



Architetture di sicurezza zero trust cloud-based

Marco Gioanola, Sales Engineer, mgioanola@zscaler.com

28/10/2022

Zscaler: leader nella sicurezza della digital transformation

Rendere il cloud un luogo sicuro dove fare business, con le migliori prestazioni

Zenith of scalability

- **Fondata nel 2007**
- **NASDAQ: ZS 2018**
- **1B USD Annual Recurring Revenue**
- Costante aggiunta di funzionalità:
 - ✓ Data Loss Prevention (DLP): 2008
 - ✓ Bandwidth Management/QoS: 2009
 - ✓ Cloud Application Visibility and Control: 2012
 - ✓ Next Generation Firewall: 2014
 - ✓ Cloud Sandboxing/Advanced Behavioral Analysis: 2014
 - ✓ Cloud IPS: 2015
 - ✓ Zscaler Private Access (ZPA): 2016
 - ✓ DLP Exact Data Match: 2018

Zero Trust Exchange



Secure Web Gateway quadrant leader



Lo stato della sicurezza informatica



Content inspection; Data Loss Prevention

Segmentation; firewalls; DMZ; IPS; RBAC

Patching; VA; PenTest

Device / User / Network Behavior analysis

E in più... change management, hardware upgrades, appliance lifecycle...

The Top 50

BIGGEST DATA BREACHES



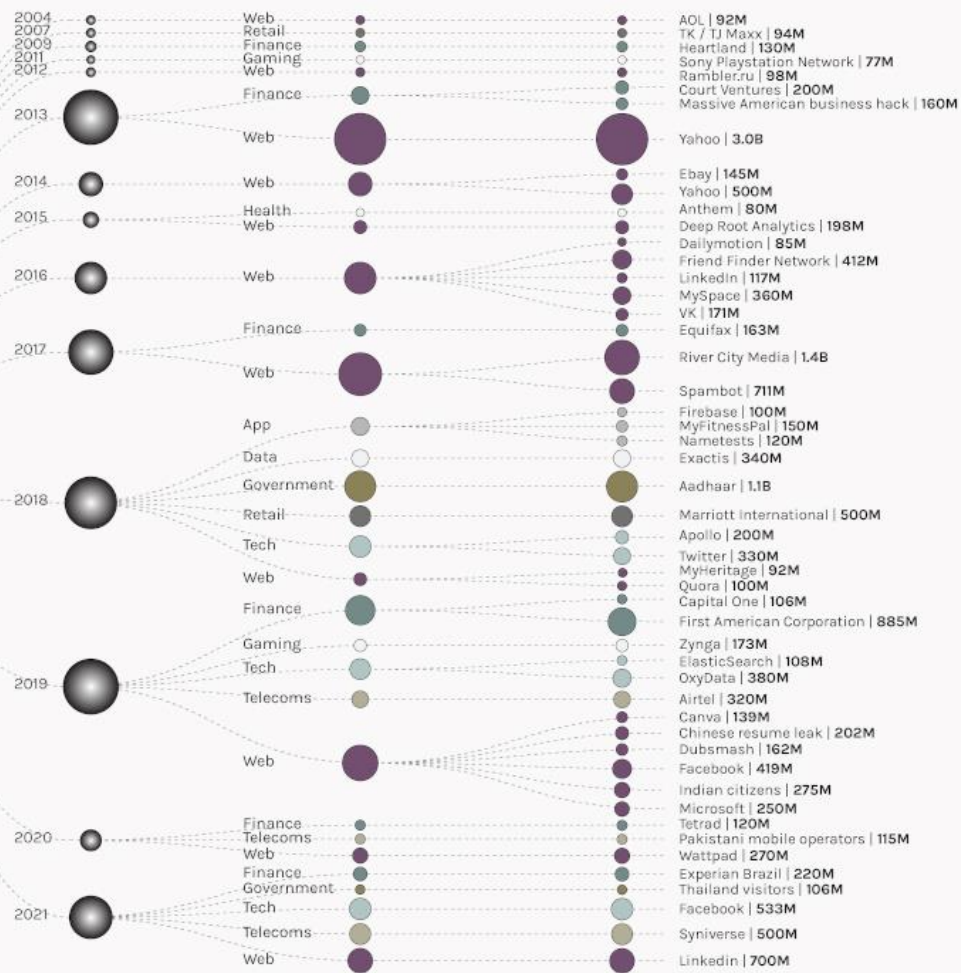
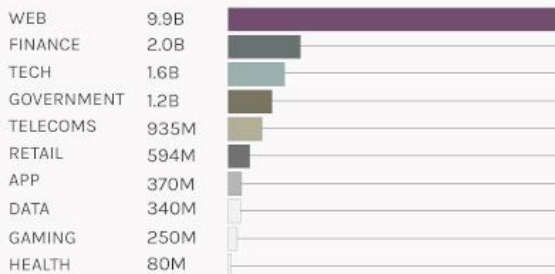
from 2004 - 2021

