customer academy
FOR EVEN SMARTER COMPANIES

EOS WEBINARS

- Luca Borio
  luca.borio@eos-solutions.it
- Alvise Giacomin
  alvise.giacomin@eos-solutions.it
- Bastiano Di Gioia
  bastiano.digioia@eos-solutions.it

Cybersecurity & Cloud: le soluzioni che proteggono davvero la tua azienda

EOS Customer Academy

eos solutions
A KUMAVISION GROUP COMPANY

Speaker

Luca Borio
Azure & AI Presales Specialist

Alvise Giacomin
Azure & Infrastructure BL Manager

Bastiano Di Gioia
Business Developer & Sales Specialist

customer academy
FOR EVEN SMARTER COMPANIES

EOS CUSTOMER ACADEMY

Overview

Progettazione del brand EOS Customer Academy

Creazione di percorsi formativi che prevedano webinar, video on-demand, sessioni in aula e demo

Percorsi rivolti a figure professionali: CFO (CdG), CIO, COO (supply chain), Vendite/Marketing

CFO

Controllo di Gestione

BC, Power BI, EOS Apps

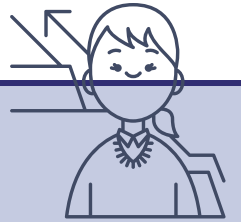
COO

Supply Chain management, digital factory, sicurezza in fabbrica

FreeHands, Demand Forecasting

CIO

Digitalizzazione



Sales/Mktg

CRM

customer academy

FOR EVEN SMARTER COMPANIES

Agenda

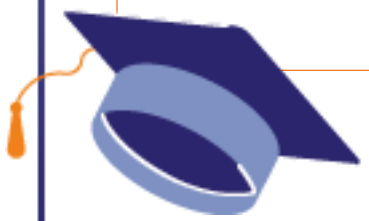
- Scenario attuale della sicurezza IT
- Infrastrutture ibride e cloud
- Demo e casi reali durante il webinar
- Servizi EOS
- Q&A interattivo durante il webinar e finale

customer academy
FOR EVEN SMARTER COMPANIES

SCENARIO ATTUALE DELLA SICUREZZA IT

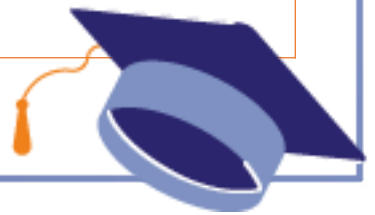
Motivazioni dell'urgenza: dati sugli attacchi e necessità di preparazione

Fonte	Dato / Trend Principale	Implicazioni per la Sicurezza / Perché è Urgente Prepararsi
Rapporto Germania (Bitkom)	Cyber attacchi sono costati all'economia tedesca quasi **300 miliardi di euro** nell'ultimo anno.	Indica che perdite finanziarie non sono teoriche ma sostanziali; anche aziende medio-piccole possono subire danni irreversibili.
Aumento globale attacchi (Q2 2025, Check Point)	+21% attacchi cyber globali anno su anno; Europa con la crescita maggiore di tutte le regioni. Numerosi settori colpiti (educazione, governo, telecomunicazioni).	Anche settori che storicamente erano meno targhettizzati sono ora nel mirino; difese spesso sotto il livello richiesto.
Furto credenziali / esfiltrazione dati	+42% anno su anno di credenziali rubate.	Le credenziali sono la chiave d'accesso: bastano per scalare privilegi, effettuare movimenti laterali, ecc. Serve protezione forte (MFA, gestione delle identità, monitoraggio).



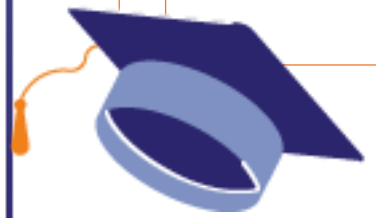
Chi vuoi che si prenda la briga di attaccare proprio noi?

