MICROSYS

# Roadmap to Modern M&A

*Il nostro approccio alla trasformazione dei gruppi di aziende*

# Scenario di business

Vi sono sempre più operazioni straordinarie di M&A che concentrano PMI in un unico nuovo contenitore aziendale.

L'informatica è protagonista:

- Mettendo le risorse in condizione di collaborare tra loro limitando al massimo discontinuità di servizio.
- Attivando una nuova infrastruttura di sistemi informativi adeguata e scalabile per il nuovo gruppo.
- Definendo le strategie e gli strumenti di governance e le azioni di Change Management.

Sicurezza, produttività, competenza, servizi mirati basati su contratti flessibili e cloud sono gli ingredienti che permettono di farlo.

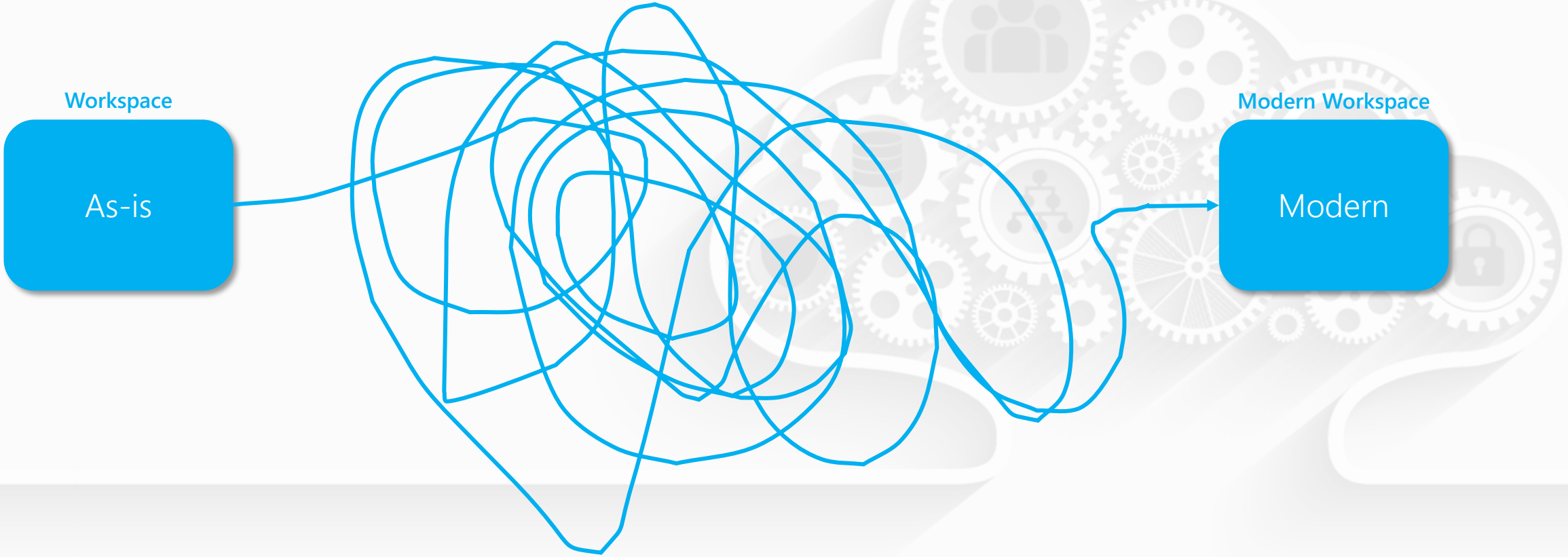
# Esigenze dei gruppi di aziende

- Mantenere la singola continuità operativa
- Impostare una governance di gruppo
- Aumentare la protezione e gestire la sicurezza
- Realizzare una comunicazione di gruppo
- Definire processi di onboarding o spin-off
- Ottimizzare e sfruttare gli investimenti

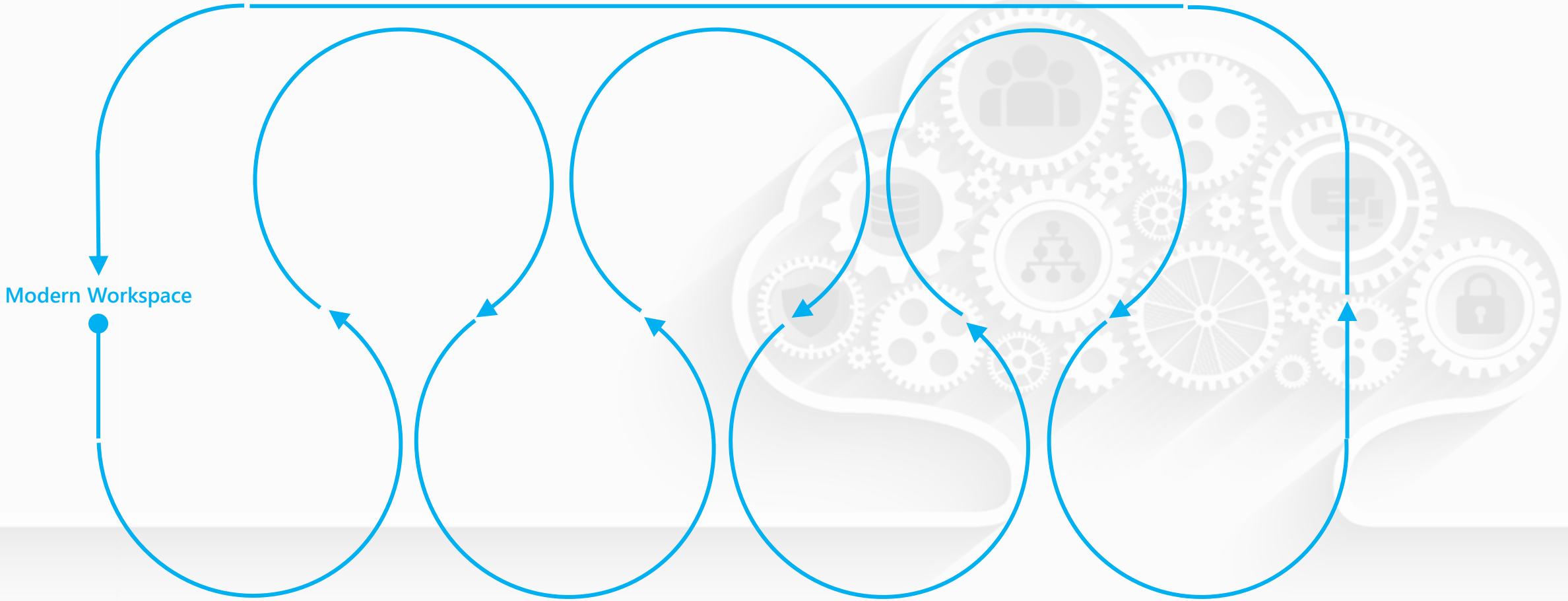
Definire un percorso operativo omnicomprensivo

