EOS SOLUTIONS
A KUMAVISION GROUP COMPANY

SICUREZZA IT:
NON PARLARE CON GLI ESTRANEI

CONDIVIDERE

webinar

Mercoledì
13.11.2019
Ore 11.00

Flora Gitti
flora.gitti@eos-solutions.it
Luca Borio
luca.borio@eos-solutions.it

Flora Gitti

Sales Manager Customer Base
EOS Solutions

Luca Borio

Team Leader Cloud Services
EOS Solutions

Agenda

01 2020, anno di addii. I prodotti che terminano il supporto

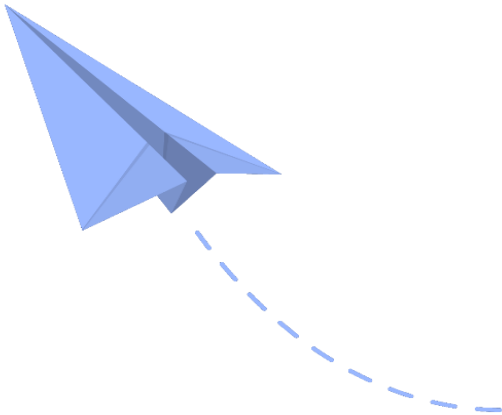
02 Laboratorio: simuliamo un attacco

03 DLP Data Lost Prevention: come proteggere la proprietà intellettuale

04 Password, siamo sicuri che sia uno strumento sicuro?

05 Lavoriamo con DLP e con le soluzioni MFA Multi - Factor Authentication

06 Microsoft 365 & Dynamics 365 Business Central: sicurezza dati al 100%



END OF SUPPORT

Windows Server 2008
Windows Server 2008 R2
SQL Server 2008
SQL Server 2008 R2
Exchange Server 2010
SharePoint Server 2010
Office 2010

GENNAIO
14

www.eos-solutions.it

https://support.microsoft.com/en-us/help/4470235/products-reaching-end-of-support-for-2020

Migrazione da WS2008

Windows Server 2019

Sicurezza

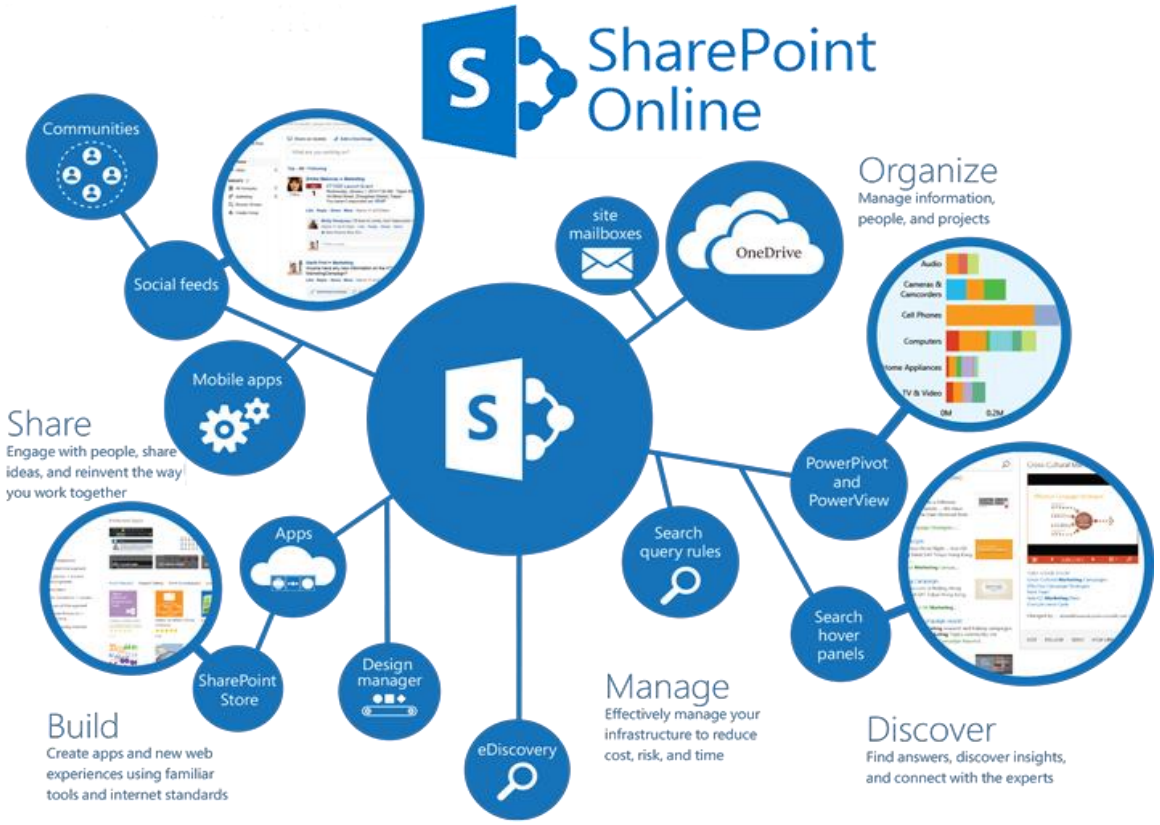
Windows Defender Advanced Threat Protection (ATP)
Windows Defender ATP Exploit Guard