Percezione Comune	La Realtà Oggi	Perché Dovresti Preoccuparti
"Non siamo famosi, quindi siamo invisibili."	Oggi il 60-70% degli attacchi è **automatizzato**: bot che scandagliano Internet alla ricerca di vulnerabilità, senza sapere chi sei.	Se hai un server esposto con una porta aperta, un account con password debole o un firewall non aggiornato, **verrai trovato e provato** nel giro di ore.
"Non abbiamo dati interessanti per i criminali."	Il dato più prezioso per un attaccante è **il tuo accesso al denaro o ai sistemi**: PC, email, IBAN, PEC, carte, contabilità, credenziali fornitori.	Anche cifrare i tuoi file e chiederti un riscatto (ransomware) è un modello di business. Paghi, o resti fermo.
"I nostri sistemi sono piccoli, non c'è nulla da rubare."	Le PMI rappresentano il **target più colpito**: circa il 43% degli attacchi globali mira a loro (dati Verizon DBIR 2025).	Proprio perché molte PMI non investono in sicurezza, sono viste come **facili prede** e porte d'ingresso verso clienti più grandi (supply chain attacks).
"Abbiamo antivirus, siamo coperti."	Gli attacchi di oggi sono spesso **malware-free** (phishing, sfruttamento credenziali, fileless attack).	Serve protezione identità (MFA), backup isolati, piani di risposta agli incidenti.
"Non abbiamo mai avuto problemi."	Nel 2025 il tempo medio prima che un'azienda scopra una violazione è di **204 giorni** (IBM Cost of a Data Breach Report).	Potresti essere già compromesso e non saperlo. Più tempo passa, più aumenta il danno potenziale.



5 punti magici della sicurezza

#	Controllo	Perché è Importante	Come Verificarlo/Subito
1	Backup affidabili e testati	Ransomware o guasti possono fermarti: il backup è l'unica rete di sicurezza.	Assicurati di avere backup giornalieri, offline o in cloud, e prova un ripristino almeno 1 volta/anno.
2	Autenticazione a più fattori (MFA)	Blocca la maggior parte dei furti di credenziali e accessi non autorizzati.	Abilita MFA su email, gestionali e VPN per tutti gli utenti.
3	Protezione email anti-phishing	Il 91% degli attacchi parte da email malevole.	Implementa protezioni avanzate (Defender for Business, Google Workspace Security) e forma i dipendenti.
4	Aggiornamenti automatici e patch	Chiude falle note che gli attaccanti sfruttano entro ore dalla scoperta.	Attiva update automatici su sistemi e software, e verifica che non ci siano versioni fuori supporto.
5	Piano di risposta agli incidenti	Sapere cosa fare riduce tempi di fermo e costi in caso di attacco.	Scrivi un protocollo base: chi chiamare, come isolare i sistemi, chi decide il ripristino.



Sicurezza = Base per l'AI Generativa

Prima di sfruttare il potere dell'AI, proteggi i tuoi dati e i tuoi accessi.

Una AI senza sicurezza è un rischio, non un vantaggio.

Metti in sicurezza la casa, poi invita l'AI a lavorare per te.

customer academy
FOR EVEN SMARTER COMPANIES

5 Punti Magici di Sicurezza per l'AI in Azienda

🔒 **Proteggi i dati sensibili**
Decidi quali documenti l'AI può usare ed evita fughe di dati.

🆔 **Identità e accessi blindati (MFA)**
Solo chi è autorizzato può interrogare l'AI o vedere i risultati.

📊 **Governance e log**
Monitora chi chiede cosa all'AI e conserva traccia delle interazioni.

🛠️ **Aggiornamenti e patch**
Mantieni piattaforme e connettori AI sempre sicuri e aggiornati.

🎓 **Formazione continua**
Insegna al team a usare l'AI in modo sicuro e responsabile.

customer academy
FOR EVEN SMARTER COMPANIES

Strumenti nativi per tracciare l’uso di Copilot e AI

- **Microsoft 365 Usage Reports**:
mostra quante query Copilot vengono fatte, da chi e in quali app (Word, Outlook, Teams).

- **Audit Log (Purview):**
registra le interazioni con Copilot, utile per investigazioni.

- **Microsoft 365 Secure Score**:
indica se l’ambiente è configurato in modo sicuro per usare AI (MFA, protezione dati).

