente:** autentica e autorizza in base a tutti i punti dati disponibili, inclusi identità utente, posizione, integrità del dispositivo, servizio o carico di lavoro, classificazione dei dati e anomalie.
- **Usare l'accesso con privilegi minimi:** limitare l'accesso agli utenti con modalità di accesso **“just-int-time”** e **“just-enough”**, politiche adattive basate sul rischio, e protezione dei dati per proteggere sia i dati che la produttività.
- **Presupporre la violazione:** ridurre al minimo il raggio d'azione per le violazioni e prevenire il movimento laterale segmentando l'accesso per rete, utente, dispositivi e consapevolezza dell'app. Verificare che tutte le sessioni siano crittografate end-to-end. Usare l'analisi per ottenere visibilità, guidare il rilevamento delle minacce e migliorare le difese.



ALWAYS ONE STEP AHEAD

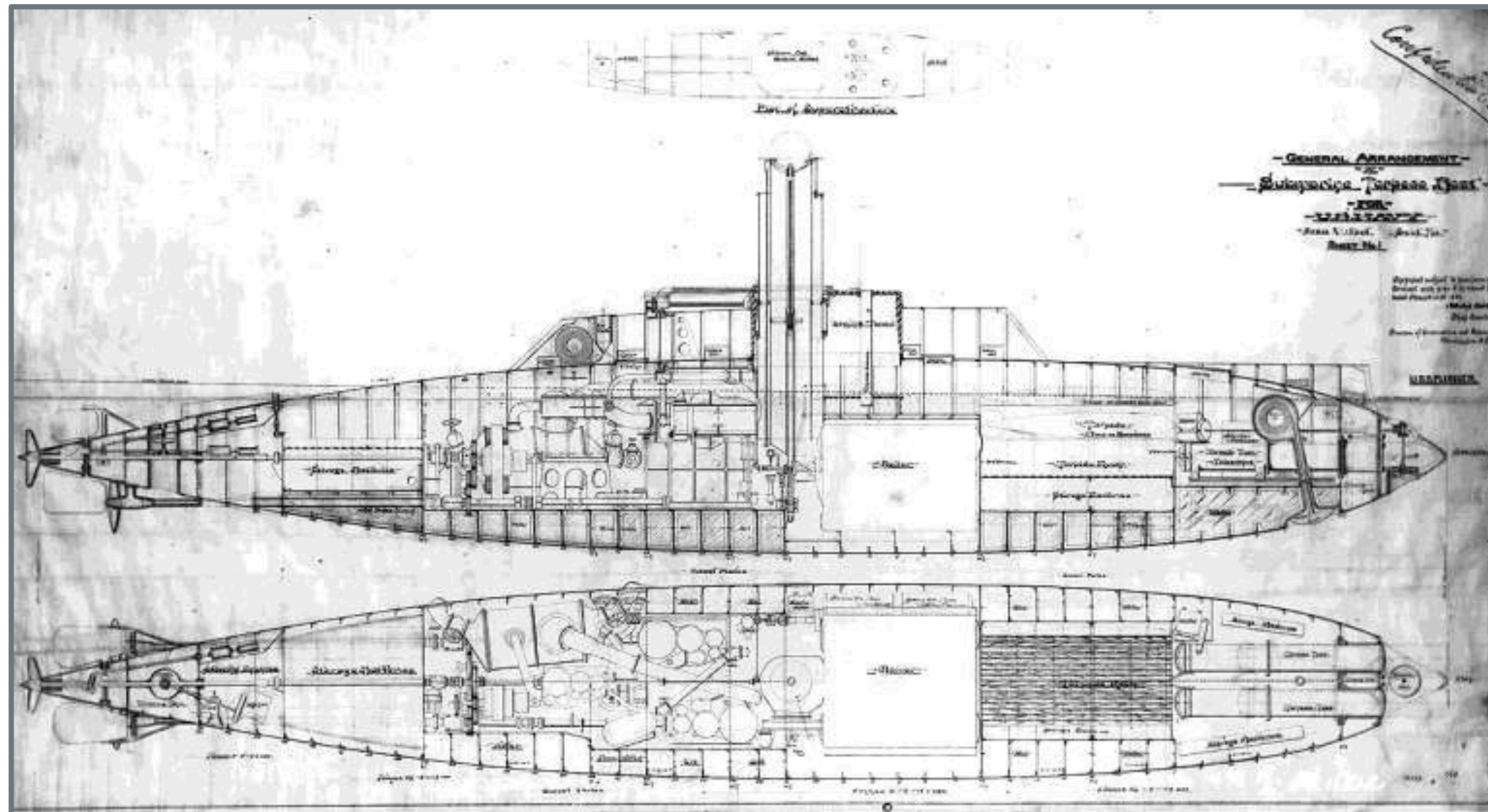
T|A|G
DISTRIBUZIONE



Zero Trust is not a security solution. It's a strategy!