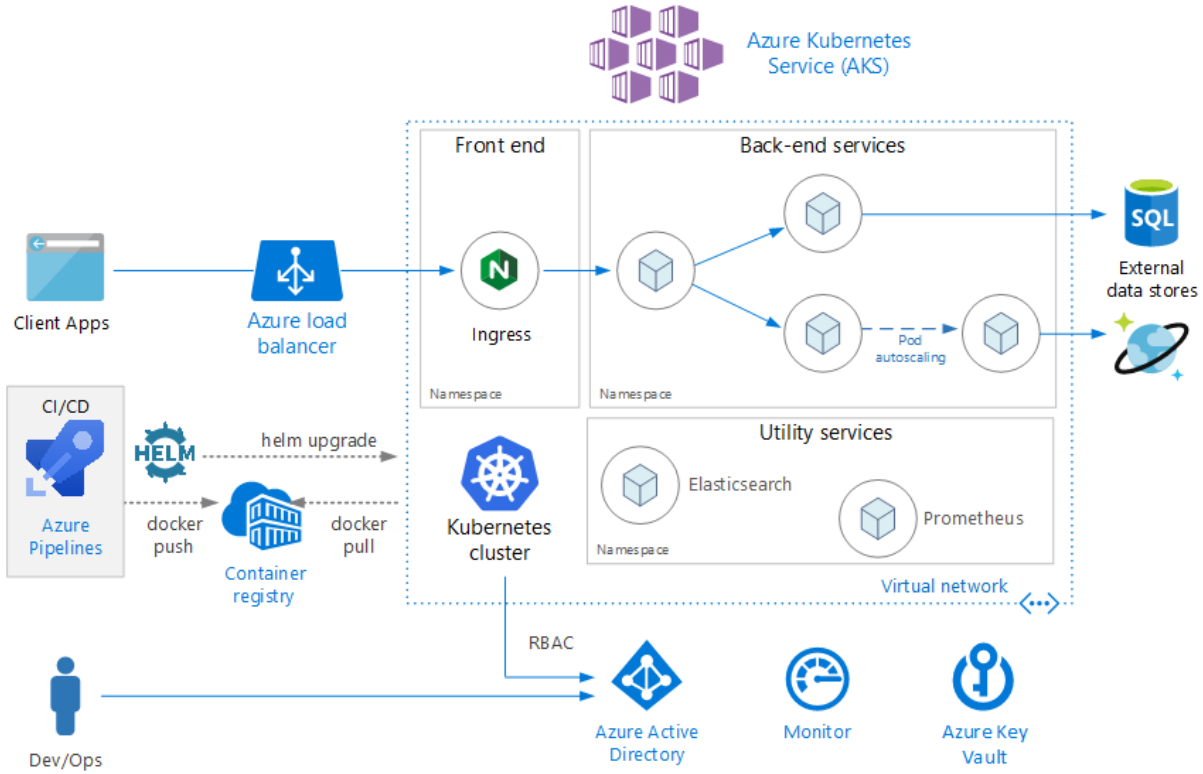
Reti crittografate
Reti codificate: la codifica di rete virtuale consente la codifica del traffico di rete virtuale tra le macchine virtuali che comunicano tra loro all'interno di subnet contrassegnate come **Codifica abilitata**.

Piattaforma per applicazioni
Contenitori di Linux in Windows
È ora possibile eseguire contenitori basati su Linux e Windows nello stesso host contenitore usando lo stesso daemon docker. Ciò consente di disporre di un ambiente costituito da host contenitori eterogenei e offre al tempo stesso flessibilità agli sviluppatori di applicazioni.

Supporto incorporato per Kubernetes
Windows Server 2019 prosegue i miglioramenti in fatto di elaborazione, rete e archiviazione introdotti dai rilasci di Canale semestrale, necessari per supportare Kubernetes su Windows. Altri dettagli sono disponibili nelle versioni future di Kubernetes.