A data breach is an incident where protected information is copied, stolen, or exposed to an unauthorized person. The largest breach in recent times was the LinkedIn breach of 2021 in which 700 million records were lost. The visual on the right highlights the Top 50 known data breaches from 2004 to 2021.

The Web sector was impacted the most. 9.9B records were lost. The Tech and Finance sectors were also severely impacted, and they lost 1.6B and 2.0B records, respectively.

SECTORS - These are industry sectors which the companies belong to. There are 10 in total.

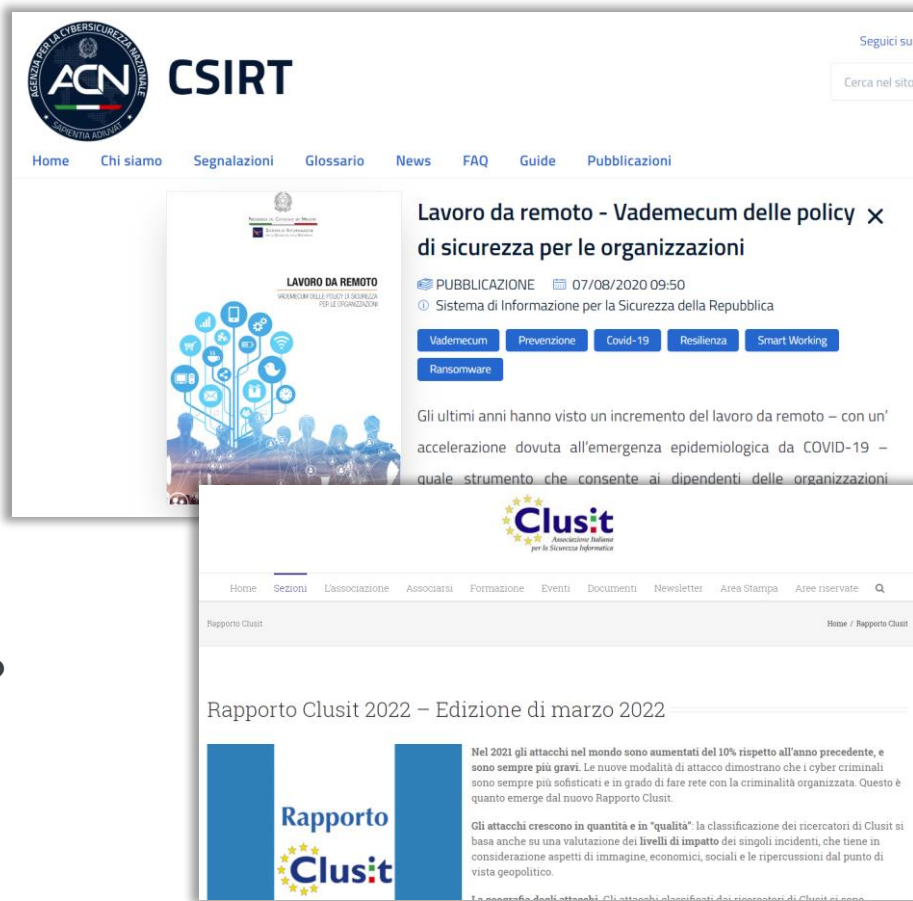
The number of records lost per sector is shown below:



E non è tutto...

