MICROSYS

Roadmap to Modern Security

Il nostro approccio per definire ed eseguire un piano di attività di sicurezza tendendo al modello Zero Trust

Roadmap to Modern Security

Approccio consulenziale e metodologico per definire il miglior percorso di attività utili a migliorare la postura di sicurezza tendendo al **modello Zero Trust.**

Modello di sicurezza Zero Trust

Invece di assumere che tutto quello che è dietro al Firewall è sicuro, il modello per assunzione predefinita considera ogni tentativo di accesso a qualsiasi risorsa come potenzialmente pericoloso **(Never Trust)** *e quindi prevede sempre dei controlli delle condizioni di autenticazione e di autorizzazione per ogni singolo tentativo di accesso a qualsiasi risorsa* **(Always Verify).**

MICROSYS

Le strategie di base della sicurezza moderna

Le strategie di sicurezza moderna devono primariamente prevedere:

- dei rigorosi controlli delle **condizioni di accesso,** non solo utente e password
- l'aumento della protezione delle **identità,** che diventano il nuovo Firewall
- l'aumento della protezione dei **dispositivi,** qualsiasi essi siano
- l'aumento della protezione dei **dati,** ovunque si trovino

Nota: è ovviamente anche coperto l'ambito delle infrastratture on-premise legacy (se presenti e se ha ancora senso aumentarne la postura di sicurezza).

MICROSYS

Lo scenario finale

Si vuole realizzare uno scenario senza differenze gestionali e operative tra perimetro interno (le LAN) e perimetro esterno (Internet), arrivando a considerare **tutti gli utenti e dispositivi sempre come esterni** anche quando sono in ufficio.

Alcune note tecniche e raccomandazioni

- Si deve tendere 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.
- Si deve tendere ad abbandonare i protocolli di autenticazione privati e proprietari (NTLM e Kerberos) a favore di protocolli open e standard **(oAuth, SAML 2.0 e Open ID Connect).**
- Categorizzare tutti i dispositivi come «gestiti» oppure «non gestiti» e la loro gestione deve diventare «internet-based».
- Applicare configurazioni **Mobile Device Management (MDM)** in caso di dispositivi **gestiti (Corporate Owned Device o COD)** oppure **Mobile Application Management (MAM)** in caso di dispositivi non gestiti **(Bring Your Own Device o BYOD).**
- In certi scenari l'utilizzo di **«VDI as a Service»** potrebbe velocizzare l'evoluzione e facilitare l'adozione del modello Zero Trust.
- Tendere ad applicare policy di sicurezza con il metodo della esclusione ad un gruppo. Per esempio, per applicare MFA tramite Conditional Access, applicare la policy con l'esclucione ad un gruppo di utenti con membri tutti gli utenti. Per applicare MFA quindi basta togliere gli utenti dal gruppo gradualmente, così i nuovi utenti «nascono» con MFA applicato.