# Il percorso ideale

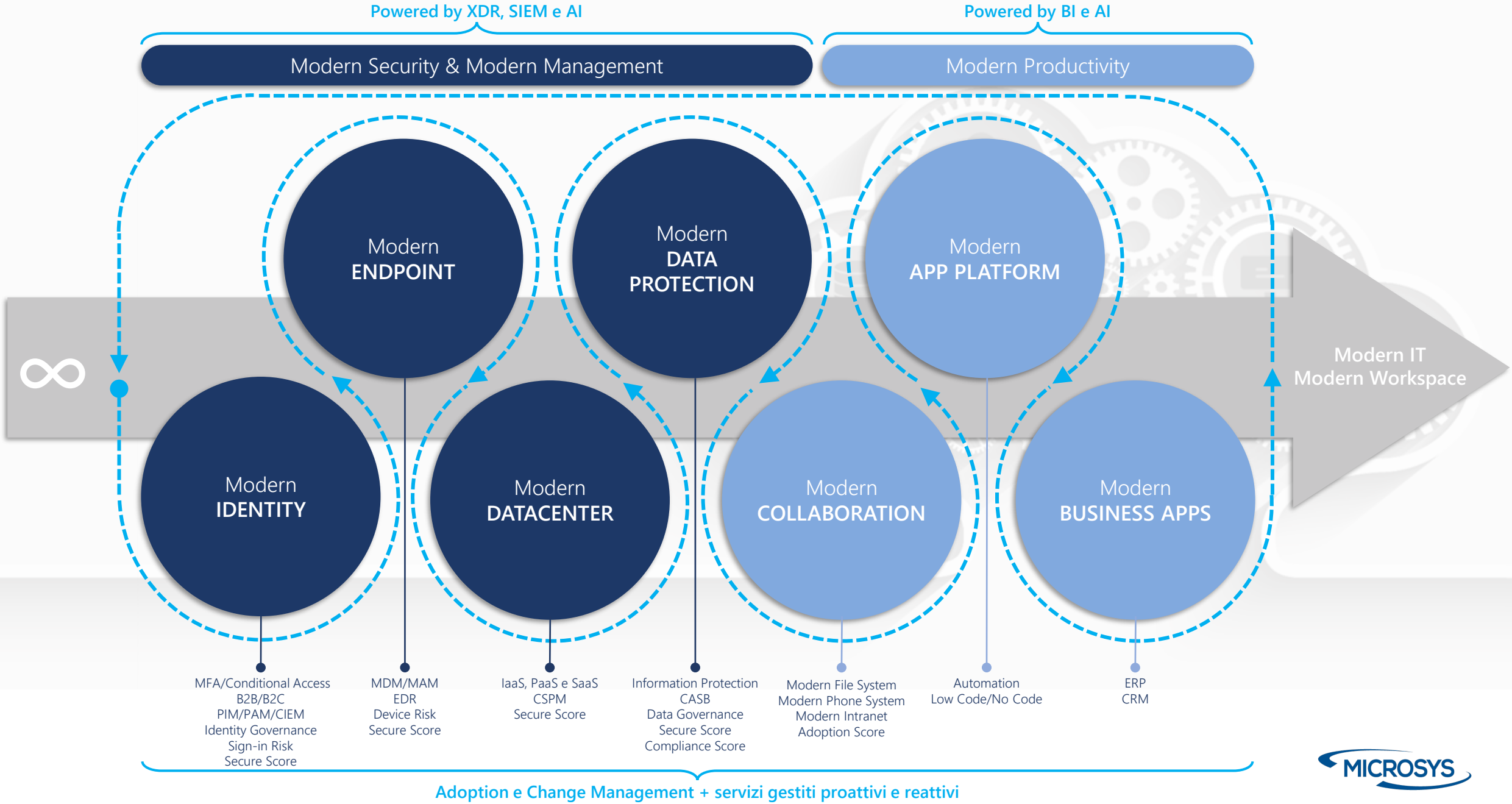
# Il rischio nascosto



# Il percorso sensato



# Continuous Modernization



# Il perimetro della proposta

Per ottimizzare i gruppi di aziende interveniamo nei seguenti ambiti:

- Sicurezza, infrastruttura e gestione
- Adoption e Change Management
- Collaborazione e produttività
- Licenze e contratti

- Governance servizi e ambiente
- Gestione proattiva a reattiva

# Componenti della proposta

# Avvio e primi passi

| | |
|---|---|
| **Documento di roadmap** | Interviste al personale IT e utenti per stesura documento con piano attività e valutazioni economiche* |
| **Licensing** | Assessment licenze (SAM) per tutte le società del gruppo |

**intervista al personale IT per l'ambito sicurezza e gestione, agli utenti per gli ambiti collaborazione, comunicazione, produttività e formazione*

MICROSYS

# Descrizione del deliverable

Documento di roadmap con:

- La attività nell'ordine migliore*
- Un'ipotesi di elapsed progettuale
- Le licenze necessarie con la miglior formula contrattuale
- Un budget progettuale complessivo
- Tabelle organizzative per gestire il percorso
  ("decisioni, azioni e motivazioni", "passaggi di consegne al personale IT o al team di gestione" e "stato completamento roadmap e chiusura attività»)

**organizzate negli ambiti identità e accessi, dispositivi, dati, infrastruttura, produttività e formazione*

# Esempio di documento di roadmap


## Roadmap to Modern IT

Percorso evolutivo di attività per l'aumento della sicurezza e per la modernizzazione dei sistemi e servizi IT

Fase 1 – febbraio 2023

### Introduzione

Con l'avvento dei servizi cloud perennemente e rapidamente in evoluzione, le necessità di nuove modalità di lavoro agile, le richieste da parte del business di avvio della trasformazione digitale e l'aumento delle minacce e degli attacchi informatici, molte organizzazioni devono affrontare una **necessaria e inevitabile modernizzazione dei propri sistemi informativi**.

La modernizzazione è un processo composto da varie attività che interagiscono tra loro; per renderle sostenibili e realizzabili bisogna incanalarle in una roadmap organizzata e razionalizzata per lo scenario di ogni organizzazione.

Generalmente le prime attività della roadmap agiscono sugli ambiti delle identità e degli accessi, della gestione dei dispositivi e della sicurezza; ovvero nel loro insieme, **la base su cui costruire le fondamenta tecnologiche per l'evoluzione continua dello scenario moderno.**

La roadmap può essere organizzata in vari ambiti, ognuno dei quali contiene le diverse attività tecniche. Ogni ambito potrebbe essere ripreso più volte nel tempo, andando a modernizzare ed evolvere con la giusta gradualità e continuità (**Continuous Modernization**); si armonizzano così gli impegni progettuali, si cadenzano gli investimenti sul licensing, si distribuisce l'impatto sull'utenza e si ottiene una costante introduzione delle nuove tecnologie e dei relativi benefici.

Nello scenario moderno gradualmente introdotto dal processo di continua modernizzazione, tutti i servizi tendono a essere fruibili via Internet e di conseguenza lo devono essere anche la gestione e il controllo degli utenti e dei dispositivi. Un effetto e una positiva conseguenza di tutto questo è la realizzazione di uno **scenario senza differenze tra perimetro interno (LAN) ed esterno (Internet)**, arrivando a poter considerare tutti gli utenti e tutti i dispositivi sempre come esterni, anche quando sono in ufficio. Per raggiungere tale scenario, tecnicamente si deve tendere ad abbandonare i protocolli di autenticazione privati e proprietari (NTLM e Kerberos) a favore di protocolli di autenticazione open e standard (oAuth, SAML 2.0, Open ID Connect).

Le strategie di sicurezza, da considerarsi ormai fondamentali in tutte le roadmap di modernizzazione, si devono quindi concentrare su dei rigorosi controlli degli accessi (Conditional Access), sulla protezione delle identità digitali (che diventano il nuovo Firewall), dei dispositivi (qualsiasi essi siano) e dei dati (ovunque si trovino). **In sostanza si tende ad adottare il modello di sicurezza Zero Trust**.

Durante l'esecuzione delle varie fasi della roadmap, non sarà mai trascurato uno degli aspetti fondamentali per aumentare la sicurezza, ovvero **la protezione delle credenziali privilegiate (anche dette "le chiavi del regno")**. Saranno quindi gradualmente introdotti tutti i processi e le tecnologie utili alla protezione degli account amministrativi interni ed esterni di Active Directory e Azure AD.

Saranno anche effettuate diverse attività per la modernizzazione ed evoluzione dei servizi di produttività (**Modern Productivity**), calate sulla base tecnologica, sulle strategie di sicurezza e di gestione introdotte (Modern Security and Modern Management). La produttività moderna è focalizzata primariamente sull'utilizzo di **OneDrive, SharePoint Online e Teams** per poi svilupparsi nell'adozione della Power Platform e nell'integrazione con le Dynamics Business Apps di Microsoft, aumentando così esponenzialmente i benefici operativi agli utenti.

### Approccio alla modernizzazione della sicurezza

La difesa perimetrale è da considerarsi obsoleta nell'era cloud e dello Smart Working. Tale modello di sicurezza assume che ciò che è all'interno del perimetro è sicuro ed è qualcosa di cui ci fidiamo. Con l'aumento dei dispositivi mobili, l'adozione dei servizi cloud, le esigenze BYOD, il fenomeno dello Shadow IT e le sempre più sofisticate tecniche di Phishing, la difesa perimetrale è ormai irrilevante. Per tali motivi si suggerisce il **modello di sicurezza Zero Trust;** la sua adozione potrebbe richiedere la revisione di scelte fatte in passato, l'introduzione di nuovi strumenti e la riorganizzazione di ambiti gestionali. Di seguito alcuni elementi che agevolano l'adozione del modello:

- Azure AD con i suoi meccanismi di autenticazione e accesso condizionale.
- La rimozione di ADFS a favore di PHS e la dismissione delle connessioni VPN.
- La revisione delle modalità di esposizione dei servizi e risorse on-premise.
- L'associazione dei PC ad Azure AD e l'adozione di uno strumento per la gestione moderna dei dispositivi.