Una delle principali sfide e incomprensioni che continuo a vedere è quale sia effettivamente la definizione di Zero Trust. Zero Trust non è un prodotto o una piattaforma; è un framework di sicurezza costruito attorno al concetto di "non fidarti mai, verifica sempre" e "presumere una violazione".

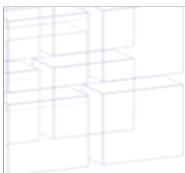
ALWAYS ONE STEP AHEAD



ALWAYS ONE STEP AHEAD
T|A|G
 DISTRIBUZIONE



SOLUZIONI
INNOVATIVE



ALWAYS ONE STEP AHEAD

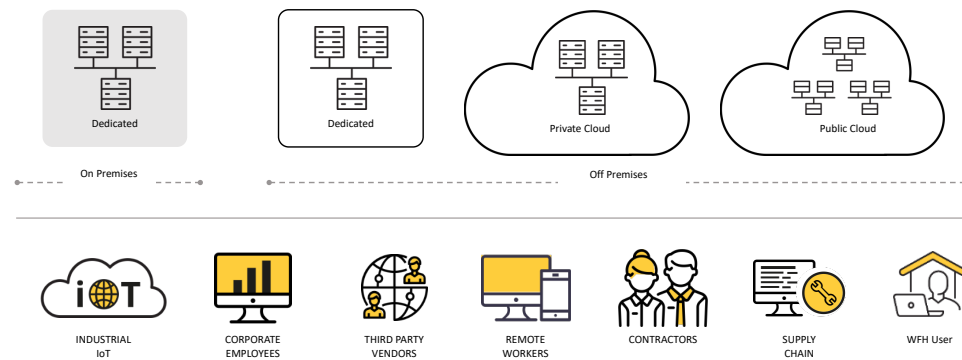
ZoneZero Perimeter Access Orchestration for True Zero Trust Network Access (ZTNA) Implementation

ZoneZero sta cambiando le regole del gioco, consentendo alle organizzazioni di fornire un accesso sicuro e trasparente a qualsiasi applicazione, servizio e dati interni. La tecnologia brevettata di Revers Access permette di aggiungere layer di security, renderle web based, aggiungere MFA ad applicazioni o protocolli che non lo prevedono.