MICROSYS

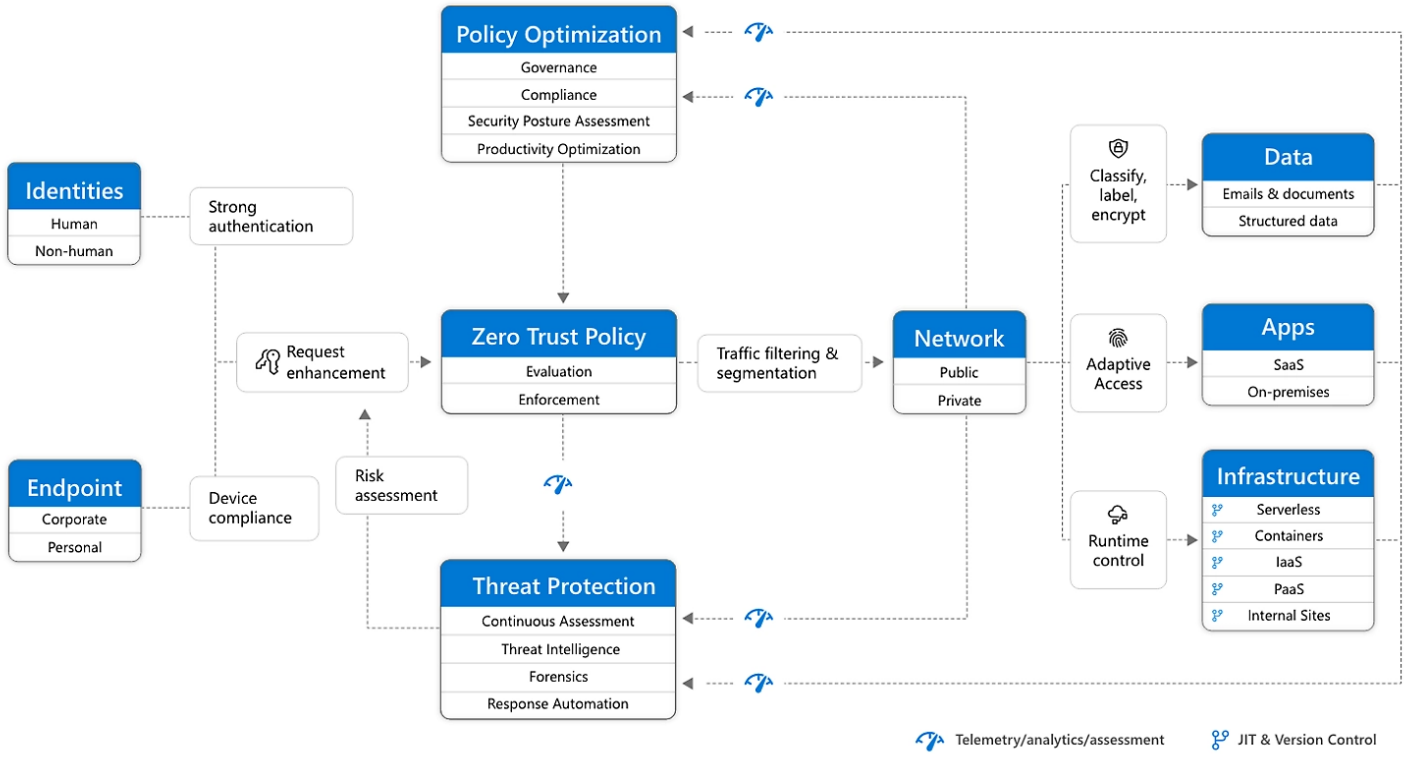
Lo scenario finale di base

A holistic approach to Zero Trust should extend to your entire digital estate inclusive of identities, endpoints, network, data, apps, and infrastructure. Zero Trust architecture serves as a comprehensive end-to-end strategy and requires integration across the elements. The foundation of Zero Trust security is identities. Both human and non-human identities need strong authorization, connecting from either personal or corporate endpoints with compliant devices, requesting access based on strong policies grounded in Zero Trust principles of explicit verification, least-privilege access, and assumed breach.

As a unified policy enforcement, the Zero Trust policy intercepts the request, explicitly verifies signals from all six foundational elements based on policy configuration and enforces least-privilege access. Signals include the role of the user, location, device compliance, data sensitivity, and application sensitivity. In additional to telemetry and state information, the risk assessment from threat protection feeds into the policy engine to automatically respond to threats in real time. Policy is enforced at the time of access and continuously evaluated throughout the session.
This policy is further enhanced by policy optimization. Governance and compliance are critical to a strong Zero Trust implementation. Security posture assessment and productivity optimization are necessary to measure the telemetry throughout the services and systems.

The telemetry and analytics feeds into the threat protection system. Large amounts of telemetry and analytics enriched by threat intelligent generates high-quality risk assessments that can either be manually investigated or automated. Attacks happen at cloud speed and because humans can't react quickly enough or sift through all the risks, your defense systems must also act at cloud speed. The risk assessment feeds into the policy engine for real-time automated threat protection and additional manual investigation if needed. Traffic filtering and segmentation is applied to the evaluation and enforcement from the Zero Trust policy before access is granted to any public or private network.

Data classification, labeling, and encryption should be applied to emails, documents, and structured data. Access to apps should be adaptive, whether SaaS or on-premises. Runtime control is applied to infrastructure with serverless, containers, IaaS, PaaS, and internal sites with just-in-time (JIT) and version controls actively engaged.
Finally, telemetry, analytics, and assessment from the network, data, apps, and infrastructure are fed back into the policy optimization and threat protection systems.