Il modello **Zero Trust per approccio assume l'avvenuta violazione** e quindi le attività di sicurezza dovrebbero anche prevedere sempre la verifica esplicita per autenticare e autorizzare gli accessi, l'adozione di un modello Least Privileged Access per segmentare gli accessi, la verifica continua della vulnerabilità a cui si è esposti e la verifica continua dello stato delle configurazioni di sicurezza. Le attività sopra indicate sono possibili con strumenti avanzati di sicurezza, come:

- **Defender for Office 365:** protezione avanzata minacce da posta elettronica
- **Defender for Endpoint:** protezione avanzata dispositivi e Continuos VA
- **Defender for Identity:** controllo attività anomale identità di Active Directory.
- **Defender for Cloud Apps:** protezione dati e controllo Shadow IT.
- **Defender for Cloud:** protezione avanzata dei workload cloud.
- **Microsoft Sentinel:** moderno SIEM per correlare tutti gli eventi di sicurezza.

Tali strumenti interagiscono realizzando un sistema **Layered Security**, aumentando la protezione a vari livelli e consentendo verifiche esplicite, automazioni e capacità di risposta nei vari stadi di un attacco. Questo permette l'approccio alle attività di sicurezza con il metodo **"Protect–Detect–Respond"**. Gli strumenti introdotti non devono essere abbandonati dopo la loro adozione poiché producono informazioni che devono essere valutate da personale IT. Si suggerisce quindi l'implementazione di periodici processi di controllo svolti da personale interno o esterno (servizio gestito proattivo o reattivo).

Un ambito di particolare attenzione, poiché eventuali debolezze in tale ambito sono sfruttate per completare attacchi con successo, è la protezione delle credenziali privilegiate di Active Directory e Azure AD. Tramite l'adozione del **modello Secure Privileged Access (SPA)** di Microsys, ispirato al modello Microsoft Enanched Security Administration Environment (ESAE) e al modello **Enterprise Access Model**, è possibile aumentare la protezione delle credenziali privilegiate e diminuire le probabilità di successo di note tecniche di attacco (**Lateral Movement ed Escalation of Privileges**). Nel caso di Azure AD, le attività di protezione delle credenziali privilegiate si concentreranno sull'adozione di uno strumento di **Privilege Identity Management** (Azure AD PIM).

### Approccio alla modernizzazione della produttività

Migliorare la produttività significa risparmiare tempo per raggiungere un maggior numero di risultati; questo è possibile eliminando tutte le barriere e mantenendo uno stretto contatto fra le risorse dei vari team, ovunque esse siano. Si mantengono così più facilmente le persone aggiornate e si assicura che ognuno possa condividere efficacemente le proprie idee e il proprio lavoro. Di fatto migliorare la produttività significa ottimizzare la comunicazione e la collaborazione fra i team e ridurre il tempo dedicato ad attività ripetitive a basso valore aggiunto tramite una diffusa automazione dei processi di business più comuni e ripetitivi. Questi obiettivi sono facilmente raggiungibili con **strumenti e soluzioni moderne di collaborazione** progettate per questo scopo, come:

- **OneDrive for Business:** storage di file personali che permette di lavorare in mobilità sui propri contenuti.
- **Microsoft Teams:** progettato per comunicare e collaborare in un unico posto.
- **SharePoint Online:** realizzato per condividere le proprie idee, le informazioni e i documenti di lavoro, per la creazione condivisa e la modifica in contemporanea di contenuti da parte di più persone.
- **Power Platform:** consente l'implementazione low-code di processi di business e l'automazione di attività ripetitive e time-consuming.

Quanto indicato sopra sempre in sicurezza, infatti si appoggio e rispetta quanto progettato nella fase di modernizzazione della sicurezza e della gestione.

### Introduzione e descrizione della roadmap

È stata eseguita un'approfondita intervista organizzata in 6 ambiti (**identità e accessi, dispositivi, dati, infrastruttura, produttività e formazione**), con l'obiettivo di raccogliere le informazioni utili per definire le attività, le priorità del percorso di modernizzazione e per rilevare gli ambiti con maggiori criticità o di impellente bisogno. Di seguito le attività per ognuno degli ambiti trattati:

| Fase | Ambito | Numero di attività previste |
|---|---|---|
| 1 | 1. Identità e accessi | 4 |
| 1 | 2. Dispositivi | 4 |
| 1 | 3. Dati | 1 |
| 1 | 4. Infrastruttura | 1 |
| 1 | 5. Produttività | 2 |
| 1 | 6. Formazione | 2 |

Nel loro insieme, queste attività perseguono le strategie di modernizzazione nei vari ambiti trattati e sono tra di loro utili per cercare di ridurre e armonizzare l'impegno progettuale, gli impatti sul personale IT e sugli utenti. Per ogni attività proposta, vengono dichiarate le stime dei costi progettuali e le licenze necessarie.

Viene anche proposta una ulteriore suddivisione delle attività e quindi del carico di lavoro e degli investimenti, dividendo la roadmap in 4 diversi scenari (minimo, standard, avanzato e completo).