Migrazione da WS2008 e SERVIZI ONLINE





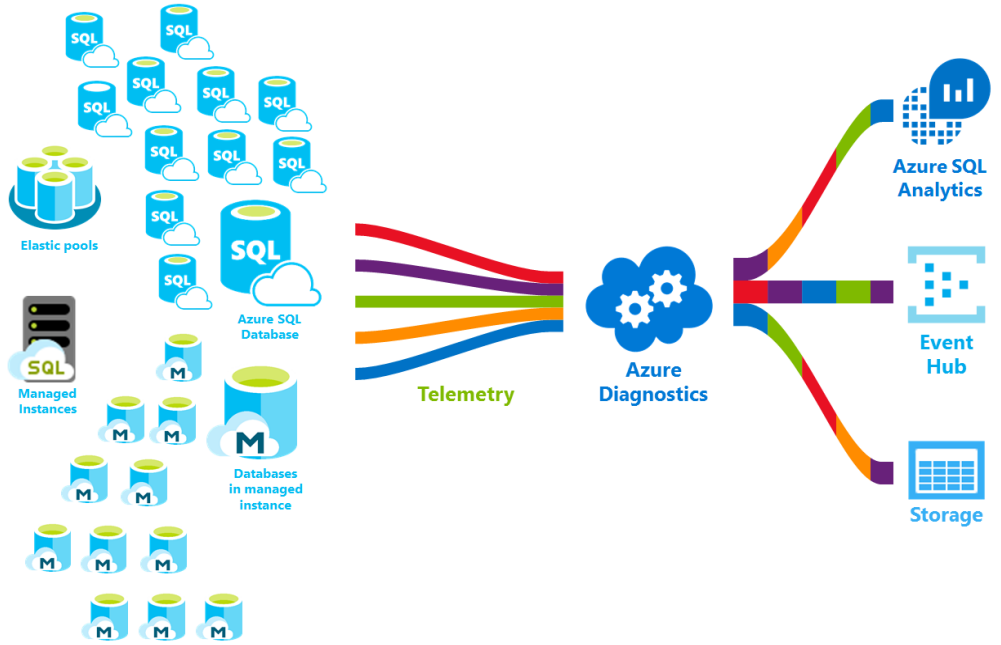
Da SQL SERVER 2008 a SQL Server 2019

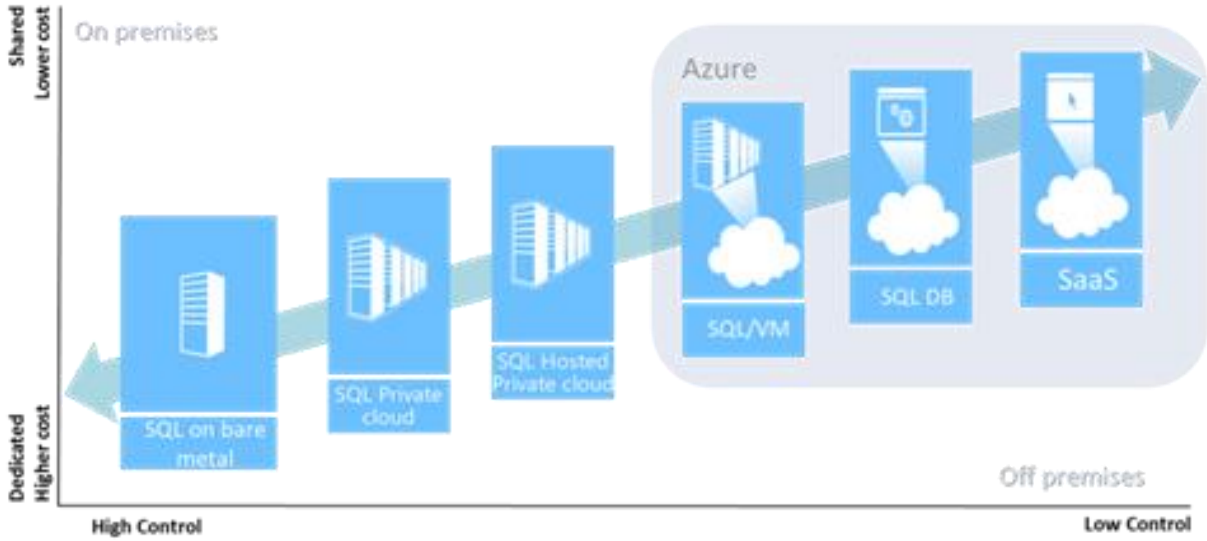
Sicurezza cruciale
SQL Server fornisce un'architettura di sicurezza progettata per consentire agli amministratori di database e agli sviluppatori di creare applicazioni di database sicure e contrastare le minacce. Ogni versione di SQL Server è stata migliorata rispetto alle versioni precedenti con l'introduzione di nuove caratteristiche e funzionalità e anche SQL Server 2019 (15.x) prosegue in questa tradizione.