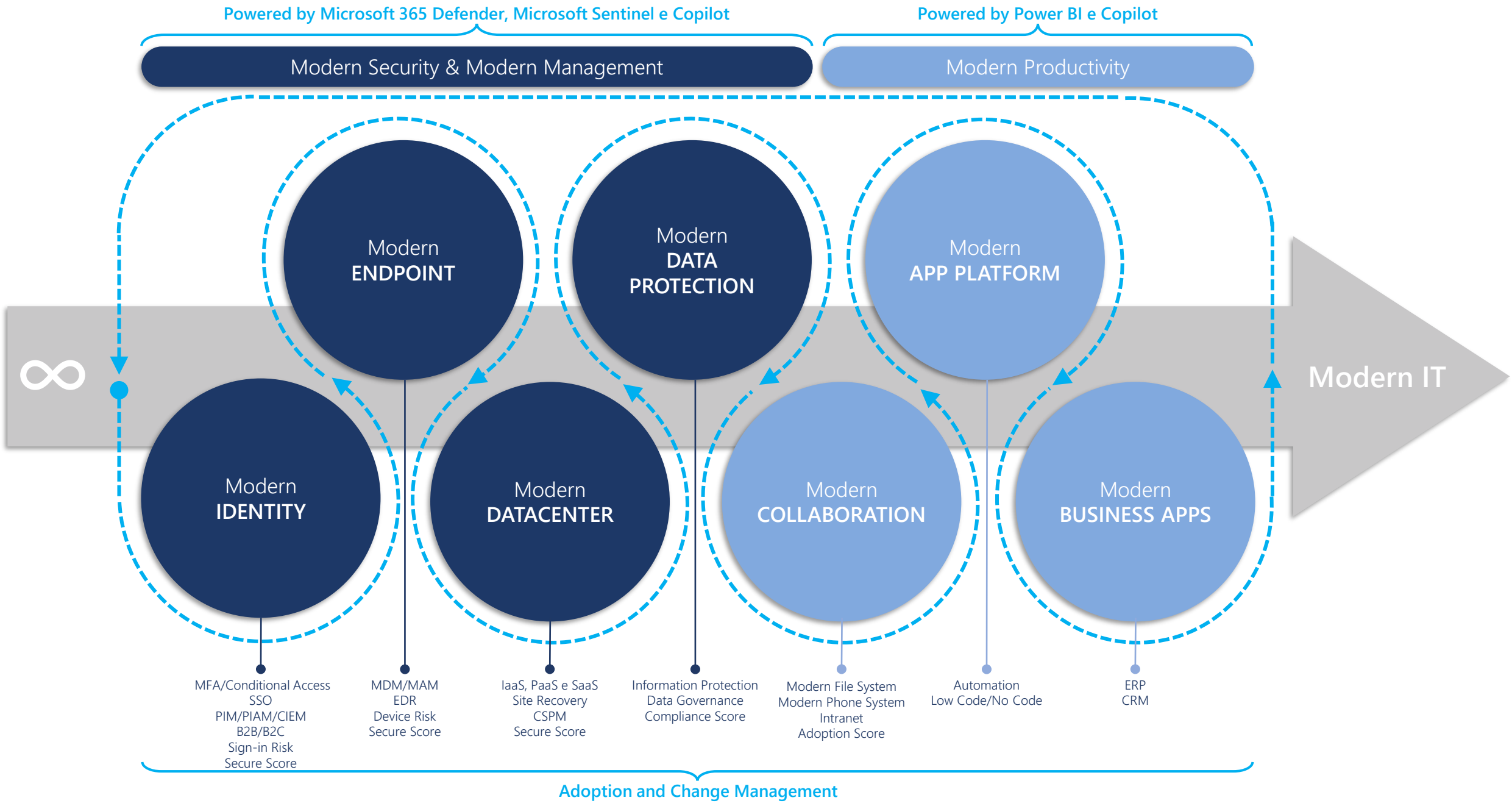
Zero Trust defined

Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify." Every access request is fully authenticated, authorized, and encrypted before granting access. Microsegmentation and least-privilege access principles are applied to minimize lateral movement. Rich intelligence and analytics are utilized to detect and respond to anomalies in real time.

Il percorso e la trasformazione

Adottare le strategie di sicurezza moderna e tendere al modello Zero Trust è una trasformazione **potenzialmente lunga e complessa** ed è quindi importante accordarsi sullo scenario finale da perseguire e descrivere il percorso per arrivarci.

Il nostro approccio (Continuous Modernization)



Lo strumento consulenziale

A seguito di una approfondita intervista al personale IT (di circa 70 domande), si produce un documento di roadmap che diventa lo «strumento» di base per gestire il percorso.

Roadmap to Modern Security

Roadmap di attività per l'aumento della sicurezza di identità, dispositivi e dati adottando il modello Zero Trust

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.

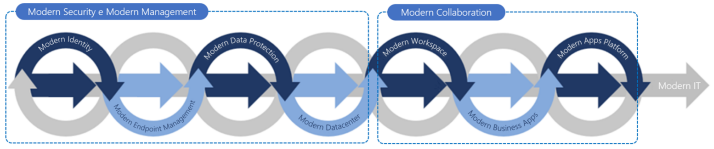
Generalmente le prime attività della roadmap agiscono sugli ambiti delle identità e degli accessi, della gestione dei dispositivi e della sicurezza informatica; ovvero nel loro insieme, **la base su cui costruire le fondamenta tecnologiche per lo sviluppo continuo dello scenario moderno.**

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 con la giusta gradualità e continuità (concetto di **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 benefici.

Nello scenario moderno gradualmente introdotto dal processo di continua modernizzazione, tutti i servizi tendono a essere fruibili via Public 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 (Public Internet)**, arrivando a poter considerare tutti gli utenti e tutti i dispositivi sempre come esterni, anche quando sono in ufficio.