### Descrizione attività fase 1

L'analisi ha prodotto un **piano di 14 attività** che aumenta la sicurezza e migliora la collaborazione di base tra le persone e i team di lavoro.

Si prevede di sviluppare la roadmap in **arco temporale massimo di 6 mesi** con un impegno stimato per il personale di BRAVO INVEST di circa 2 giorni al mese.

Le attività della fase 1 sono un mix tra attività tecniche, di sicurezza e di adozione base degli strumenti moderni di collaborazione degli utenti.

Grazie alle attività tecniche e di sicurezza si aumenta la protezione, si migliora la postura di sicurezza tendendo al modello Zero Trust e si introducono capacità di gestione moderna (Modern Management). Per raggiungere questi obiettivi si agisce primariamente sulle identità, sugli accessi e sui dispositivi. I benefici di sicurezza si massimizzano applicando, dove possibile, le funzionalità di sicurezza introdotte a tutte le applicazioni, servizi e risorse.

In questa fase si inizia anche l'adozione di base degli strumenti moderni di collaborazione, introducendo per tutti gli utenti OneDrive for Business (storage di file personali), Teams (collaborazione audio/video e store di file di team di lavoro) e SharePoint Online (storage di file di team di lavoro o dipartimento), proponendo l'adeguata formazione e gestione del cambiamento.

Inoltre, sono state specificate le tipiche azioni di **Operations (change e incident)** che potrebbe essere necessario eseguire a seguito dell'adozione dei vari strumenti e servizi. Nello scenario di Bravo Invest, ovvero senza personale IT dedicato, queste operazioni saranno probabilmente eseguire da una terza parte.

È proposta anche un'ipotesi di **attività suggerite successive (fase 2)**; sono attività sempre volte ad aumentare la sicurezza e la produttività e sono una conseguenza logica e coerente delle attività e strategie adottate in questa fase.

### Valutazione e ordine di esecuzione delle attività previste

| Cod. | Attività | Ambito | Funzionalità | Licenze | Scenario | Effort | Impatto IT | Impatto utenza | Beneficio sicurezza |
|---|---|---|---|---|---|---|---|---|---|
| 1.4.01 | Revisione infrastruttura di rete | Infrastruttura | - | No | Minimo | Basso | Basso | Basso | Basso |
| 1.5.01 | Adozione Modern Phone System | Produttività | - | Si | Minimo | Alto | Medio | Alto | Basso |
| 1.6.01 | Formazione utenti Modern Phone System | Formazione | - | No | Minimo | - | - | - | - |
| 1.1.01 | Aumento protezione credenziali privilegiate | Identità e accessi | Protect | Si | Minimo | Basso | Basso | Basso | Alto |
| 1.1.02 | Aumento protezione identità | Identità e accessi | Protect | Si | Minimo | Basso | Basso | Alto | Alto |
| 1.1.03 | Aumento protezione posta elettronica | Identità e accessi | Protect | Si | Standard | Basso | Basso | Basso | Medio |
| 1.2.01 | Aumento protezione dispositivi | Dispositivi | Protect | Si | Standard | Medio | Medio | Basso | Alto |
| 1.2.02 | Aumento postura di sicurezza dispositivi | Dispositivi | Protect-Detect-Respond | Si | Avanzato | Basso | Basso | Basso | Alto |
| 1.5.02 | Adozione Modern File System | Produttività | - | No | Minimo | Alto | Alto | Alto | Medio |
| 1.6.02 | Formazione utenti Modern File System | Formazione | - | No | Minimo | - | - | - | - |
| 1.3.01 | Aumento protezione dati | Dati | Protect | Si | Avanzato | Basso | Basso | Basso | Medio |
| 1.1.04 | Aumento protezione accessi Salesforce | Identità e accessi | Protect | Si | Completo | Basso | Basso | Medio | Alto |
| 1.2.03 | Aumento protezione esecuzione applicazioni | Dispositivi | Protect | Si | Completo | Basso | Basso | Medio | Alto |
| 1.2.04 | Adozione processo moderno di rilascio dei dispositivi | Dispositivi | - | Si | Completo | Medio | Medio | Basso | Medio |

### Decisioni e motivazioni

| Cod. | Attività | Decisioni | Motivazioni |
|---|---|---|---|
| 1.4.01 | Revisione infrastruttura di rete | ▪ data:decisione | ▪ motivazione |
| 1.5.01 | Adozione Modern Phone System | | |
| 1.6.01 | Formazione utenti Modern Phone System | | |
| 1.1.01 | Aumento protezione credenziali privilegiate | | |
| 1.1.02 | Aumento protezione identità | | |
| 1.1.03 | Aumento protezione posta elettronica | | |
| 1.2.01 | Aumento protezione dispositivi | | |
| 1.2.02 | Aumento postura di sicurezza dispositivi | | |
| 1.5.02 | Adozione Modern File System | | |
| 1.6.02 | Formazione utenti Modern File System | | |
| 1.3.01 | Aumento protezione dati | | |
| 1.1.04 | Aumento protezione accessi Salesforce | | |
| 1.2.03 | Aumento protezione esecuzione applicazioni | | |
| 1.2.04 | Adozione processo moderno di rilascio dei dispositivi | | |

