RSA

OWN YOUR IDENTITY.

Minacce alle Identità nella nuova Era Digitale

Evoluzione dei rischi e dei relativi controlli di mitigazione

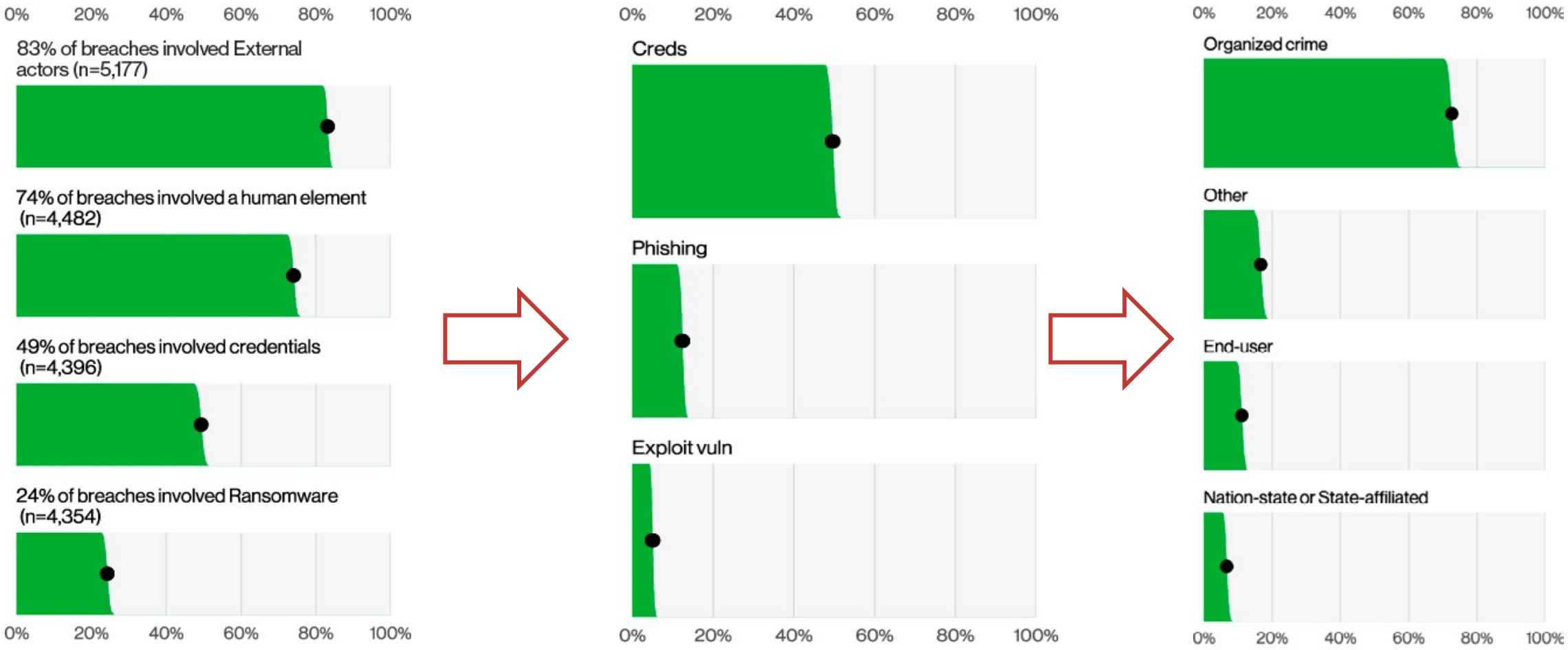
Pietro Valente *CISM®*, *CISSP®*, *CEH®*
pietro.valente@rsa.com
Sr. Sales Engineer