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 IT, 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.



Approccio alla modernizzazione della sicurezza

La difesa perimetrale è da considerarsi obsoleta nell'era cloud e del **Modern Workspace**. 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 l'adozione del **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.
- La dismissione delle connessioni VPN
- La revisione delle modalità di esposizione dei servizi e risorse on-premise.
- L'associazione dei PC ad Azure AD.
- 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 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 dello Shadow IT.
- **Azure Defender:** protezione avanzata server e workload cloud.
- **Azure Sentinel:** un 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 alla sicurezza con il metodo definito "**Protect–Detect–Respond**".

Quindi gli strumenti introdotti non devono essere abbandonati dopo la loro adozione poiché producono informazioni che devono essere valutate da personale IT specializzato. Si suggerisce quindi l'implementazione di periodici processi di controllo svolti da personale interno o esterno (SOC).

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. Tramite l'adozione del **modello Secure Privileged Access (SPA)** di Microsys, ispirato al modello Microsoft Enanched Security Administration Environment (ESAE), è possibile aumentare la protezione delle credenziali privilegiate e diminuire le probabilità di successo di note tecniche di attacco (**Lateral Movement e Escalation of Privileges**).

Introduzione e descrizione della roadmap

È stata eseguita un'approfondita intervista di circa 50 domande divise in 4 ambiti (**identità e accessi, dispositivi, dati e infrastruttura**), con l'obiettivo di raccogliere le informazioni utili per definire le attività, le priorità del percorso di sicurezza per l'adozione del modello di sicurezza Zero Trust e per rilevare gli ambiti con maggiore criticità definendo così i primi rimedi. L'analisi ha prodotto un **piano di 10 attività** che aumenta la protezione e migliora la Security Posture. Nella roadmap sono state indicate le attività che non richiedono investimenti in licensing, sfruttando quindi servizi e funzionalità già a disposizione. La roadmap prevede le seguenti attività:

Cod.	Attività	Ambito
1-01	Aumento protezione credenziali privilegiate	Identità e accessi
1-02	Aumento protezione password	Identità e accessi
1-03	Aumento protezione minacce da posta elettronica	Identità e accessi
2-01	Aumento protezione dispositivi Windows	Dispositivi
2-02	Aumento protezione esecuzione applicazioni	Dispositivi
4-01	Aumento protezione VPN	Infrastruttura
3-01	Aumento protezione dati	Dati
2-03	Aumento protezione dispositivi mobili	Dispositivi
4-02	Igiene di Active Directory	Infrastruttura
4-03	Implementazione DR per AD e Azure AD	Infrastruttura

Valutazioni e ordine di esecuzione delle attività

Cod.	Attività	Ambito	Fase protezione	Licenze richieste	Effort	Impatto IT	Impatto utenza	Beneficio sicurezza	Scenario
4-01	Igiene di Active Directory	Infrastruttura	Protect	No	Basso	Basso	Basso	Medio	Minimo
1-01	Aumento protezione credenziali privilegiate	Identità e accessi	Protect	No	Alto	Alto	Basso	Alto	Minimo
1-02	Aumento protezione accessi	Identità e accessi	Protect	No	Medio	Medio	Basso	Alto	Base
1-03	Aumento protezione identità	Identità e accessi	Protect	No	Medio	Medio	Medio	Alto	Minimo
1-04	Aumento protezione password	Identità e accessi	Protect	No	Basso	Basso	Medio	Alto	Base
1-05	Aumento postura di sicurezza identità	Identità e accessi	Protect, Detect e Respond	No	Basso	Medio	Basso	Alto	Avanzato
2-01	Aumento protezione dispositivi Windows	Dispositivi	Protect	No	Basso	Medio	Basso	Alto	Base
2-02	Aumento protezione navigazione	Dispositivi	Protect	No	Basso	Basso	Basso	Alto	Base
2-03	Aumento posture di sicurezza dispositivi Windows	Dispositivi	Protect, Detect e Respond	No	Basso	Medio	Basso	Alto	Avanzato
2-04	Aumento protezione dispositivi iOS e Android	Dispositivi	Protect	No	Medio	Medio	Basso	Alto	Avanzato
1-06	Aumento protezione risorse	Identità e accessi	Protect	No	Basso	Medio	Medio	Alto	Completo
3-01	Aumento protezione dati	Dati	Protect	No	Basso	Medio	Basso	Alto	Base
3-02	Aumento postura di sicurezza dati	Dati	Protect, Detect e Respond	No	Basso	Medio	Basso	Medio	Avanzato
2-05	Aumento protezione esecuzione applicazioni	Dispositivi	Protect	No	Medio	Medio	Medio	Alto	Completo
4-02	Aumento protezione reti Wi-Fi	Infrastruttura	Protect	No	Alto	Medio	Basso	Alto	Completo
4-03	Implementazione DR per AD e Azure AD	Infrastruttura	Protect	Sì	Medio	Medio	Basso	Alto	Completo