- **Message Center + Admin Alerts**:
notifiche su nuove funzionalità AI e cambiamenti di policy.

customer academy
FOR EVEN SMARTER COMPANIES

Governance e tracciamento AI in Azure

- **Azure Monitor:**

raccoglie metriche e log delle chiamate agli endpoint OpenAI e Cognitive Services.

- **Azure Policy:**

controlla se i modelli AI vengono usati nel rispetto delle regole aziendali (es. regioni di deployment).

- **Cost Management + Budgets:**

monitora il consumo economico di servizi AI per evitare sforamenti.

- **Defender for Cloud:**

segnala configurazioni non sicure e anomalie sugli account che accedono ai modelli.

Monitoraggio proattivo & auditing continuo

- **Microsoft Sentinel:**

SIEM per correlare log AI con altri eventi di sicurezza (accessi sospetti, exfiltrazione dati).

- **Copilot Admin Center** (novità 2025):

dashboard dedicata per analisi di utilizzo e policy di sicurezza AI.

- **Data Loss Prevention (DLP):**

regole per impedire che dati sensibili vengano inviati a modelli AI.

- **Training & Awareness:**

report mensili per i manager + campagne di sensibilizzazione per i dipendenti.

customer academy
FOR EVEN SMARTER COMPANIES

Zero Trust perché è un buon approccio

5 Benefici dello Zero Trust per le PMI

01

Riduzione drastica del rischio di attacco
Ogni accesso viene verificato (utente, dispositivo, posizione): meno possibilità che un hacker entri indisturbato.

02

Protezione dei dati ovunque
I dati restano sicuri anche se utenti lavorano in remoto o da dispositivi personali.

03

Minore impatto di una violazione
Anche se un account viene compromesso, l'attacco resta confinato grazie al principio del "least privilege".

04

Conformità più semplice a GDPR e normative
Controlli granulari e tracciabilità degli accessi facilitano audit e report normativi.

05

Maggiore fiducia in AI e Cloud
Con Zero Trust puoi adottare AI generativa e servizi cloud sapendo che i dati e le identità sono protetti.

La sicurezza come investimento, non costo

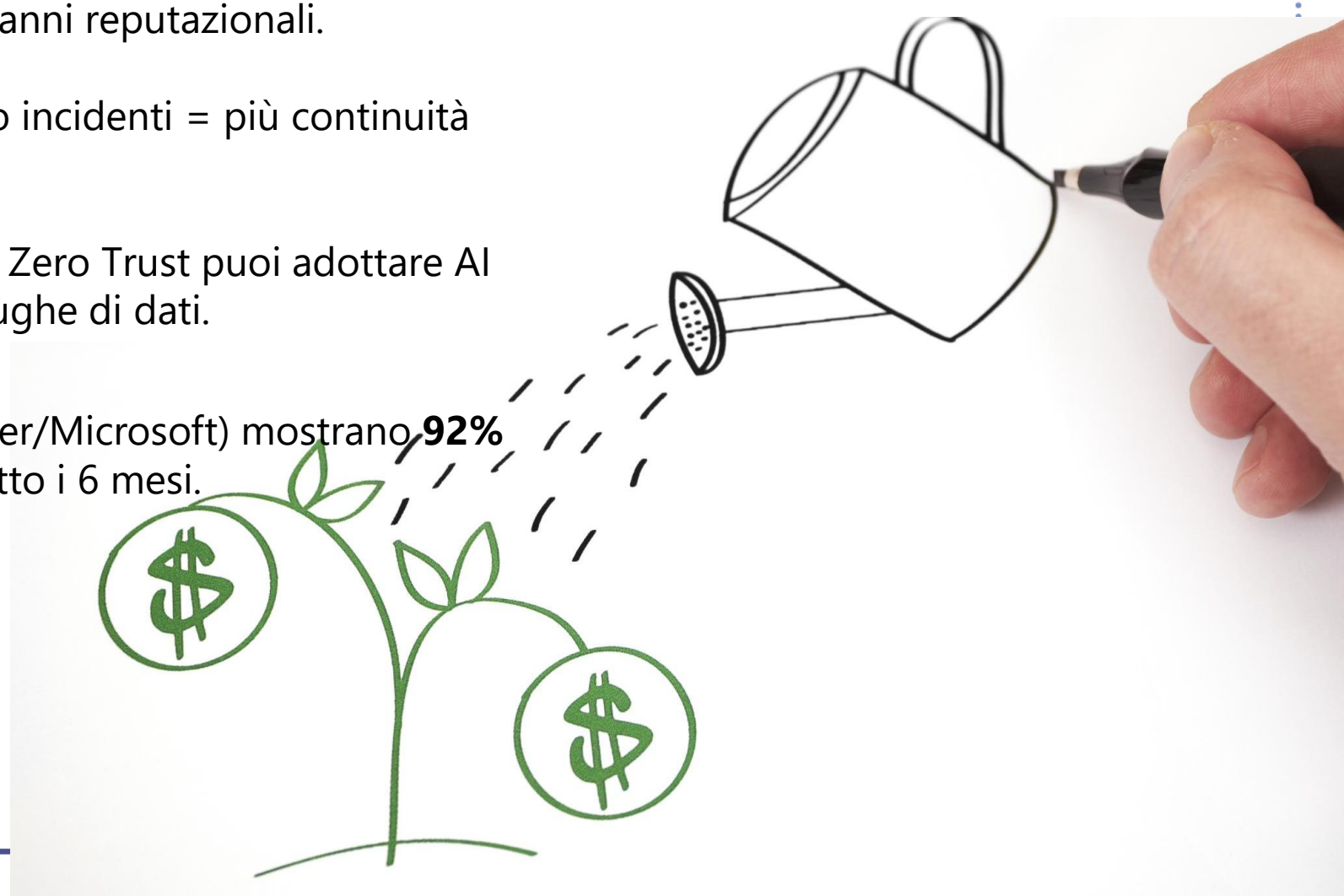
💎 **Proteggi il valore aziendale:** ogni euro speso in prevenzione può risparmiarne decine in ripristino e danni reputazionali.