Agenda

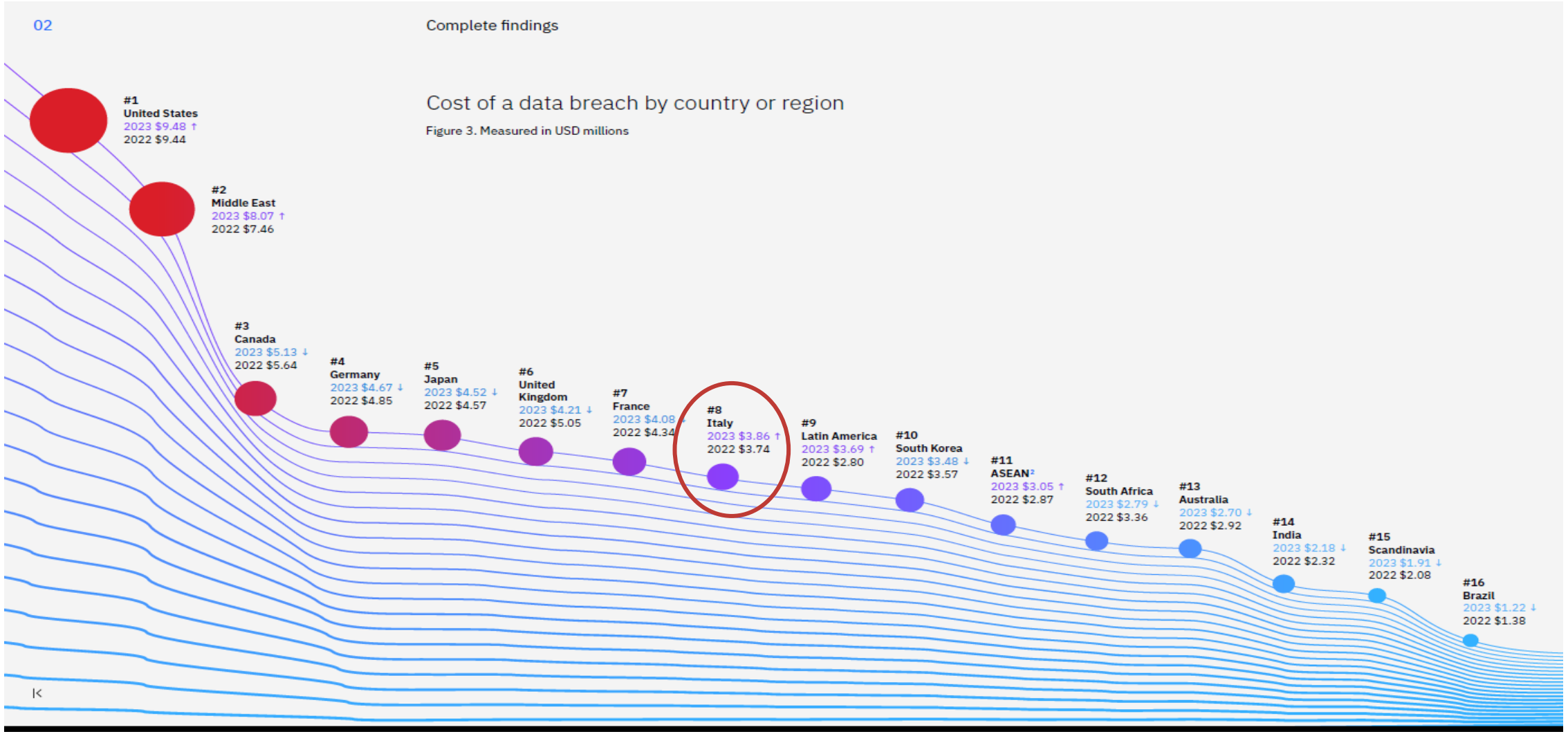
SECURITY SUMMIT 2024

- Analisi dati Report di settore
- Evoluzione attacchi con utilizzo Artificial Intelligence
- Quali sono i threat actors che ne stanno beneficiando
- Esempi di attacchi basati su AI avvenuti di recente
- Possibili Contromisure per abbassare il livello di esposizione