Database in memoria
Le tecnologie di database in memoria di SQL Server sfruttano le ultime innovazioni in campo hardware per offrire prestazioni e scalabilità senza precedenti. SQL Server 2019 (15.x) si basa su innovazioni precedenti in quest'area, ad esempio l'elaborazione delle transazioni online (OLTP) in memoria, per rendere possibile un nuovo livello di scalabilità in tutti i carichi di lavoro del database.

Database intelligente
SQL Server 2019 (15.x) si basa sulle innovazioni delle versioni precedenti per offrire prestazioni leader nel settore già in configurazione di base. Dall'elaborazione intelligente delle query al supporto di dispositivi con memoria persistente, le funzionalità del database intelligente di SQL Server migliorano le prestazioni e la scalabilità di tutti i carichi di lavoro di database senza apportare modifiche alla progettazione di applicazioni o database.

SQL Server 2019: scalabilità, sicurezza e performance





Da EXCH 2010 verso EXCH 2019

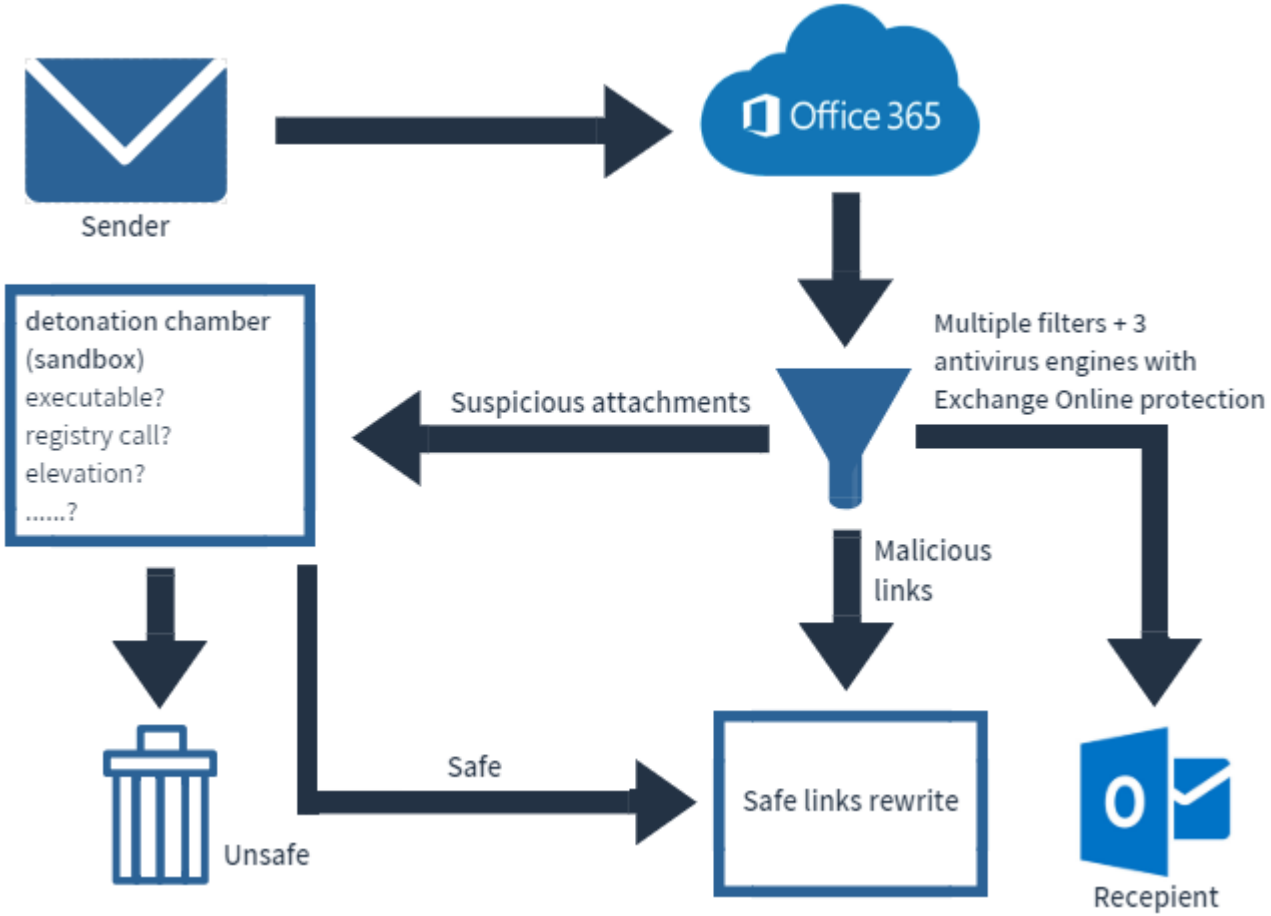
Sicurezza

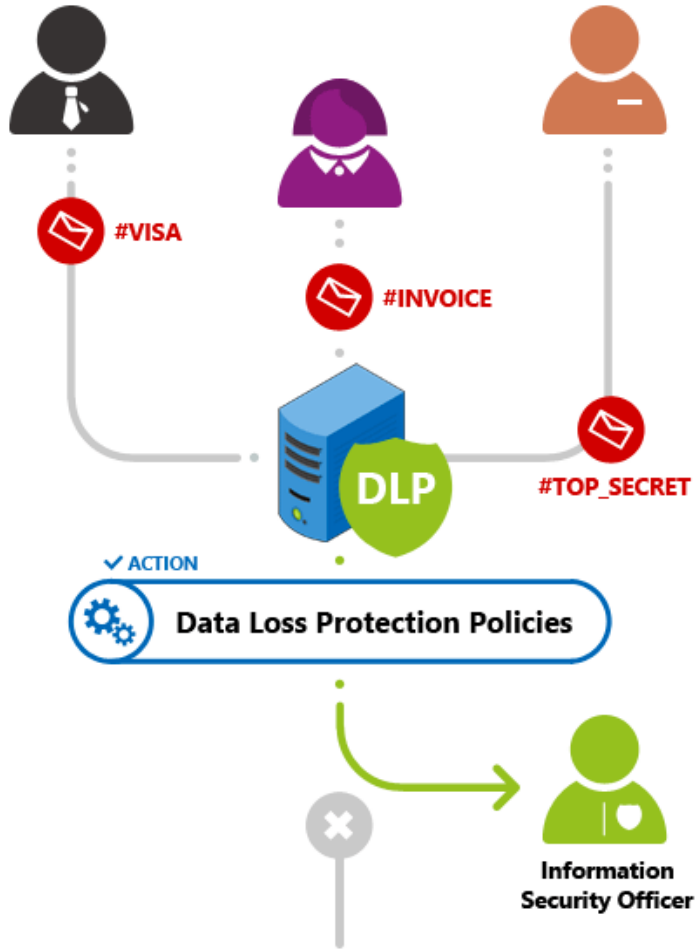
Supporto di Windows Server Core: l'esecuzione di Exchange in una distribuzione di Windows con una superficie di attacco ridotta indica una riduzione della superficie di attacco e della quantità di componenti da gestire.
Blocco dell'accesso esterno all'interfaccia di amministrazione di Exchange (EAC) e a Exchange Management Shell: è possibile utilizzare le regole di Accesso client per consentire l'amministrazione di Exchange solo dalla rete interna, anziché utilizzare regole di firewall e di rete complesse.

Collaborazione su documenti

Exchange 2019, con SharePoint Server 2019, consente agli utenti di Outlook sul web di collegarsi e condividere i documenti archiviati in OneDrive for Business in un server SharePoint locale, anziché allegare file ai messaggi. Gli utenti in un ambiente locale possono collaborare sui file nello stesso modo utilizzato in Office 365.

SERVIZI ONLINE e PROTEZIONE inclusa





Data Loss Prevention

Helps to
identify
monitor
protect
sensitive data through deep content analysis

DLP (Data Loss Prevention)
Ovvero Prevenzione della Perdita di Dati

With a DLP policy, you can:

- Identify sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.
- Prevent the accidental sharing of sensitive information.
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word.
- Help users learn how to stay compliant without interrupting their workflow.
- View DLP reports showing content that matches your organization's DLP policies.