⚙️ **Riduci il rischio di fermo:** meno incidenti = più continuità operativa, più fatturato.

🚀 **Accelera innovazione e AI:** con Zero Trust puoi adottare AI generativa e cloud senza paura di fughe di dati.

📈 **ROI dimostrabile:** studi (Forrester/Microsoft) mostrano **92% di ritorno in 3 anni** e “payback” sotto i 6 mesi.

🏆 **Vantaggio competitivo:** clienti e partner si fidano di più di chi dimostra di proteggere i dati.



Calcola il ROI

$$\text{ROI} = \frac{\text{Perdite Evitate} + \text{Risparmi Operativi} - \text{Costo della Soluzione}}{\text{Costo della Soluzione}} \times 100$$

📊 Esempio rapido (PMI 50 utenti)

Voce	Valore
Probabilità attacco ransomware/anno	20%
Costo medio fermo produzione (5gg)	€50.000
Rischio annuale stimato	€10.000
Investimento sicurezza (MFA + backup)	€4.000/anno
Riduzione rischio	80% → €8.000 evitati
ROI annuo	((8.000 - 4.000) ÷ 4.000) × 100 = **+100**

customer academy
FOR EVEN SMARTER COMPANIES

INFRASTRUTTURE IBRIDE E CLOUD

Sfide delle infrastrutture ibride e domande frequenti dei clienti

- **Infrastrutture ibride comuni**

  Molti clienti gestiscono server locali insieme a servizi cloud per flessibilità e continuità operativa.

- **Semplificazione senza stravolgere**

  È possibile ottimizzare l'uso delle infrastrutture esistenti semplificando processi senza cambi radicali.

Azure Arc è la tecnologia Microsoft che permette di **estendere i servizi e la gestione di Azure** a infrastrutture che non sono fisicamente in Azure.