Data Breach Investigation Report (DBIR) di VERIZON



Costo Data Breach*



*Fonti tratte da “Cost of a Data Breach Report 2023” di IBM Security

Costo Data Breach*

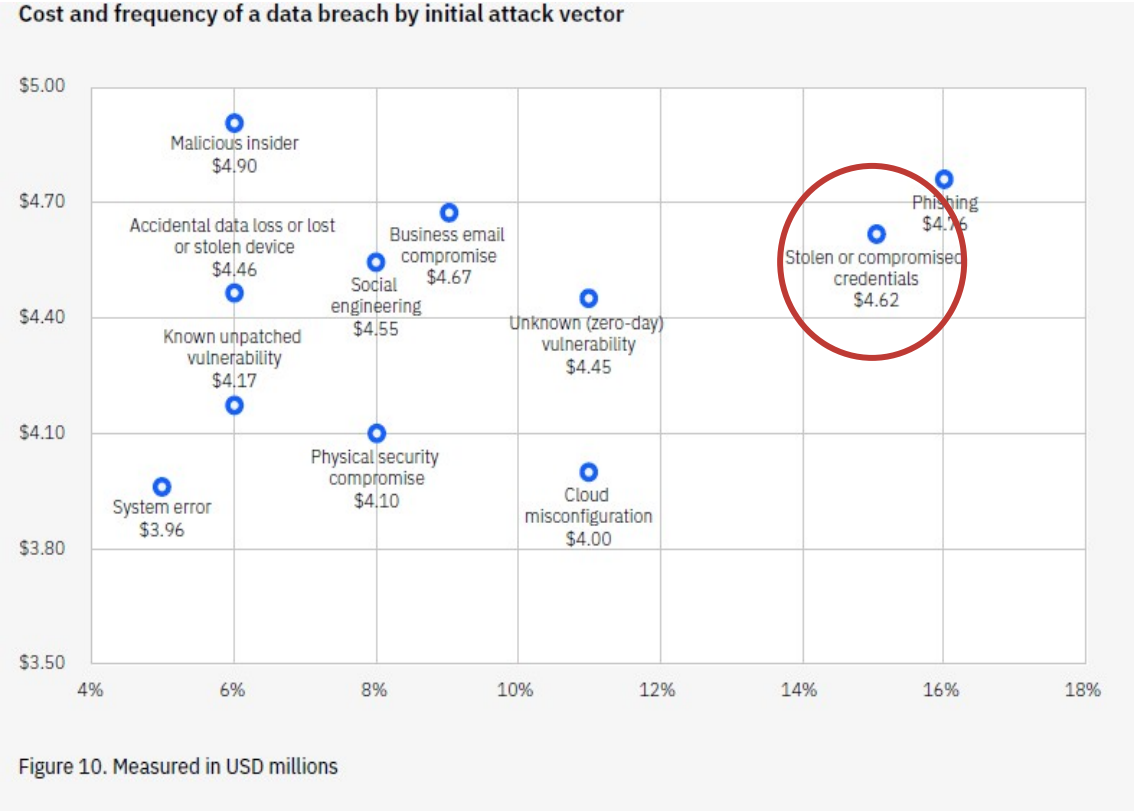


Figure 10. Measured in USD millions

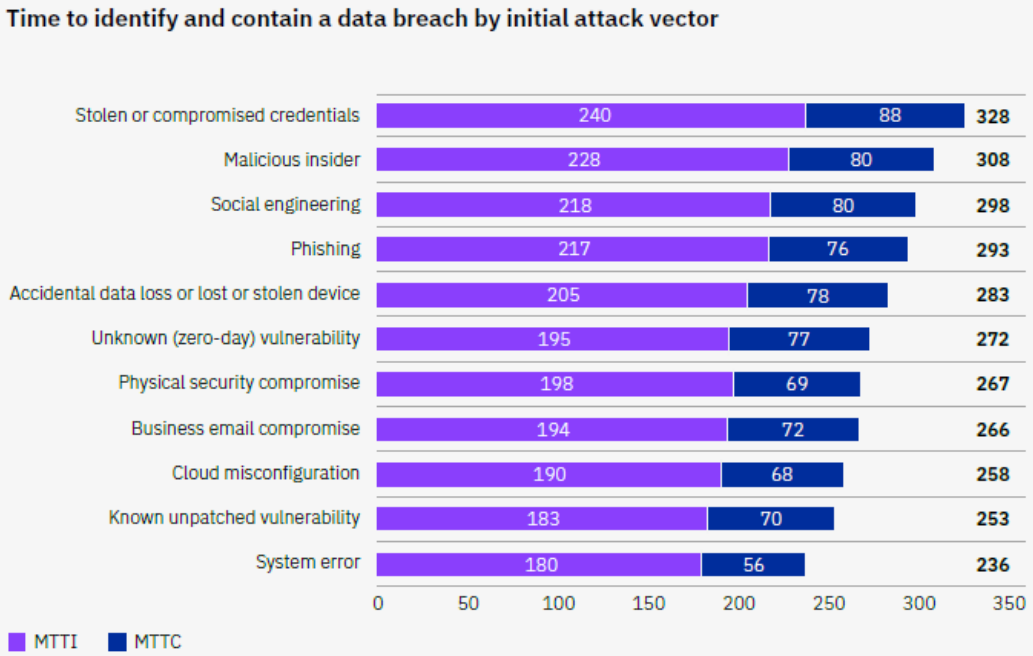


Figure 11. Measured in days

*Fonti tratte da “Cost of a Data Breach Report 2023” di IBM Security

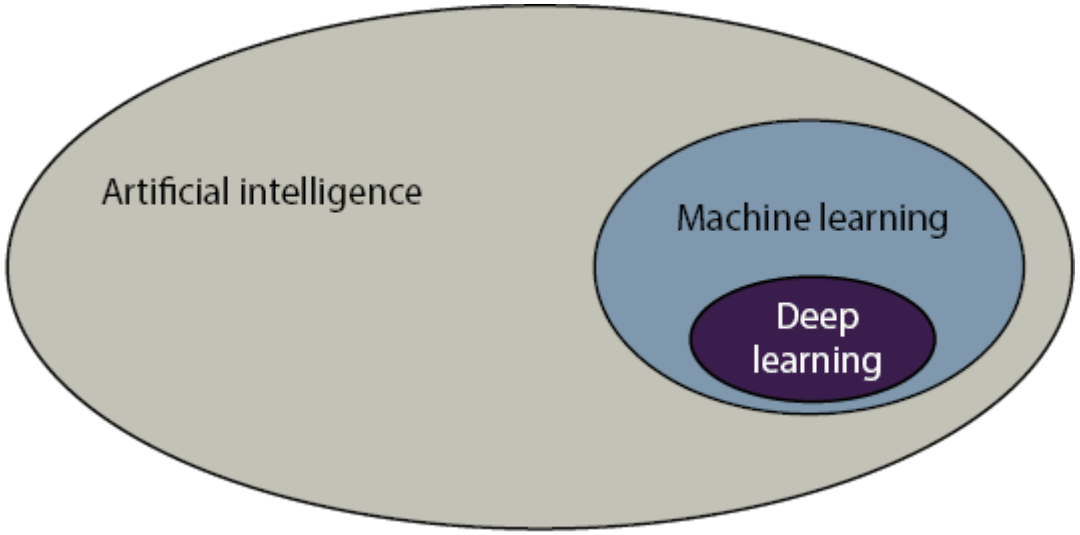
Artificial Intelligence

- *Impatto AI su Cyber Threats?*
- *Come possiamo affrontarle?*

RSA

Cosa è l'Artificial Intelligence (AI)?

- "*The set of all tasks in which a computer can make decisions*"
- Nelle community di Computer Science si parlava di AI già dal 1950 (Prof. Marvin Lee Minsky – Dartmouth AI Workshop 1956 – Cofounder of MIT).
  Il primo modello di "artificial neuron" è stato introdotto nel 1943 (McCulloch & Pitts)
- Machine Learning is the set of all tasks in which a computer makes decisions "*based on data*" (aka experience for humans… instead of logic and reasoning)
- Deep Learning è un campo del Machine Learning che usa le Neural Networks… o meglio… utilizza Deep Neural Networks