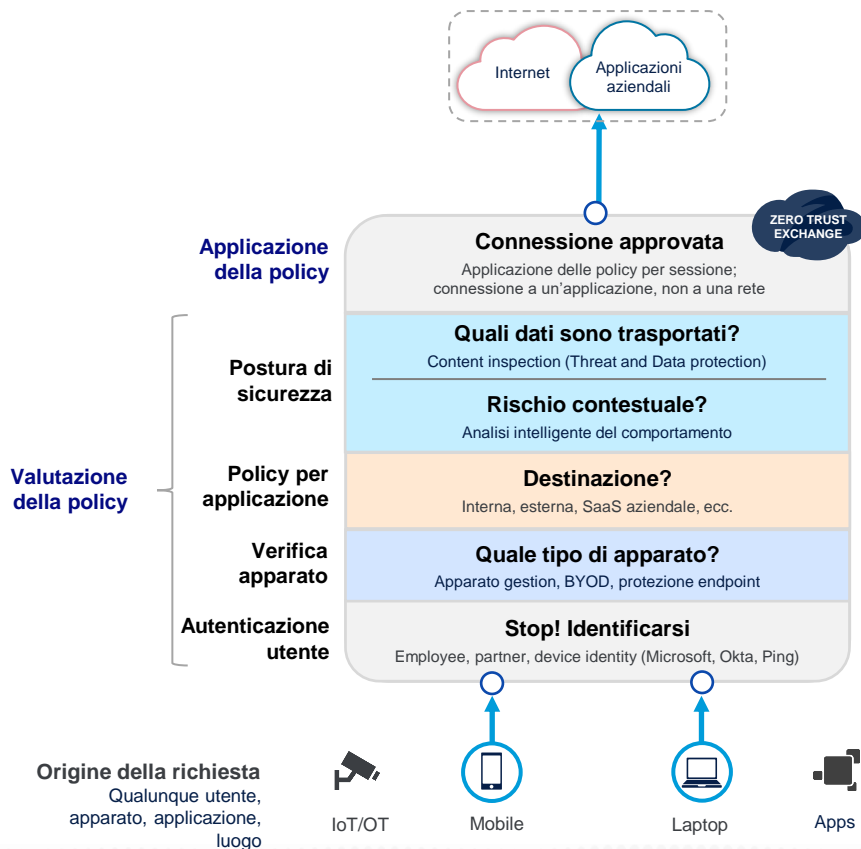
- Massiccio ricorso al telelavoro
- VPN gateways sotto stress
- Massiccio ricorso al SaaS
- Massiccio ricorso a IaaS
- Shadow IT

Come tenere sotto controllo tutto ciò?



The image displays two overlapping screenshots of Italian cybersecurity websites. The top screenshot is the CSIRT (Computer Security Incident Response Team) website, featuring the ACN logo and a navigation menu. The main article is titled "Lavoro da remoto - Vademecum delle policy di sicurezza per le organizzazioni" and includes a publication date of 07/08/2020 09:50. It lists categories such as Vademecum, Prevenzione, Covid-19, Resilienza, Smart Working, and Ransomware. The bottom screenshot is the Clusit website, showing the "Rapporto Clusit 2022 - Edizione di marzo 2022". The main text states: "Nel 2021 gli attacchi nel mondo sono aumentati del 10% rispetto all'anno precedente, e sono sempre più gravi. Le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata. Questo è quanto emerge dal nuovo Rapporto Clusit." It also mentions that attacks are increasing in quantity and quality, and that Clusit's classification considers aspects like image, economic, social, and geopolitical.

1. Zero Trust Exchange Architecture



Zero trust presuppone che non vi sia **alcuna fiducia implicita** concessa alle risorse o agli account utente in base esclusivamente alla loro posizione fisica o di rete o in base alla proprietà delle risorse.

L'autenticazione e l'autorizzazione sono funzioni discrete eseguite **prima** che venga stabilita una sessione di una risorsa dell'organizzazione.

Zero trust è una risposta alle tendenze della rete aziendale che includono utenti remoti, bring your own device, e risorse basate su cloud che non si trovano all'interno del confine di rete di proprietà aziendale.