In pratica, porta il modello di gestione cloud (policy, sicurezza, automazione) anche su:

- **Server on-premises** (Windows e Linux)
- **Macchine virtuali in altri cloud** (AWS, GCP, ecc.)
- **Cluster Kubernetes** ovunque si trovino
- **Database SQL** in locale o multi-cloud

Azure Arc: perché è utile alle PMI

🎛️ **Gestione centralizzata:**
un'unica "control plane" per tutto, cloud e on-prem.
📜 **Policy e compliance unificate:**
applichi le stesse regole di sicurezza dappertutto.
📊 **Scalabilità semplificata:**
puoi usare servizi Azure come Defender, Monitor o Update Management anche su macchine locali.
🌐 **Abilitazione Hybrid Cloud:**
prepari il terreno a una migrazione graduale al cloud.

Microsoft Defender for Cloud è la piattaforma unificata di **Cloud Security Posture Management (CSPM)** e **Cloud Workload Protection (CWPP)** di Microsoft.
In parole semplici: è il “radar” e lo “scudo” che protegge tutte le risorse nel cloud e on-prem, in un’unica console.

customer academy
FOR EVEN SMARTER COMPANIES

Defender for Cloud 🔑 Funzioni principali

- **Visibilità e posture management**

Analizza le tue risorse in Azure, altri cloud (AWS, GCP) e on-prem per segnalare configurazioni errate, vulnerabilità e priorità di remediation.

- **Protezione dei workload**

Fornisce difesa avanzata per VM, container, database, storage e servizi PaaS, con avvisi in tempo reale.

- **Defender Plans**

Moduli specifici per server, Kubernetes, SQL, Storage, App Service, Key Vault, ecc.

- **Integrazione con SIEM/SOAR**

Puoi inviare alert a **Microsoft Sentinel** o altri sistemi per orchestrare risposta automatica.

Defender for Cloud – I benefici per le PMI

🔍 Una **vista unica** della sicurezza: niente più strumenti sparsi.

✅ Migliora la compliance (ISO, NIS2, GDPR) con punteggio Secure Score e raccomandazioni.

⚡ Riduce tempi di risposta: avvisi prioritizzati e integrazione con playbook automatici.

Azure Local **è un servizio di Azure gestito da Microsoft**, ma installato fisicamente vicino o dentro il tuo datacenter (o in un datacenter di un partner locale).

Porta i principali servizi di Azure (VM, Kubernetes, database, AI, sicurezza) on-premises o edge, mantenendo però la gestione unificata dal portale Azure.

Azure Local Perché è utile

- **Località dei dati** – utile per aziende con **requisiti di sovranità dei dati**, ad esempio sanità, pubblica amministrazione o manifatturiero con dati sensibili.
- **Bassa latenza** – i dati restano “vicini” e riducono i tempi di risposta, ottimo per IoT, automazione industriale, AI real-time.
- **Stessa esperienza Azure** – usi lo stesso portale, API e strumenti DevOps di Azure, ma il carico gira “a casa tua”.
- **Compliance e sicurezza** – ideale per settori regolati che non possono mandare tutto nel cloud pubblico.
- **Integrazione ibrida** – puoi combinare carichi su Azure pubblico e su Azure Local con un’unica governance (IAM, policy, monitoraggio).

Azure Local Differenze rispetto ad Azure Arc

Azure Arc collega le tue risorse locali al controllo di Azure (ma le risorse le gestisci tu).

Azure Local invece porta un **pezzo di Azure gestito da Microsoft** vicino a te: infrastruttura, patching, aggiornamenti sono in mano a Microsoft.

customer academy
FOR EVEN SMARTER COMPANIES

SERVIZI EOS

EOS Services ->
MICROSOFT SECURITY START-PACK

- Security Assessment by CSAT
- Entra ID - Identity
- Exchange Online - Mail Protection
- Intune - Endpoint Management
- Defender - Endpoint Protection
- Purview - Document Compliance Basic

EOS Services ->
MICROSOFT AZURE START-PACK

- Azure Infrastructure Assessment by AMT
- Azure Arc & Cloud for Defender
- Azure Local

MICROSOFT AZURE ESSENTIALS

- Azure Arc & Cloud for Defender Essentials (servizi Microsoft gratuiti)

Grazie!

customer academy
FOR EVEN SMARTER COMPANIES

WEB
www.eos-solutions.it

SEGUICI SU

eos solutions
A KUMAVISION GROUP COMPANY