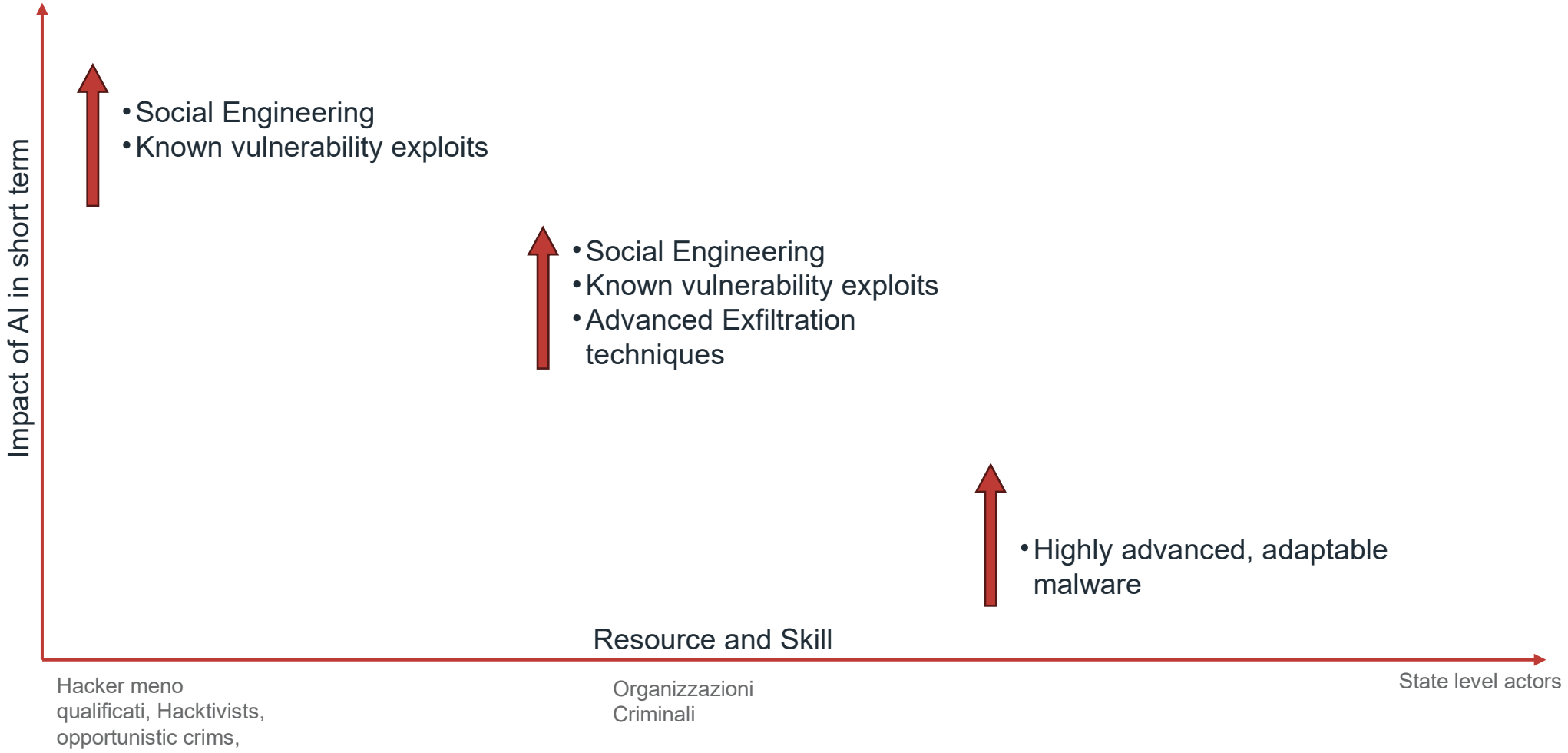


Improvements per un Attaccante

- **Prediction:** può essere usata per identificare la sequenza di tasti su uno smartphone o individuare il target o il software più vulnerabile da attaccare;
- **Generation:** può essere utilizzata per manomettere audio, video, individuare password o camuffare traffico di rete malevoli per eludere sistemi di detection;
- **Data Analysis:** può essere usata per estrarre informazioni utili da grosse quantità di dati al fine di individuare quali sono gli asset o i target critici da attaccare;
- **Information Retrieval:** può essere utilizzata per osservare oggetti o individui al fine di trovare dei punti di debolezza da sfruttare. Ad esempio attraverso l'analisi semantica di post sui social media si può individuare un dipendente scontento che può diventare un potenziali insider.