**considerando i piani di licenze a disposizione di CONTOSO nel momento della redazione del documento*

Decisioni e motivazioni

Cod.	Attività	Decisioni	Motivazioni
4-01	Aumento protezione Active Directory		
1-01	Aumento protezione password Administrator		
1-02	Aumento protezione credenziali privilegiate		
1-03	Aumento protezione identità		
1-04	Aumento protezione posta elettronica		
1-05	Aumento protezione password		
2-01	Aumento protezione dispositivi		
1-06	Aumento protezione risorse		
1-07	Aumento protezione accessi VPN		
2-02	Aumento postura di sicurezza dispositivi		
2-03	Aumento protezione esecuzione applicazioni		
4-02	Aumento protezione Wi-Fi		
3-01	Aumento protezione dati		

1-01: Aumento protezione credenziali privilegiate

Il modello SPA è un insieme di impostazioni in Active Directory che permettono la gestione e utilizzo sicuro delle credenziali privilegiate. Tale attività si ritiene fondamentale per abbattere le probabilità di successo di attacchi che sfruttano le tecniche di Lateral Movement e Escalation of Privileges (tecniche che nella maggior parte dei casi si attacco provocano i danni maggiori). Gli elementi utili a realizzare il modello SPA sono:

- Revisione gruppi privilegiati, ovvero rivedere i membri dei Domain Admins, Administrators, Enterprise Admins, Schema Admins.
- Implementazione del Tier Model, ovvero un sistema per isolare in diversi livelli i vari amministratori (tra workstation, server e Domain Controller), senza possibilità di passare tra i livelli.
- Realizzare delle Privileged Access Workstation (PAW) per le attività amministrative con particolari e severe configurazioni di sicurezza.
- Introduzione e utilizzo del Local Administrator Password Solution (LAPS), ovvero una soluzione per gestire automaticamente la password dell'utente locale Administrator delle workstation e server in Active Directory.
- Opzionalmente, una dashboard basata su Log Analytics per il controllo degli eventi e monitoring relativo al modello SPA.

1-01: Aumento protezione credenziali privilegiate	
Requisiti	• Sistema operativo dei Domain Controller, FFL e DFL in supporto.
Attività Microsys	• Ridefinizione struttura OU. • Implementazione GPO e configurazioni per abilitare il Tier Model (workstation, server e Domain Controller). • Implementazione GPO e configurazioni per le PAW. • Abilitazione e configurazione del LAPS. • Migrazione pilota nelle nuove OU (10 utenti, 10 PC e 3 server)
Riferimenti	Securing privileged access

Nota: applicazione limitata a un solo dominio della foresta principale.

1-02: Aumento protezione password

Microsoft, grazie alla quantità di autenticazioni che esegue Azure AD, ha abilitato una verifica delle password più comuni e potenzialmente compromesse. Queste password vengono inserite automaticamente in una lista di password proibite o "banned" e quindi non più utilizzabili dagli utenti al reset della password.

Questa protezione è estendibile ad Active Directory in scenari ibridi, installando uno o più agenti on-premise, permettendo così a utenti o amministratori di rispettare la stessa password policy degli utenti cloud e impedire l'utilizzo di password troppo semplici o compromesse.

1-02: Aumento protezione password	
Requisiti	• Azure AD Premium P1
Attività Microsys	• Abilitazioni Banned Password in scenario ibrido e installazione Azure AD Password Protection DC Agent (su 2 server) • Definizione password policy in audit mode • Configurazione agenti sui Domain Controller • Verifica report compatibilità (dopo 30 giorni) • Abilitazione funzionalità
Riferimenti	• Eliminate bad passwords in your organization • Enforce Azure AD password protection for Active Directory

1-03: Aumento protezione minacce da posta elettronica

Defender for Office 365 è lo strumento che protegge da minacce ricevute tramite mail o link nei tool di collaborazione (SharePoint e Teams). Defender for Office 365 aumenta la capacità di protezione di Exchange Online Protection (EOP) includendo le seguenti funzionalità:

- Configurazioni di politiche "anti" (anti-malware, anti-phishing, anti-spam)
- Impostazioni di politiche "safe" (safe links, safe attachments)
- Impostazioni di politiche di "impersonation"
- Protezione estesa ad altri workload (SharePoint Online, OneDrive e Teams)
- Protezione con "Zero-Hour auto purge"

1-03 Aumento protezione minacce da posta elettronica	
Requisiti	• Defender for Office 365 P1
Attività Microsys	• Impostazione di due policy (Standard e Strict) • Applicazione policy Standard a tutti (gruppo dinamico) • Applicazione policy Strict a insieme di utenti pilota (fino a 10 utenti).
Riferimenti	• Microsoft Defender for Office 365

