Hybrid Workplace, la Gestione della Leadership

CUSTOMER ACADEMY

- Flora Gitti – flora.gitti@eos-solutions.it
- Luca Borio – luca.borio@eos-solutions.it
- Alberto Duò – alberto.duo@eos-solutions.it
- Alvise Giacomin– alvise.giacomin@eos-solutions.it

eos solutions
A KUMAVISION GROUP COMPANY

EOS WEBINARS

Speaker

Flora Gitti
Sales Manager
Customer Service

Luca Borio
Business Line Manager
Azure & Modern Workplace

Alberto Duò
PreSales
Azure & Modern Workplace

Alvise Giacomin
Azure Specialist
Azure & Modern Workplace

Agenda

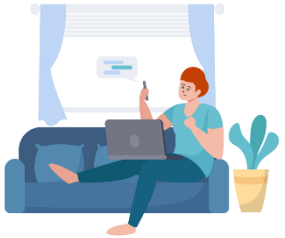
- Hybrid Work quarta puntata
- Endpoint: da dispositivo di backup a cuore dello smart working
- Hands on lab: simuliamo un attacco e vediamo come la piattaforma Microsoft ci protegge
- Phishing e Malware: i tuoi utenti sanno come proteggersi? Mettiamoli alla prova con le Campagne integrate in 365
- Q&A

Hybrid Work 4ª puntata

studio condotto dal Boston Consulting Group

Non si tornerà al classico lavoro d'ufficio, ma non si resterà nemmeno in smart working per sempre. Quello che ci aspetta, una volta lasciata alle spalle l'emergenza sanitaria, è il **lavoro ibrido**, partendo dal fatto che maggiore flessibilità ha garantito benefici alle aziende come ai dipendenti.

ora le aziende sono chiamate a ripensare lo spazio di lavoro, adottando un modello ibrido.



L'indagine mostra che una cospicua maggioranza dei lavoratori ha mantenuto e spesso **accresciuto i propri livelli di produttività**

EOS ti aiuta nella transizione

Le persone sono **al centro del hybrid work**

Gli spazi **cambiano forma e funzione**

Tutti i processi devono per forza **essere digitali**

EOS ti aiuta nella transizione

PERSONE

- Il lavoro ibrido è inevitabile. Si deve creare la cultura aziendale per abilitarlo.
- Tutti i manager devono essere motivati per applicare il lavoro ibrido.
- Rendi Viva il punto di riferimento per i tuoi collaboratori.
- Costruisci un sistema per ascoltare i tuoi collaboratori.
- Aiutare le persone a imparare e a crescere durante il loro lavoro.
- Prevenire il bornout 'digitale' dalla testa del problema.
- La flessibilità come strumento per attrarre e trattenere nuovi e talenti.

LUOGHI

- Riportare le persone sul posto di lavoro in sicurezza.
- Gli ambienti devono essere pensati anche per chi non è nella stanza.
- Trasforma i tuoi spazi fisici in servizi intelligenti basati su cloud.

PROCESSI

- Usa Teams per trasformare il tuo business.
- Sposta tutto al cloud – come e più in fretta che puoi.
- Digitalizzare ogni processo aziendale - dai processi gestionali a quelli di vendita.
- Gestire la sicurezza dal client al cloud senza soluzione di continuità.