National Cyber Security Centre

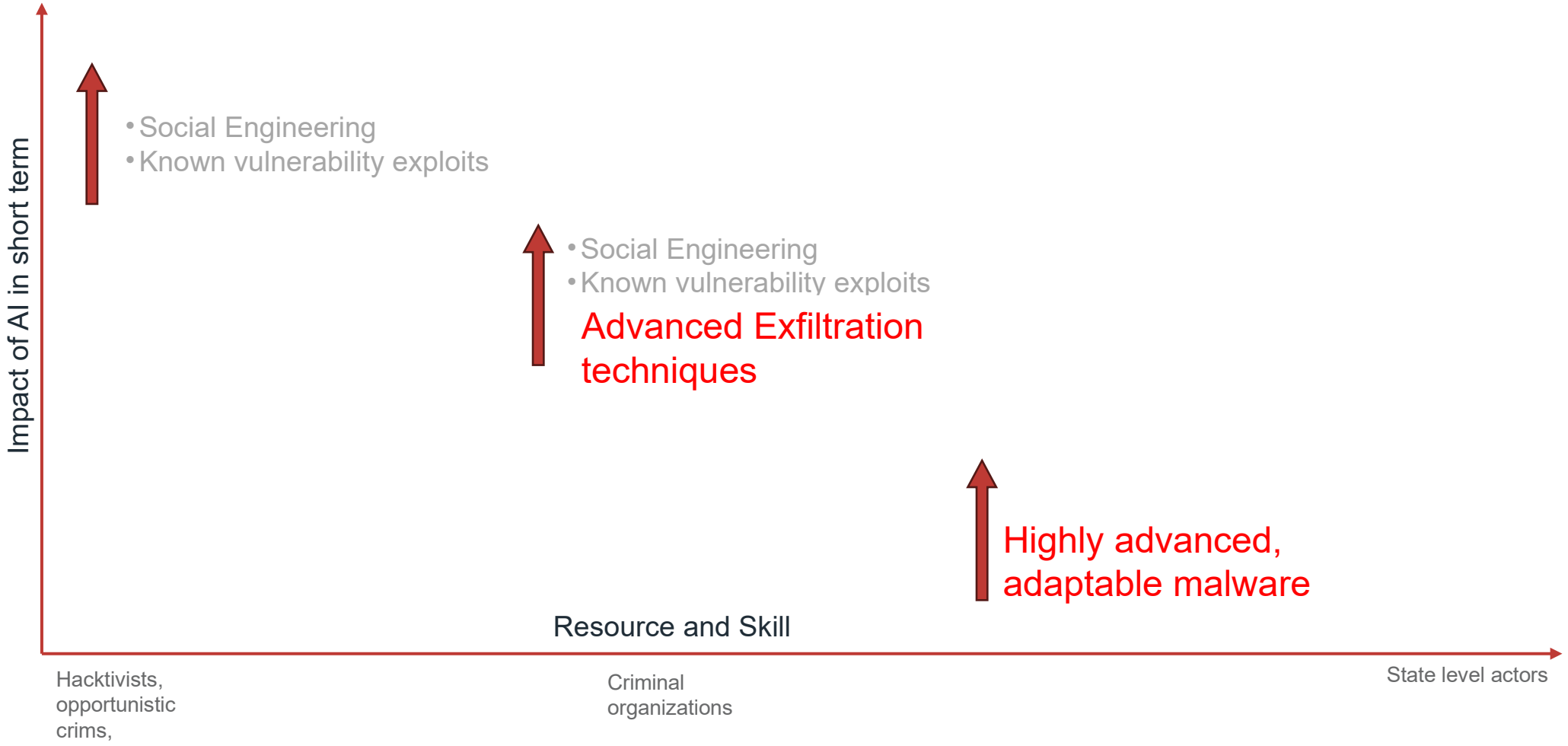
The near-term impact of AI on the cyber threat



RSA

National Cyber Security Centre

The near-term impact of AI on the cyber threat



RSA

OWN YOUR
IDENTITY.