MFA Multi-Factor Authentication

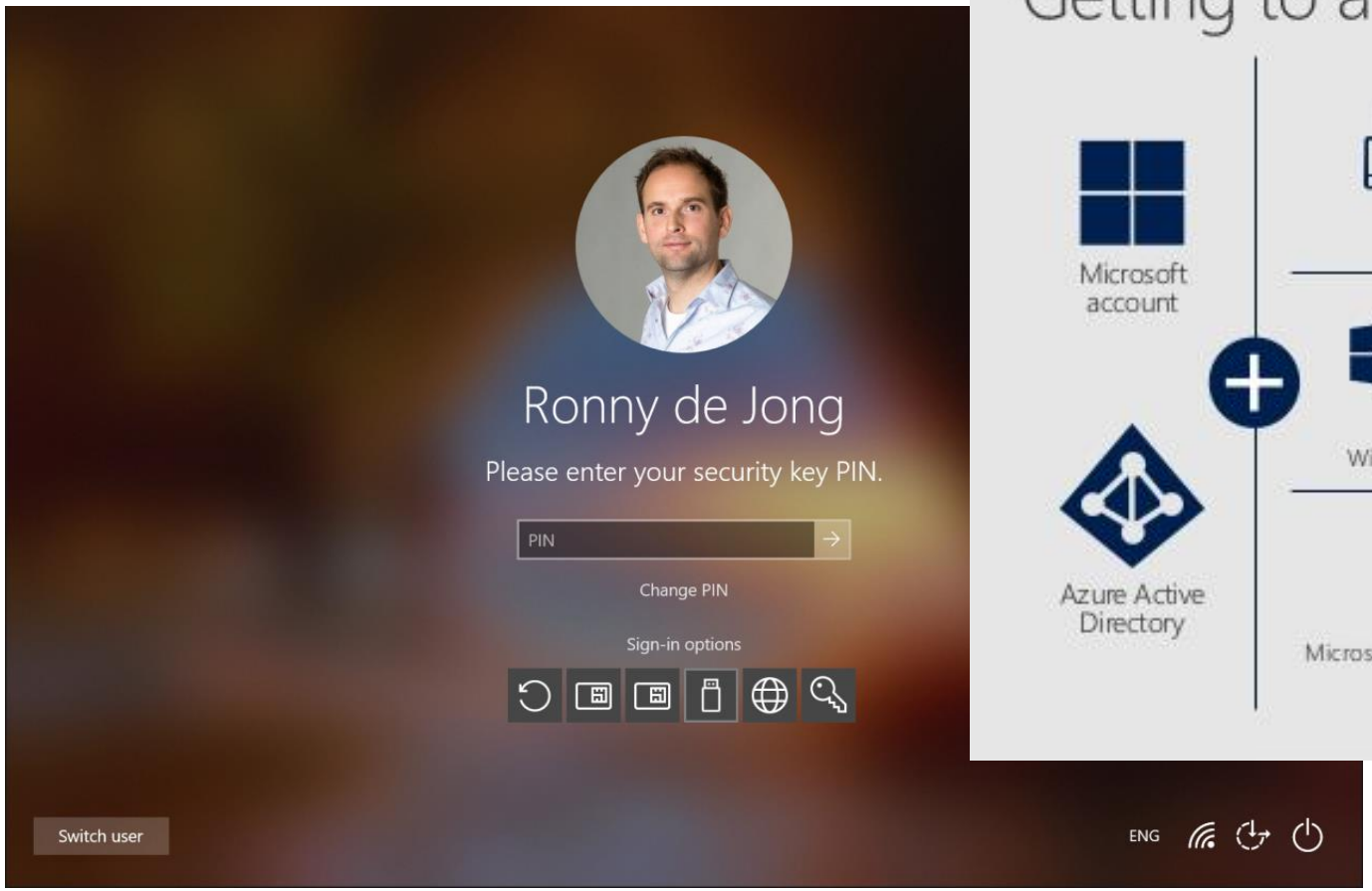
La sicurezza della verifica in due passaggi sta nel suo approccio a livelli. La manomissione di più fattori rappresenta una sfida significativa per gli autori di attacchi.

Tuttavia, anche se un autore di un attacco riesce a ottenere la password dell'utente, questa risulta inutile se non è in possesso del metodo di autenticazione aggiuntivo.

In genere richiede due o più dei metodi di autenticazione seguenti:

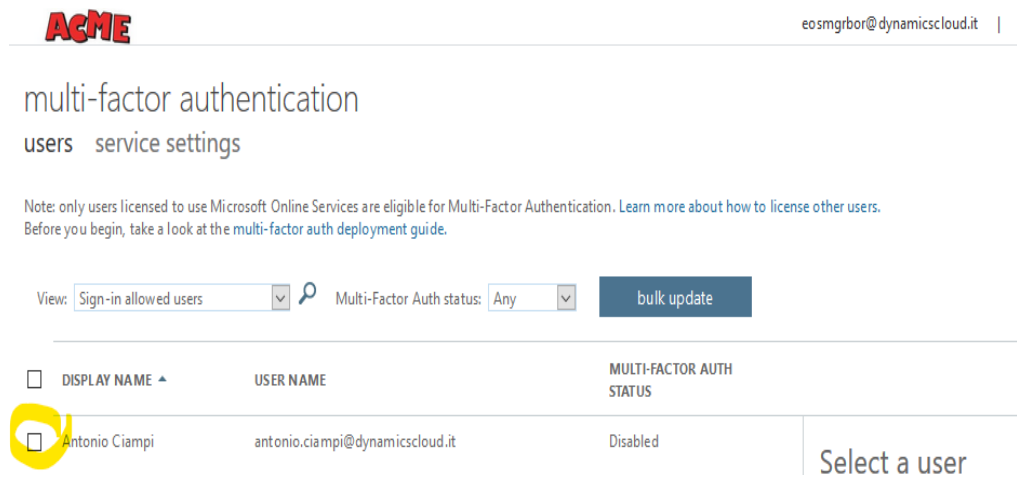
- Un elemento noto, in genere una password
- Un oggetto fisico (un dispositivo attendibile non facilmente duplicabile, come un telefono)
- Una caratteristica personale (biometria)

SECURITY NON SOLO PASSWORD



Multi-Factor Authentication for Dynamics 365 Business Central

- Anche Dynamics 365 Business Central può utilizzare la MFA per proteggere l'accesso ai dati aziendali.
- L'accesso a soluzioni ERP avanzate quali **Dynamics 365 Business Central** deve essere protetto, quale miglior modo se non attivare una soluzione MFA.
- Microsoft 365 consente a tutti gli utenti **Dynamics 365 Business Central** di godere dei massimi livelli di sicurezza con un click



Microsoft 365 – One subscription for Productivity + Security + Device Management

- Device Management
- Archiving
- Data Loss Prevention
- Email Threat Protection
- Email Filtering
- Device Anti Virus
- Online Chat & Meetings
- Storage
- Email
- Productivity Software

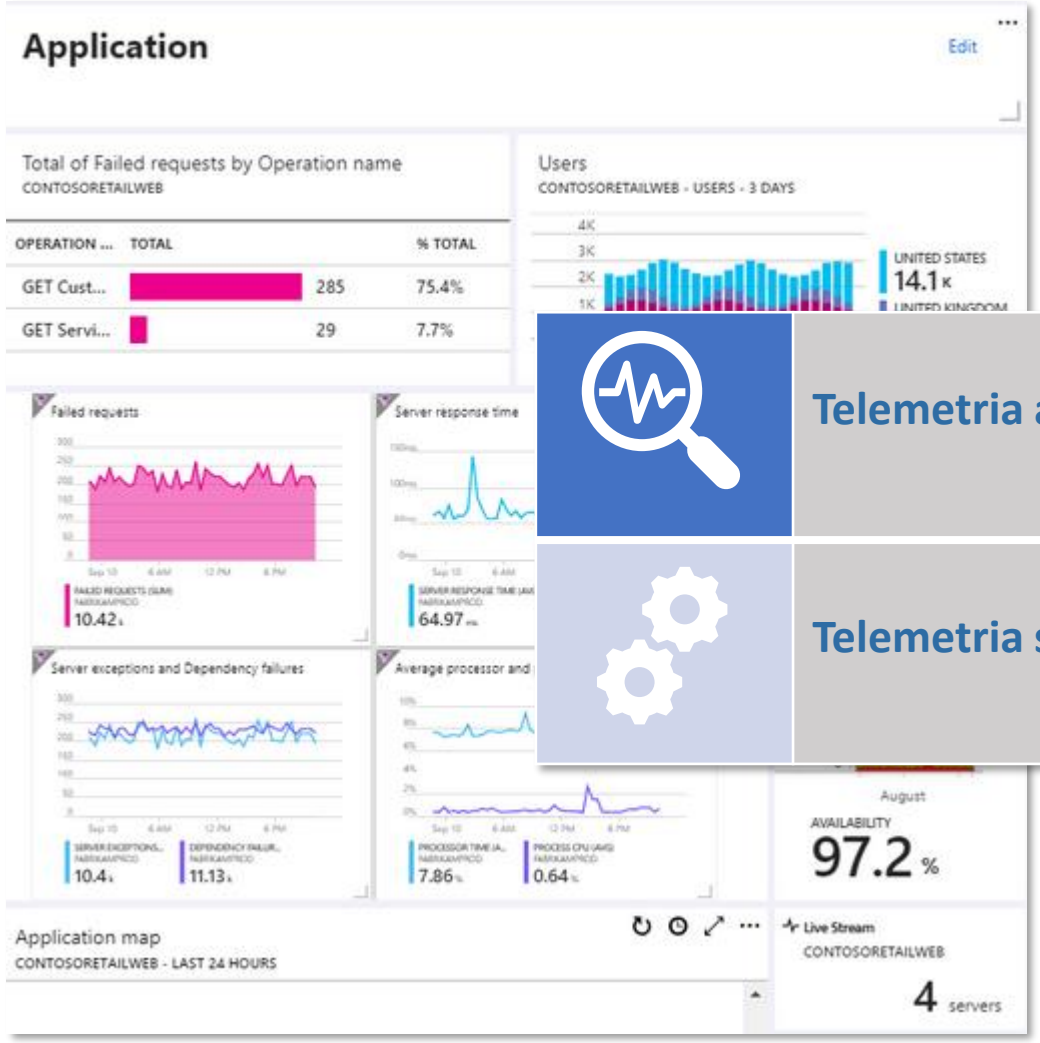
3rd party solutions
(bought separately, expensive & hard to integrate)