Zero trust si focalizza sulla **protezione delle risorse, non dei segmenti di rete.**

(<https://www.nist.gov/publications/zero-trust-architecture>)

2. L'architettura SASE – Secure Access Service Edge

Secure Access Service Edge (SASE) offre funzionalità convergenti di **rete e security as a service**, tra cui SD-WAN, SWG, CASB, NGFW e **zero trust network access (ZTNA)**. SASE supporta casi d'uso di filiali, lavoratori remoti e accessi sicuri on-premise.

SASE viene fornito principalmente come servizio e consente l'accesso **zero trust** in base all'identità del dispositivo o dell'entità, combinata con il contesto in tempo reale e le politiche di sicurezza e conformità.

(<https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase>)

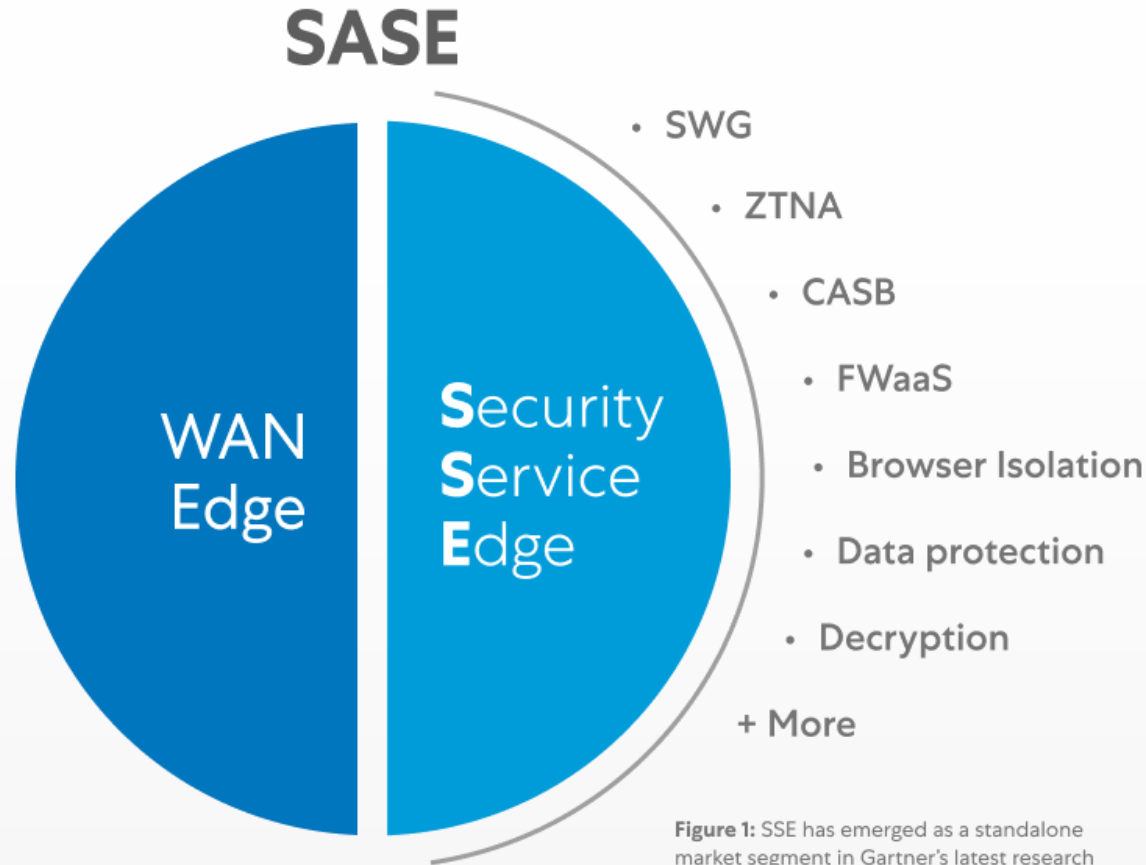


Figure 1: SSE has emerged as a standalone market segment in Gartner's latest research



GRAZIE!



“It’s a rare occasion in history where it got **more secure**,
provided a **better experience** and got **cheaper** all at once.”