2-01: Aumento protezione dispositivi Windows

Per arrivare a gestire i dispositivi Windows ovunque siano, è necessario eseguire delle attività preparatorie. Tali attività estenderanno il confine amministrativo e gestionale, consentendo una gestione dei PC Windows "Internet-based". Una volta che i PC saranno "Hybrid-Join", avverrà automaticamente l'operazione di

Stato completamento roadmap

Cod.	Attività	Stato attività	Task	Stato task	Note e riferimenti
1-01	Aumento protezione credenziali privilegiate	Da fare	Ridefinizione struttura OU	Da fare	
			Implementazione GPO e configurazioni per abilitare il Tier Model (workstation, server e Domain Controller)	Da fare	
			Implementazione GPO e configurazioni per le PAW	Da fare	
			Abilitazione e configurazione del LAPS	Da fare	
1-02	Aumento protezione esecuzione applicazioni	Da fare	Configurazioni e abilitazione policy SRP e AppLocker	Da fare	
			Applicazione policy ad un gruppo di PC pilota (fino a 2)	Da fare	
1-03	Aumento protezione identità	Da fare	Verifica configurazione e definizione eventuale piano di attività	Da fare	
1-04	Aumento protezione accessi VPN	Da fare	Configurazione server NPS su Azure (o su infrastruttura del cliente)	Da fare	
			Applicazione Azure MFA a un gruppo di utenti pilota (fino a 2)	Da fare	
1-05	Aumento protezione reti Wi-Fi	Posticipato	Revisione o reinstallazione della PKI per predisporla all'erogazione degli opportuni template di certificati	Da fare	
			Installazione e configurazione server NDES	Da fare	
			Distribuzione dei certificati necessari all'avvio del servizio	Da fare	
			Configurazione delle opportune policy su Active Directory	Da fare	
			Supporto per la configurazione dell'autenticazione basata su certificato (CBA) per Wi-Fi	Da fare	
			Applicazione policy ad un insieme di PC pilota (fino a 10)	Da fare	
1-06	Aumento protezione dispositivi Windows	Posticipato	Installazione e configurazione SCCM (singolo server e singolo sito)	Da fare	
			Abilitazione e configurazione funzionalità di Software Updates	Da fare	
			Impostazione ciclo mensile di Patch Management basato su 3 ring	Da fare	
			Abilitazione e configurazione Cloud Management Gateway	Da fare	
			Applicazione a tutti i server e PC	Da fare	
1-07	Aumento protezione accessi	Da fare	Verifica configurazione e definizione eventuale piano di attività	Da fare	
1-08	Aumento protezione posta elettronica	Da fare	Verifica configurazione e definizione eventuale piano di attività	Da fare	

MICROSYS

Gli strumenti tecnici

Strumento, soluzione o servizio	Licensing
Tiering model o Modello SPA di Microsys: per la protezione delle credenziali privilegiate di AD	Potrebbe comportare costi Azure
Azure AD (Conditional Access, Azure MFA, Azure AD Application Proxy): gestione e protezione identità	Business Premium, EMS E3 o Microsoft 365 E3
Intune (MDM e MAM): gestione e protezione dei dispositivi	Business Premium, EMS E3 o Microsoft 365 E3
Information Protection: classificazione e protezione dei dati	Business Premium, EMS E3 o Microsoft 365 E3
Defender for Office 365: protezione avanzata delle minacce dalla posta elettronica	Microsoft 365 E5 Security
Defender for Endpoint: protezione avanzata dispositivi e Continuos Vulnerability Assessment	
Defender for Identity: controllo attività anomale sulle identità di Active Directory	
Identity Protection: rileva i rischi sulle identità e automatizza la risposta	
Defender for Cloud Apps: protezione dati e controllo del fenomeno Shadow IT	
Defender for Cloud: protezione avanzata server e workload cloud e on-premise	Azure
Microsoft 365 Defender: soluzione XDR per la gestione e controllo della sicurezza	Compreso nei piani Microsoft 365
Microsoft Sentinel: un moderno SIEM per correlare tutti gli eventi di sicurezza	Azure
Quest (vari tool per aggiungere capacità di rilevamento e risposta al modello SPA e protezione avanzate di AD)	Da definire in base al tool

*La unica piattaforma di strumenti Microsoft offre evidenti vantaggi di gestione completa della sicurezza. I vari servizi interagiscono realizzando un sistema **«Layered Security»** che aumenta la protezione a vari livelli, consentendo verifiche esplicite, automazioni e capacità di risposta nei vari stadi di un attacco introducendo il metodo **«Protect–Detect–Respond».***

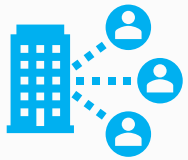
Gli ostacoli principali

- **File server «classici»:** conviene trasformarli in Office 365 e/o storage Azure; questo tipo di migrazioni potrebbero non essere veloci, semplici o a basso costo.
- **L'insieme delle applicazioni, servizi e risorse:** se si vuole perseguire il modello Zero Trust, tutte delle applicazioni, servizi e risorse dovrebbero adattarsi al SSO in Azure AD. In caso di applicazioni legacy non adattabili, queste si possono virtualizzare in modo da lasciarle operative in un ambiente più sicuro e controllato.