ALWAYS ONE STEP AHEAD
T|A|G
D I S T R I B U Z I O N E

ALWAYS ONE STEP AHEAD

safe-+
Masters of Access

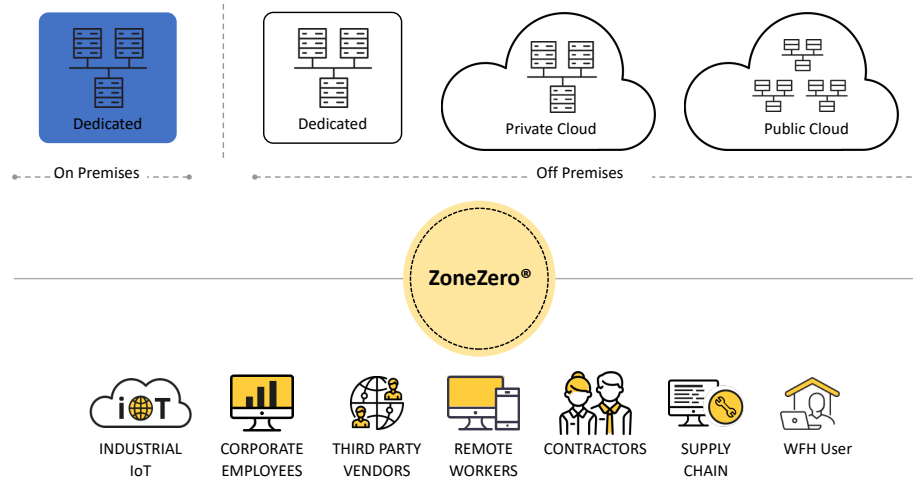


Defining and securing the perimeter is complicated.