### Stato completamento roadmap e chiusura attività

| Cod. | Attività | Stato | Note |
|---|---|---|---|
| 1.4.01 | Revisione infrastruttura di rete | Da fare | ▪ data: testo |
| 1.5.01 | Adozione Modern Phone System | Da fare | |
| 1.6.01 | Formazione utenti Modern Phone System | Da fare | |
| 1.1.01 | Aumento protezione credenziali privilegiate | Da fare | |
| 1.1.02 | Aumento protezione identità | Da fare | |
| 1.1.03 | Aumento protezione posta elettronica | Da fare | |
| 1.2.01 | Aumento protezione dispositivi | Da fare | |
| 1.2.02 | Aumento postura di sicurezza dispositivi | Da fare | |
| 1.5.02 | Adozione Modern File System | Da fare | |
| 1.6.02 | Formazione utenti Modern File System | Da fare | |
| 1.3.01 | Aumento protezione dati | Da fare | |
| 1.1.04 | Aumento protezione accessi Salesforce | Da fare | |
| 1.2.03 | Aumento protezione esecuzione applicazioni | Da fare | |
| 1.2.04 | Adozione processo moderno di rilascio dei dispositivi | Da fare | |

# Linee guida – sicurezza e gestione

- La destinazione finale a cui tendere deve essere uno scenario senza differenze tra perimetro interno (LAN) ed esterno (Internet), considerando utenti e dispositivi sempre come esterni, anche quando sono in ufficio
- Utenti e dispositivi («tier 2») devono essere consolidati in una foresta AD centrale con applicato il «tiering model» e in relazione con Azure AD. Se possibile, associare il «tier 2» direttamente in Azure AD («Azure AD Join»).
- La vera sfida tecnica è abbandonare i protocolli di autenticazione privati e proprietari (NTLM e Kerberos) per tutte le applicazioni, servizi e risorse a favore di protocolli open e standard (oAuth, SAML 2.0 e Open ID Connect).
- Iniziare a categorizzare tutti i dispositivi come «gestiti» (quindi gestiti con tecniche «MDM») oppure «non gestiti» (quindi gestiti con tecniche «MAM») e la loro gestione deve diventare «internet-based».
- Le strategie di sicurezza possono essere semplificate se si blocca l'accesso i dispositivi personali (BYOD).
- Si tende ad abbandonare le connessioni VPN, che sono un sistema per portare dentro chi è fuori, a favore di autenticazioni native Azure AD oppure tramite Azure AD Application Proxy.
- In certi scenari l'utilizzo di «VDI as a Service» potrebbe facilitare e velocizzare l'adozione del modello Zero Trust.
- Tendere ad applicare policy di sicurezza con il metodo di esclusione ad un gruppo.
- UPN sempre e comunque esattamente uguale all'indirizzo email.
- Dopo l'attivazione del Self-service Password Reset (SSPR), togliere i permessi «orizzontali» agli utenti Help Desk su tutte le password.

MICROSYS

# Linee guida – collaborazione e produttività

- Definire una chiara mappatura tra contenuti e funzionalità in cui farli risiedere
- Iniziare a classificare il dato caldo e il dato freddo, importante per eventuali ottimizzazioni nel passaggio ai servizi cloud
- Definire per ogni strumento di collaborazione il modello di governance e le relative procedure e strumenti di gestione
- Rivedere o progettare di una Intranet di gruppo basata sugli stessi strumenti di collaborazione e comunicazione a disposizione
- Verificare l'opportunità di inserire strumenti per il controllo della compliance rispetto a quanto definito

MICROSYS

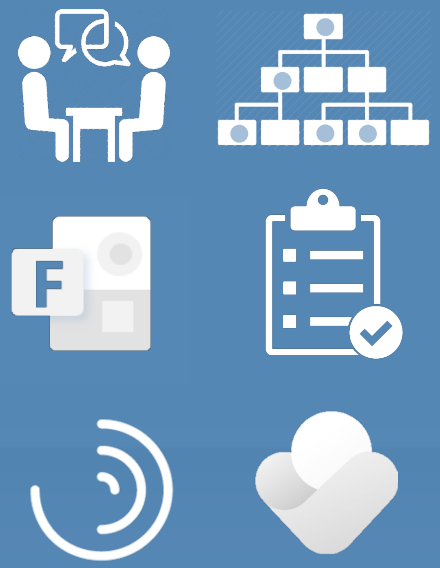
# Linee guida – Adoption e Change Management

Ogni trasformazione digitale comporta un processo di cambiamento e una profonda evoluzione culturale perché abbia successo duraturo l'adozione delle nuove tecnologie deve essere adeguatamente gestita

## Model

- Awareness
- Desire
- Knowledge
- Ability
- Reinforcement

## Assessment



## Design

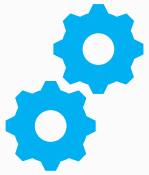
## Delivery


MICROSYS

# Il ruolo e le capacità del nostro gruppo

Sempre più attività di «advisory»