La definizione …

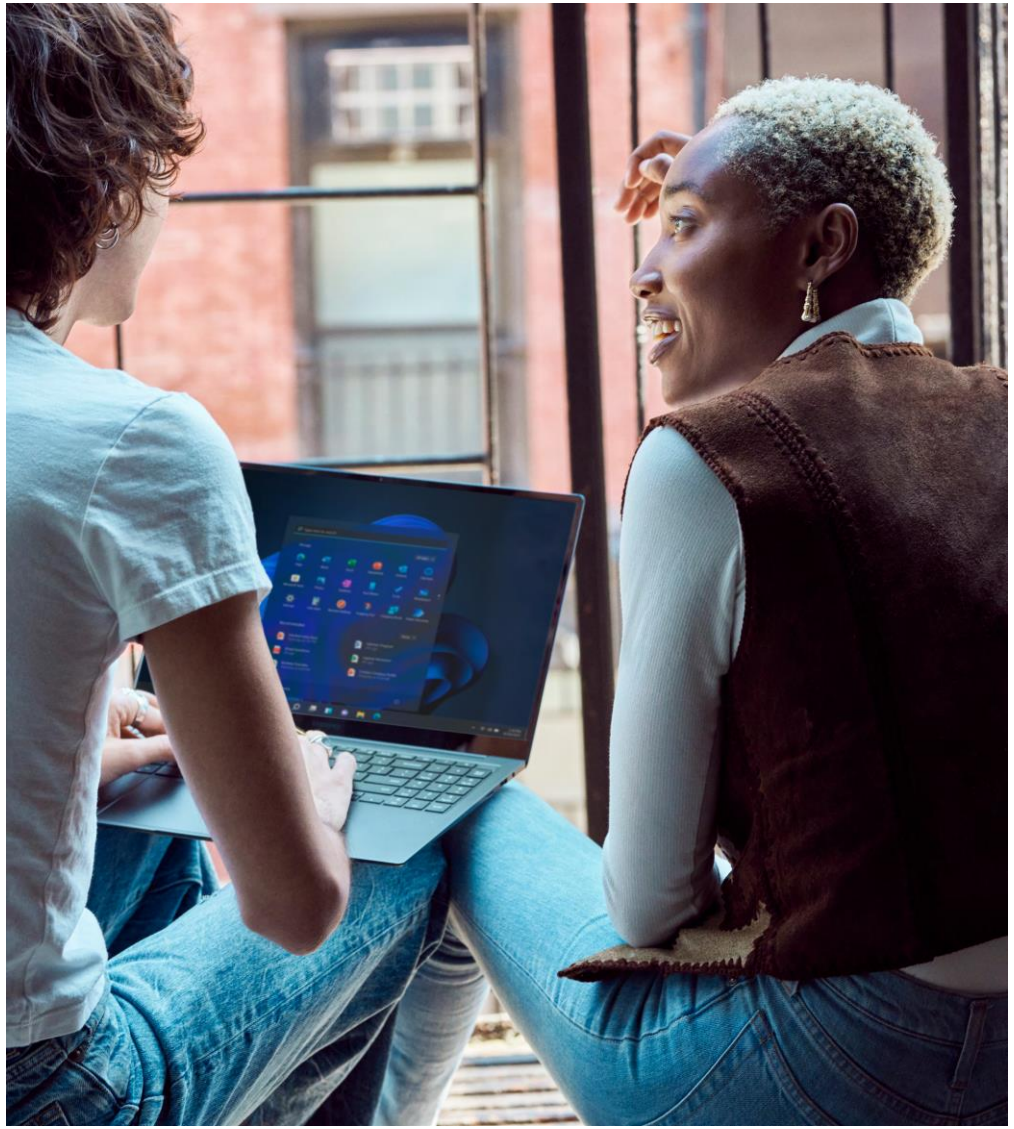
Leadership

- Con **leadership**, in italiano **direzione** o **comando** o **guida**, si intende la posizione di colui che in una struttura sociale organizzata occupa la posizione più elevata, nell'**interazione** col resto del **gruppo**.
  Tale figura viene generalmente definita **capo** o **guida** o **leader**.

Endpoint Vs castello: chi difendere

Inizia dall'endpoint

Un nuovo approccio alla modernizzazione
dei dispositivi, dei sistemi e del lavoro in team



L'endpoint è il nuovo ambiente di lavoro

- Il mondo è cambiato i lavoratori desiderano una maggiore flessibilità e i clienti cercano più convenienza.
- La diffusione del lavoro remoto, ha ispirato un nuovo approccio, che richiede un sistema operativo che includa tutte le funzionalità per gestire e proteggere la nostra leadership aziendale.
- Si tratta di un investimento fondamentale che semplifica le operazioni, protegge i dati e prepara l'azienda alla resilienza e alla crescita.

Definizione/Modernizzazione degli endpoint

- Procedure volte al miglioramento della facilità d'uso, delle performance hardware e software, delle funzionalità trasversali e della sicurezza di desktop, tablet e dispositivi mobili dei lavoratori, inclusi i dispositivi personali su cui vengono eseguite applicazioni di lavoro.