ALWAYS ONE STEP AHEAD
T|A|G
D I S T R I B U Z I O N E

ALWAYS ONE STEP AHEAD

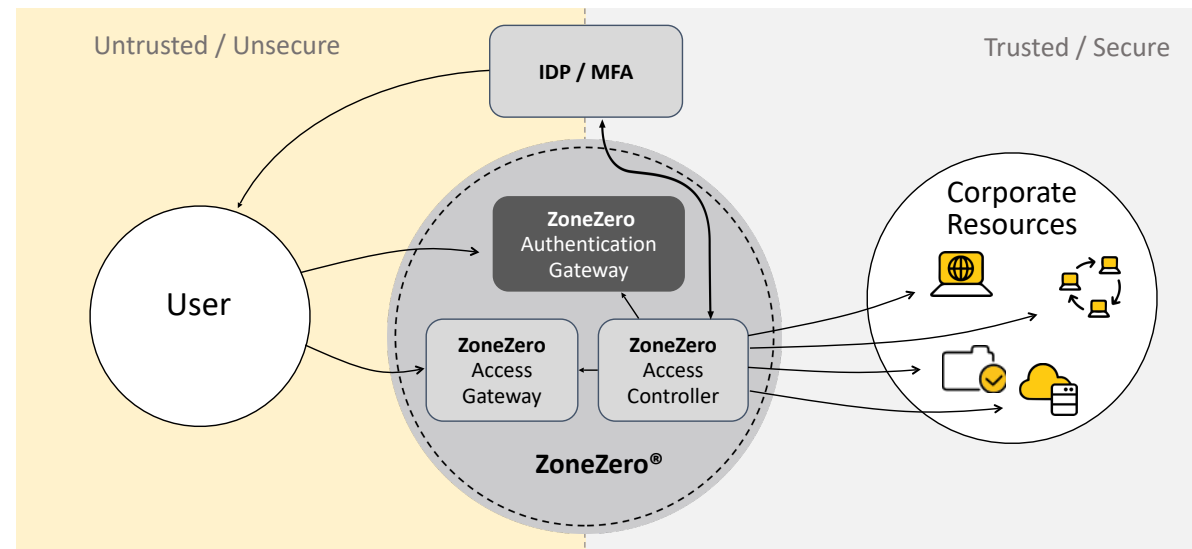
safe-+
Masters of Access

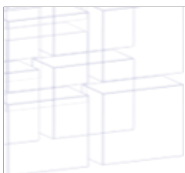


ALWAYS ONE STEP AHEAD
T|A|G
DISTRIBUZIONE

ALWAYS ONE STEP AHEAD

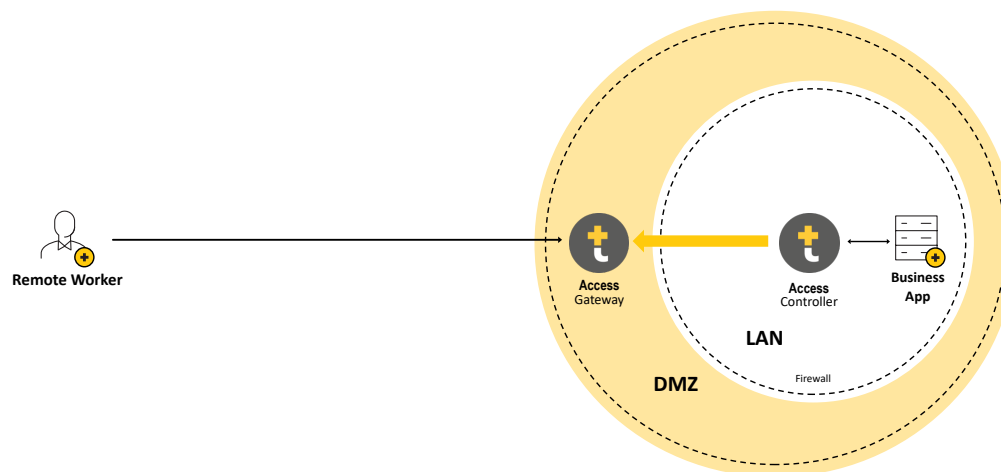
safe-t
Masters of Access





ALWAYS ONE STEP AHEAD

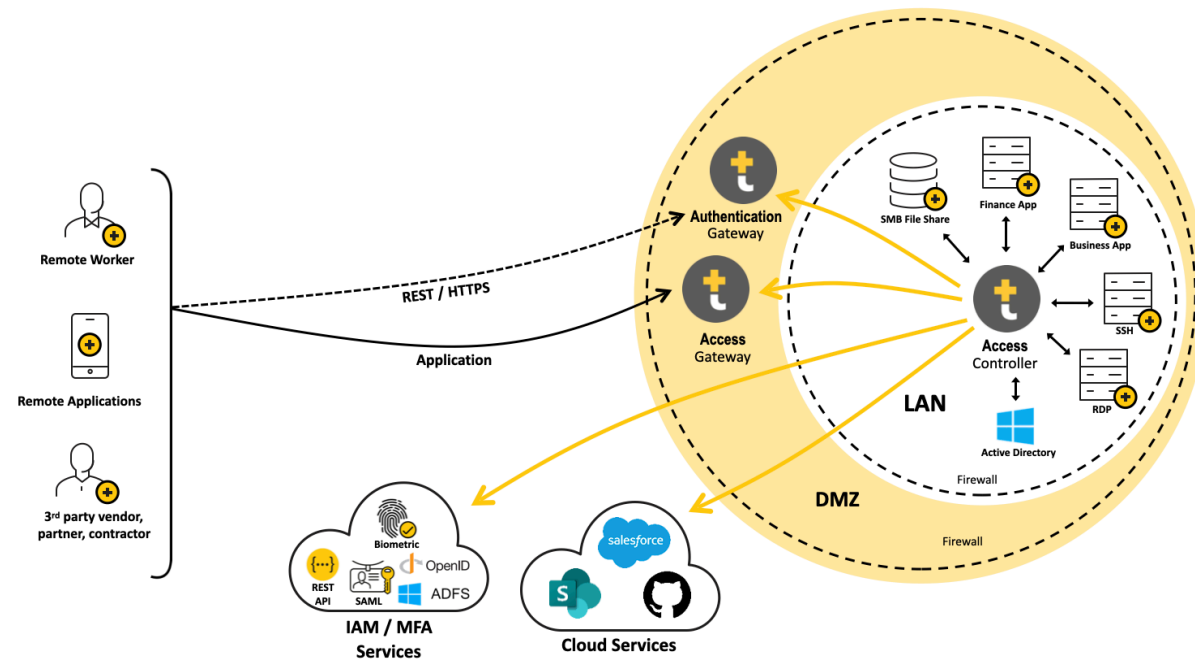
safe-t
Masters of Access



Safe-T's Patented Reverse Access - How It Works

ALWAYS ONE STEP AHEAD

safe-+
Masters of Access



ALWAYS ONE STEP AHEAD
T|A|G
DISTRIBUZIONE

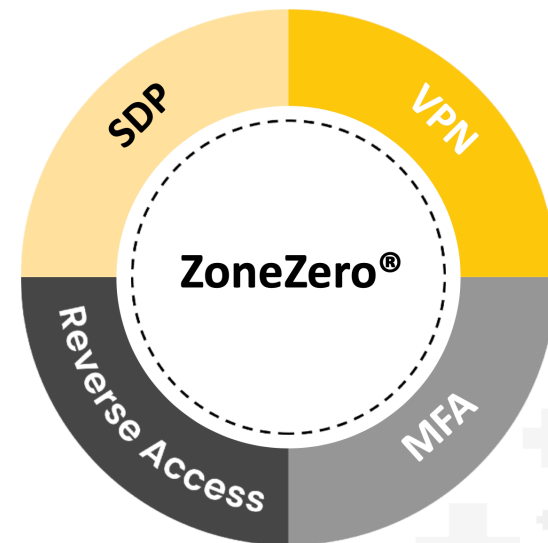