MICROSYS

Ma prima proteggere le credenziali privilegiate

Gli hacker riescono a monetizzare le loro azioni (rif. Human-operated ransomware)

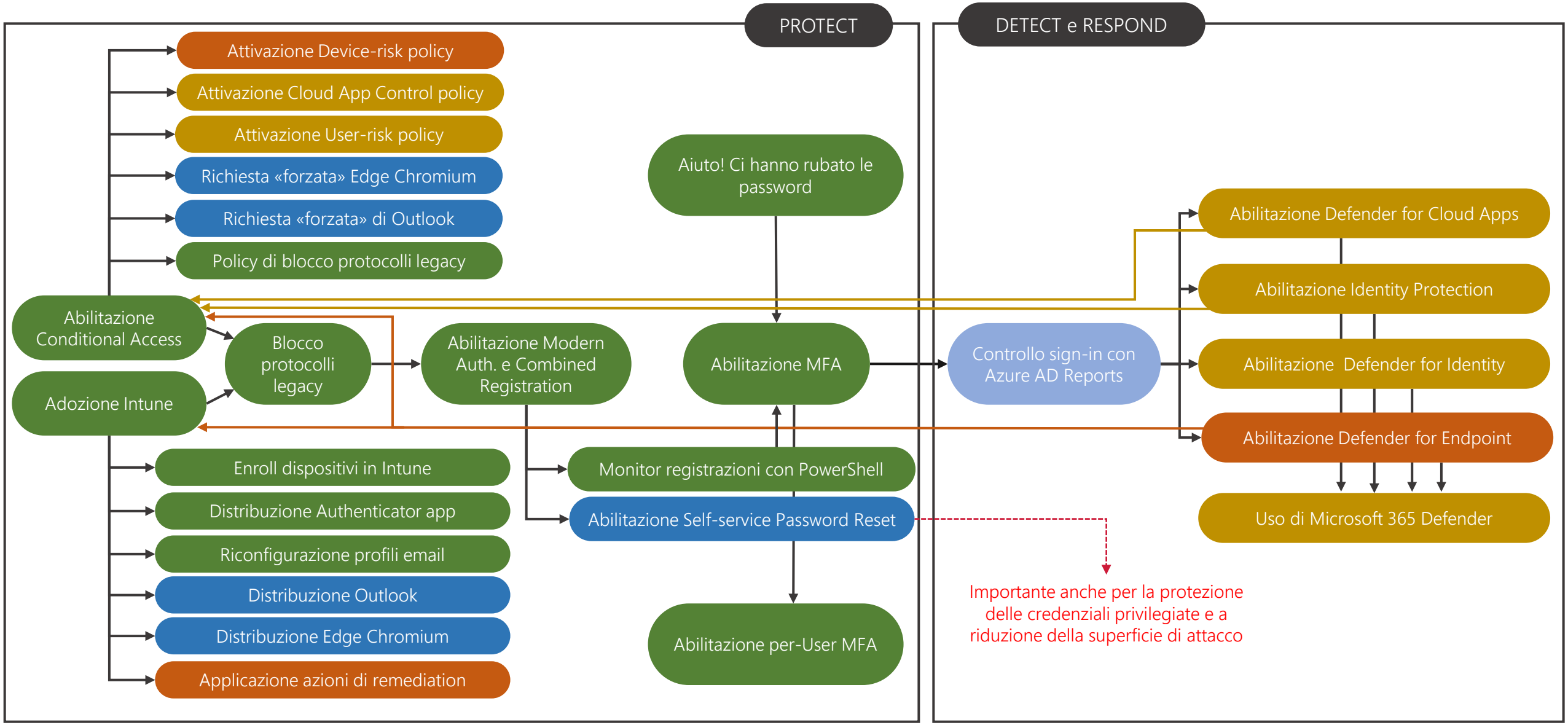


Gli operatori IT lavorano sempre di più da remoto

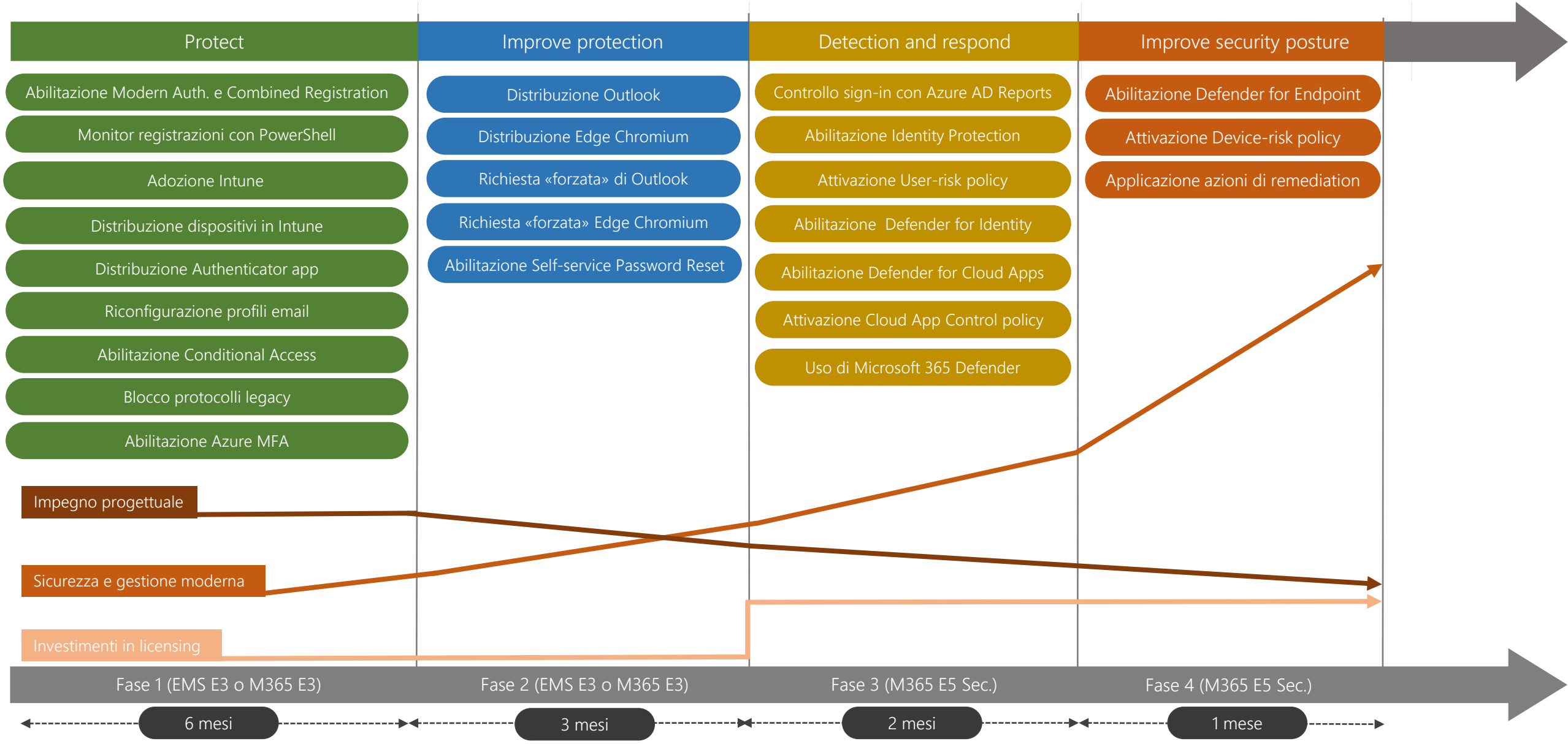
E' quesitone di **sicurezza sul lavoro**; oltre a proteggere identità, dispositivi, dati e infrastrutture bisogna proteggere anche il lavoro dei professionisti, operatori e consulenti IT. Questi usano le credenziali più critiche dell'organizzazione per cui lavorano, devo quindi lavorare in sicurezza.

MICROSYS

Esempio di roadmap e integrazione tra i vari strumenti



Esempio di roadmap e integrazione tra i vari strumenti



Gestione della sicurezza

- Nell'ambito della sicurezza, le strategie, il dato, la correlazione, gli strumenti, le procedure e la documentazione è importante che siano un **patrimonio del cliente.**
- Durante e dopo l'esecuzione della «Roadmap to Modern Security» è fondamentale avviare dei **servizi proattivi** di sicurezza e se necessario dei **servizi reattivi** di sicurezza (per esempio un SOC 24x7).
- Microsys ha sviluppato un **servizio proattivo di gestione della postura di sicurezza** che si prende in carico gli strumenti del cliente (progettati e abilitati durante la roadmap) e tramite questi continua a mantenere il livello della postura di sicurezza.
- In caso di necessità, tramite un nostro partner è possibile erogare un servizio SOC 24x7, allineato e in contatto con il team di sviluppo della roadmap e con il team di gestione proattiva della sicurezza.

MICROSYS