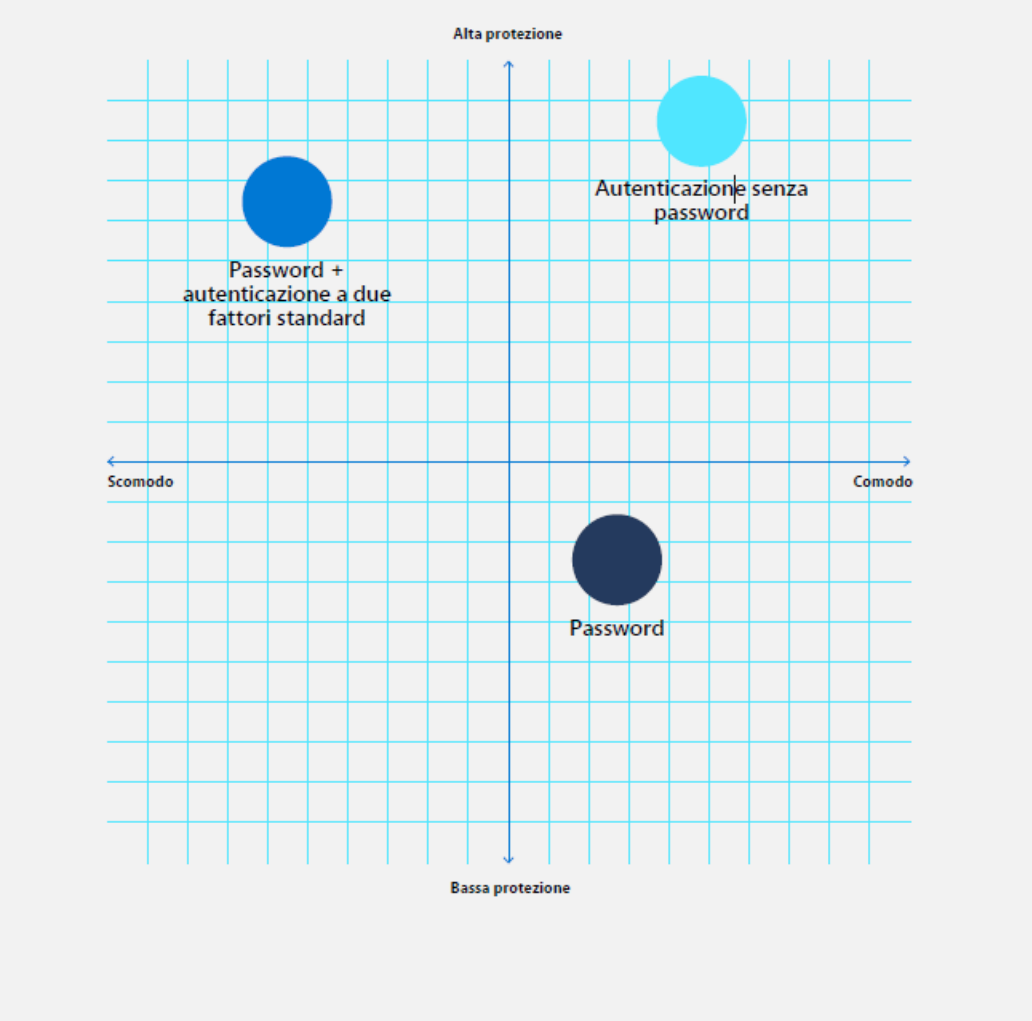
Aumenta la flessibilità modernizzando gli endpoint

In passato, la possibilità di lavorare sempre e ovunque, su qualsiasi dispositivo, era un vantaggio. Ora è un aspetto imprescindibile per la maggior parte delle persone e delle imprese.

1. In uno studio di Forrester commissionato da Microsoft, infatti, i datori di lavoro hanno dichiarato che l'uso dei dispositivi personali per il lavoro e una maggiore flessibilità sulla scelta di lavorare da casa o in ufficio migliorano la soddisfazione dei dipendenti e riducono il turnover.
2. Il passaggio da un dispositivo all'altro non può essere semplicemente possibile: deve essere facile e presentarsi in modo coerente ovunque.

Le persone devono poter creare una presentazione sul portatile, modificarla sul telefono e presentarla con il tablet, senza dover mai perdere tempo a risolvere i problemi relativi ai dispositivi.

Nuove minacce e nuove strategie …



L'autenticazione senza password è più sicura e conveniente rispetto ad altre opzioni

Offrire employee experience sorprendenti è sicuro !

Nel Work Trend Index 2022 di Microsoft, l'80% dei dipendenti ha dichiarato di aver mantenuto o superato il livello di produttività precedente da quando è passato alla modalità ibrida.

Il 57% dei dipendenti remoti sta valutando il passaggio all'ibrido, mentre il 51% dei dipendenti ibridi sta valutando il passaggio al remoto.

Inoltre, le posizioni remote su LinkedIn attirano 2,6 volte più visualizzazioni e quasi il triplo dei candidati rispetto ai lavori in ufficio.
Le imprese che offrono questa flessibilità grazie a un ambiente endpoint modernizzato spiccano in un mercato dei talenti competitivo.