ALWAYS ONE STEP AHEAD

safe-t
Masters of Access

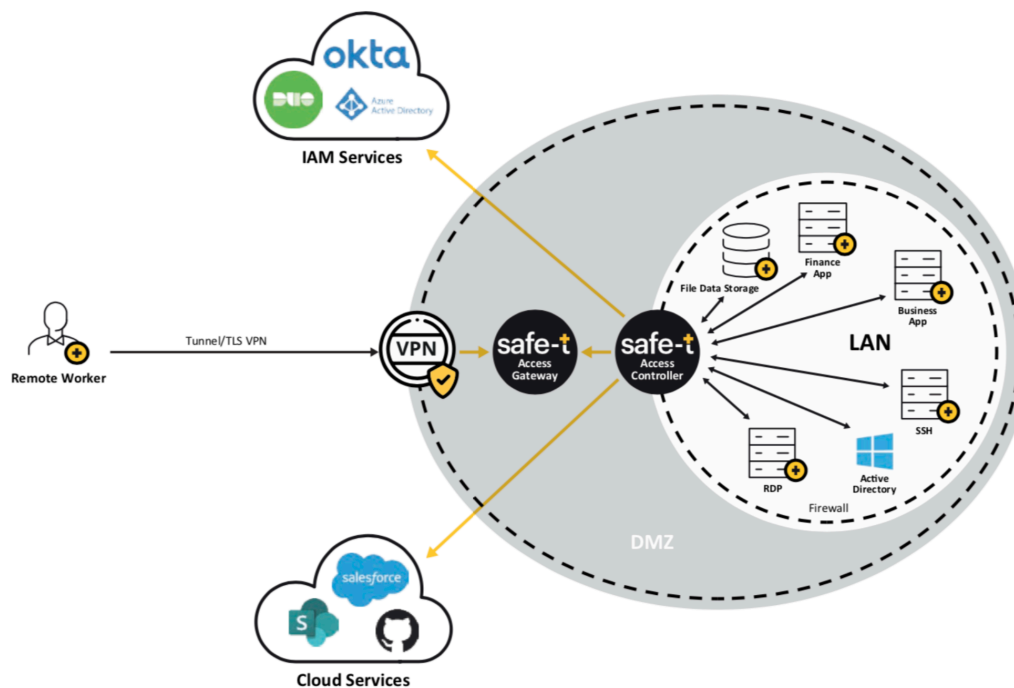
ZoneZero – Perimeter Access Orchestration

The only access orchestration solution in the market, that:

- + Unifies all access use cases
- + Combines best of breed access technologies
- + Based on Safe-T's patented reverse-access
- + Supports any user and application
- + Fits both current and future access needs



ALWAYS ONE STEP AHEAD
T|A|G
DISTRIBUZIONE



ALWAYS ONE STEP AHEAD



“A CyberSecurity Mindset May Involve
Being The Guy With The Most Negative
Attitude.”