$20 **PER USER STANDALONE**

- Device & App Management across PCs, Macs, iOS & Android
- Information Protection
- Archiving + Litigation Hold
- Data Loss Prevention
- Email + Device Threat Protection
- Email Filtering
- Windows Defender AV
- Teams & Skype for Business
- 1 TB File Storage
- 50 GB Cloud Email
- Office (Word, PowerPoint, Excel, Outlook, Onenote, Access)

Microsoft 365
(all included, seamlessly integrated)

Telemetria EOS - Servizi inclusi

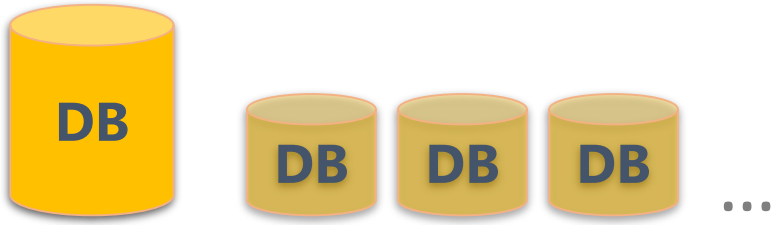


Telemetria aggiornamento sistemi (Fix di sicurezza)

Telemetria sul Db e verifica backup

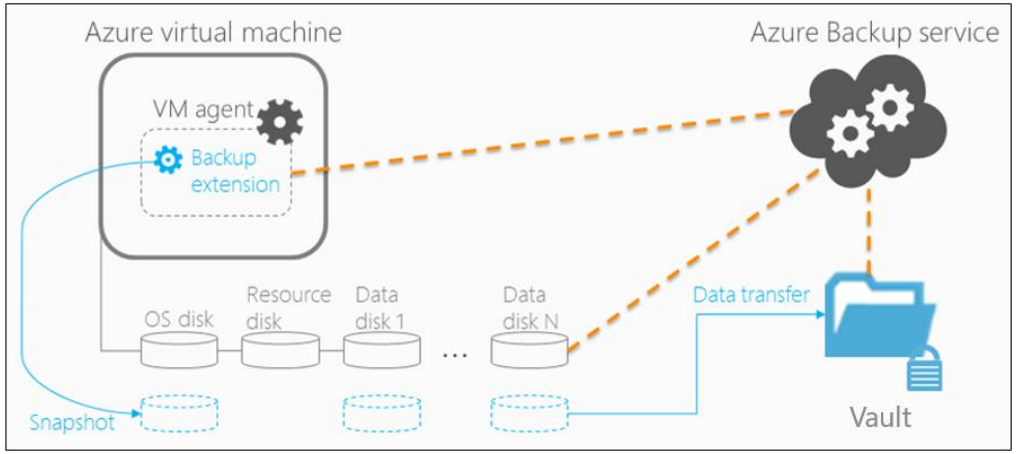
Politiche di Backup e manutenzione sistemi

Database backup



- Manutenzione DB
  - Check DB
  - Rebuild Index full
  - Rebuild Statistics
- Backup SQL
  - Transation log ogni ora
  - Backup Full giornaliero alle ore 23.00
- Eliminazione dei backup del transation log
- Eliminare i backup full più vecchi di 7 giorni

Virtual machine



- Backup Giornaliero VM alle ore 21.00
  Retention policy :
  - 14 giorni
  - 4 settimane (backup della domenica)
  - 4 mensili (backup prima domenica del mese)
- Sistema Operativo
  - Aggiornamenti di sicurezza installati settimanalmente.

Grazie!

EOS SOLUTIONS
A KUMAVISION GROUP COMPANY

www.eos-solutions.it