Proteggi persone, dati e servizi

La sicurezza degli endpoint comincia da un approccio olistico Zero Trust

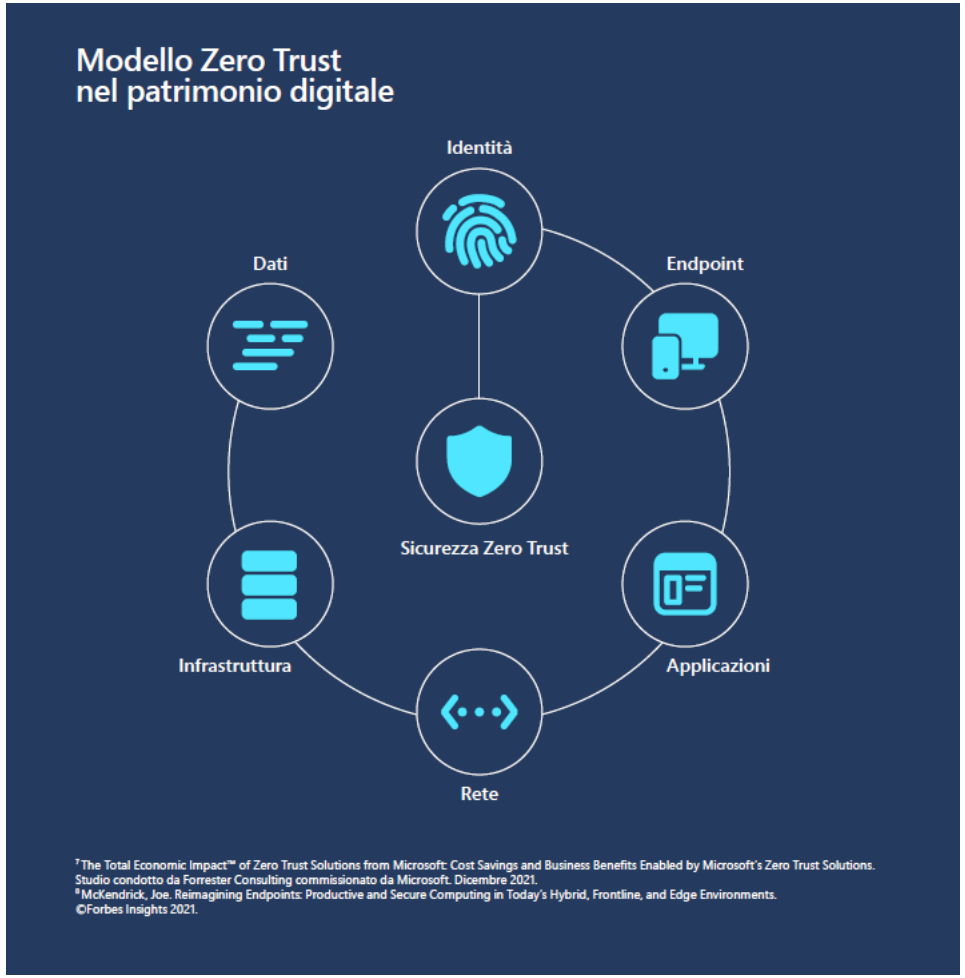
I principi del modello Zero Trust sono:

Verifica in modo esplicito. Esegui sempre l'autenticazione e l'autorizzazione includendo tutti i punti dati disponibili.

Usa l'accesso con privilegi minimi. Limita l'accesso degli utenti con approcci Just-In-Time e Just-Enough-Access, criteri adattivi basati sul rischio e protezione dei dati.

Presupponi la presenza di violazioni. Riduci al minimo il raggio di azione e segmenta l'accesso. Verifica la crittografia end-to-end e usa le analisi per migliorare la visibilità, il rilevamento delle minacce e le difese.

Microsoft incoraggia l'uso dei controlli Zero Trust per fornire visibilità, automazione e orchestrazione tra identità, endpoint, applicazioni, rete, infrastruttura e dati.