Competenze ed esperienze interdisciplinari

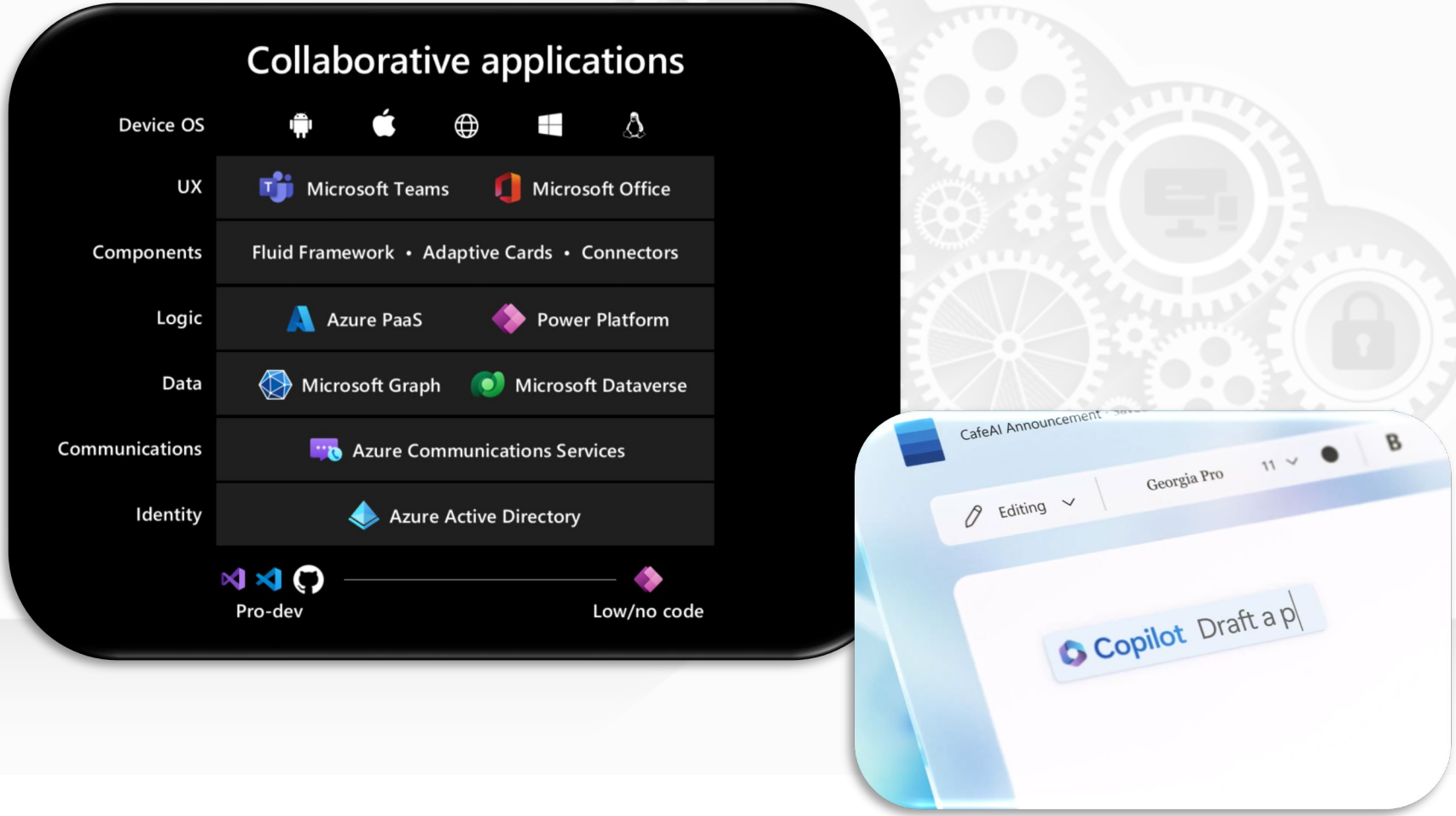


Capacità tecniche su tutto lo stack Microsoft (e di altri partner strategici)

Presidio per i servizi gestiti (dalla progettazione alla gestione)