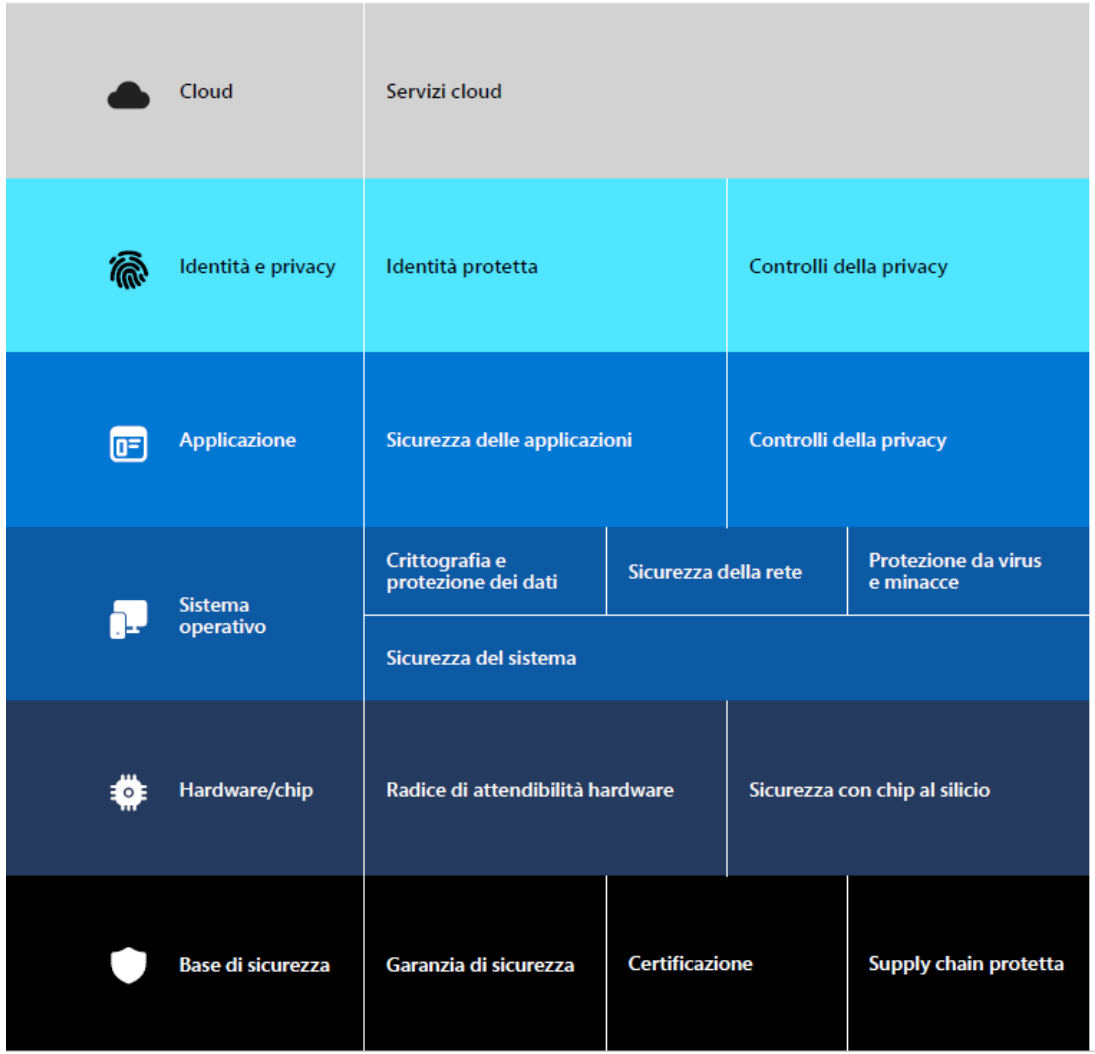


I sei livelli di sicurezza Zero Trust

Il modello Zero Trust si estende dal chip al cloud

Solide strategie di sicurezza end-to-end dovrebbero:

- Separare l'hardware dal software per la protezione da minacce: il dispositivo endpoint è protetto ancora prima di essere avviato.
- Proteggere il sistema operativo dall'accesso non autorizzato ai dati critici.
- Dare priorità alla sicurezza delle applicazioni e impedire l'accesso al codice non verificato.
- Proteggere le identità degli utenti con la sicurezza senza password.
- Estendere la sicurezza al cloud per proteggere i dispositivi, i dati, le app e le identità in remoto.



Mitiga rischi e vulnerabilità

Nell'immaginario comune, gli attacchi informatici sono visti come operazioni complesse e difficili da fermare. In realtà, **la maggior parte degli attacchi nasce dalla resistenza dei dipendenti a seguire le procedure consigliate per la sicurezza di base relative alla creazione delle password e all'identificazione dei tentativi di phishing**. Infatti, le password rubate sono di gran lunga la causa più diffusa della compromissione degli account e dei dati aziendali.

Anche gli attacchi sferrati dagli stati-nazione si basano in genere su tattiche semplici come il password spraying, che sfrutta la scelta di password deboli da parte dei dipendenti.

Nel solo 2021, Microsoft ha rilevato e bloccato più di 25 miliardi di tentativi di dirottare gli account aziendali.

Grazie!

eos solutions
A KUMAVISION GROUP COMPANY

- Bologna
- Bolzano
- Carpi
- Cuneo
- Milano
- Padova
- Treviso
- Udine
- Verona

WEB
www.eos-solutions.it