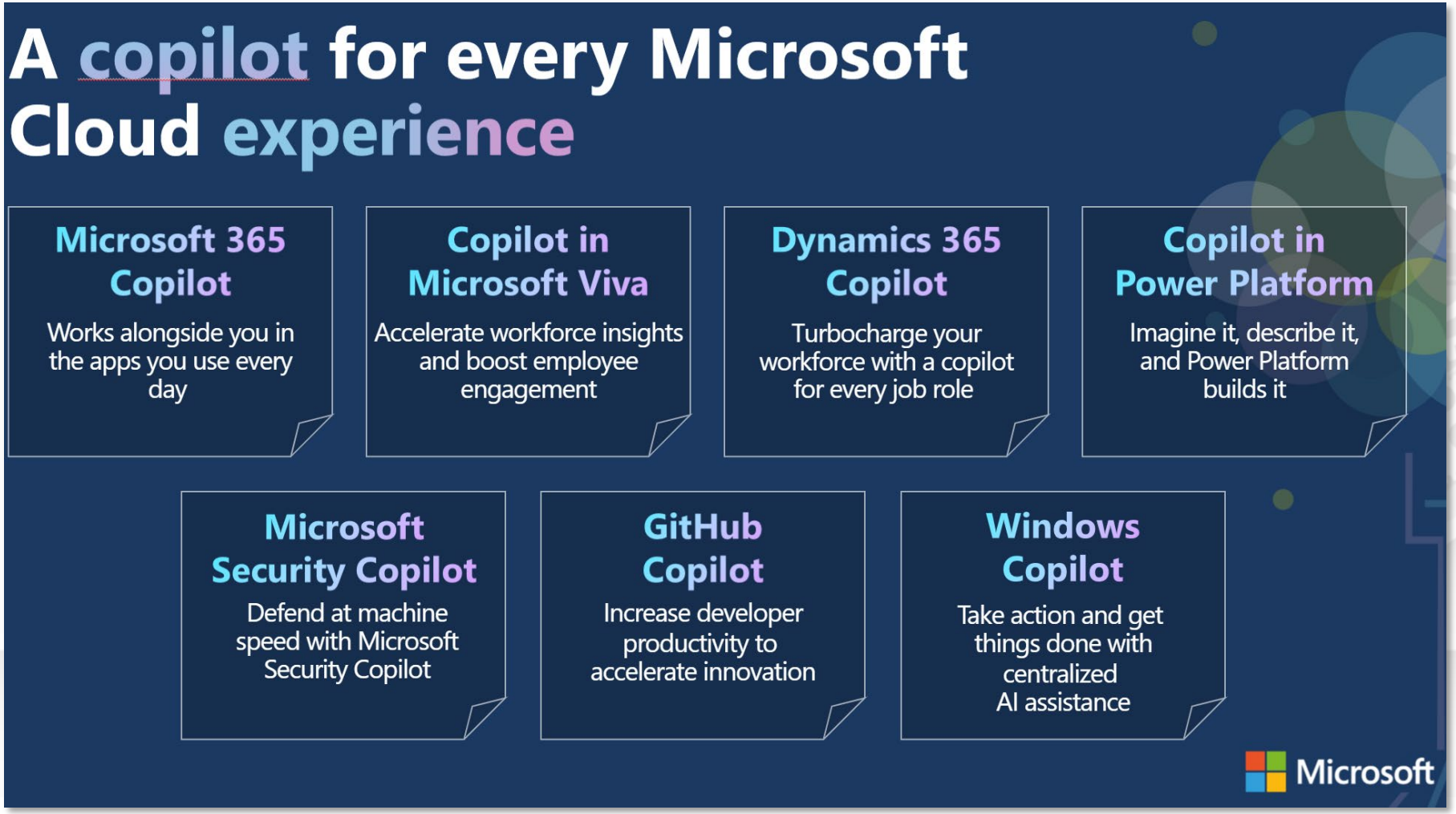
# Allegati

Microsoft




MICROSYS

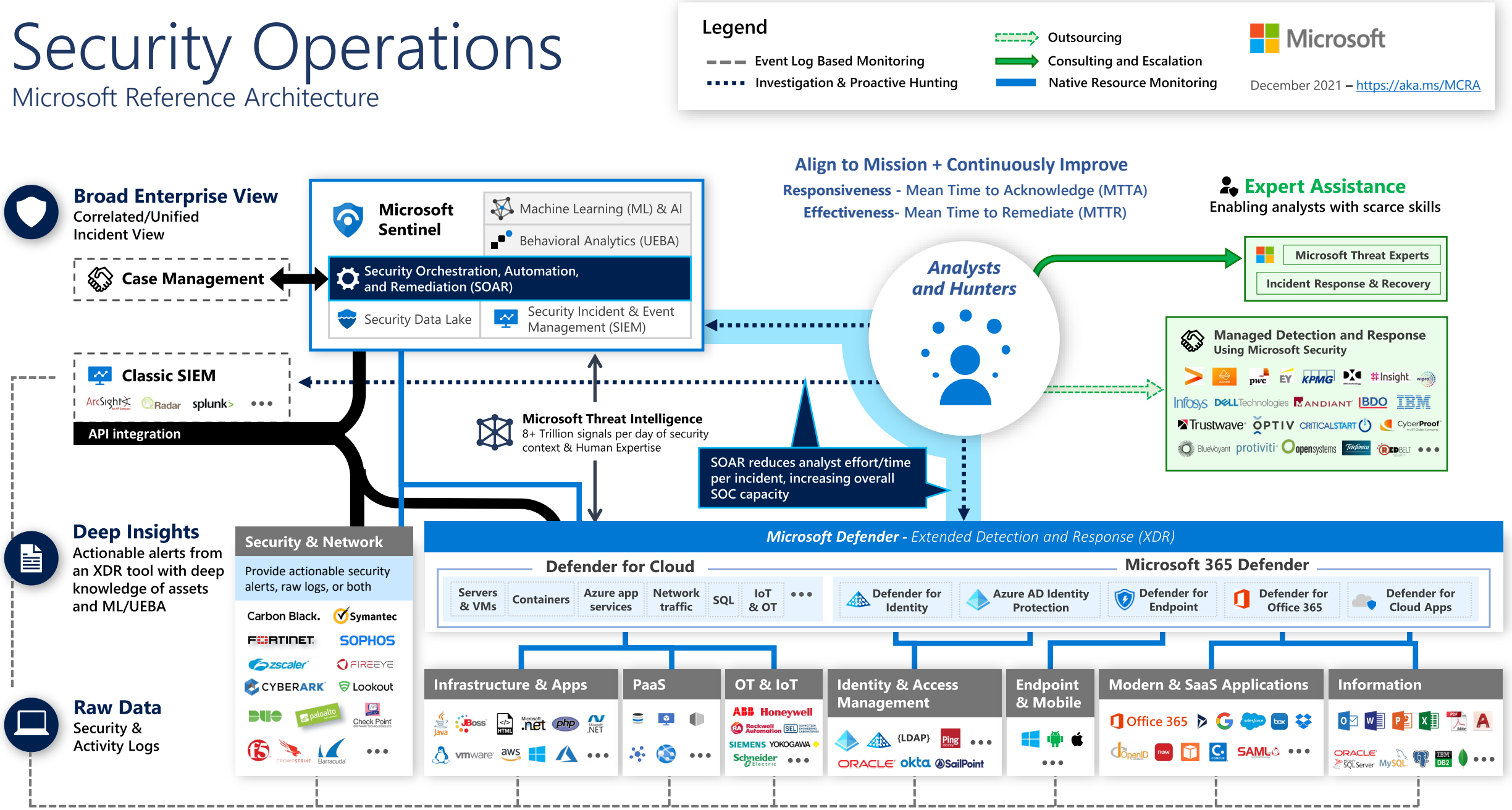
Microsoft




MICROSYS

# Security Operations

## Microsoft Reference Architecture



MICROSYS

# Roadmap to Modern M&A

*Il nostro approccio alla trasformazione dei gruppi di aziende*