Bad AI needs to eat too

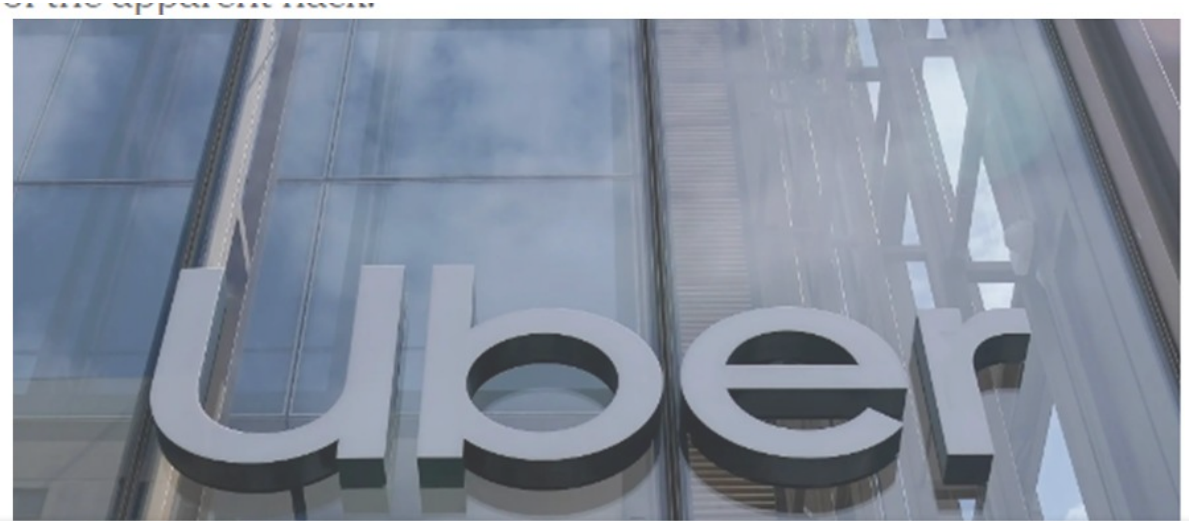
Breaking Down the SolarWinds Supply Chain Attack

March 11, 2021 Team SpyCloud Cyberattack Trends

When the public became aware of an advanced persistent threat (APT) responsible for compromising the SolarWinds Orion software supply chain in December 2020, experts were quick to warn it would likely be years – maybe decades – before the fallout could be fully accounted for. The more we learn about the attack, however, the more it seems we may never know the full extent of its damages. As speculation continues to abound, witness

By **Bill Toulas** October 6, 2023 09:53 AM 1

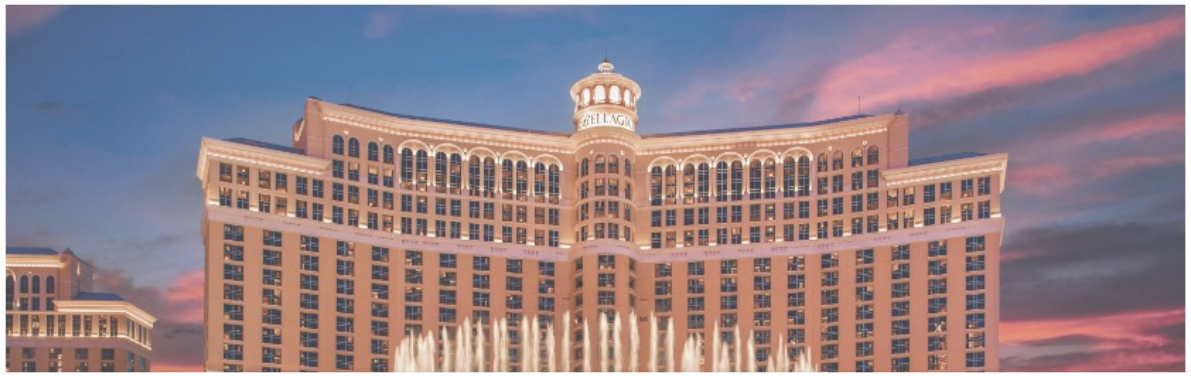
Third-party access controls



Third-party access controls, MFA bombing prevention

By **Bill Toulas**

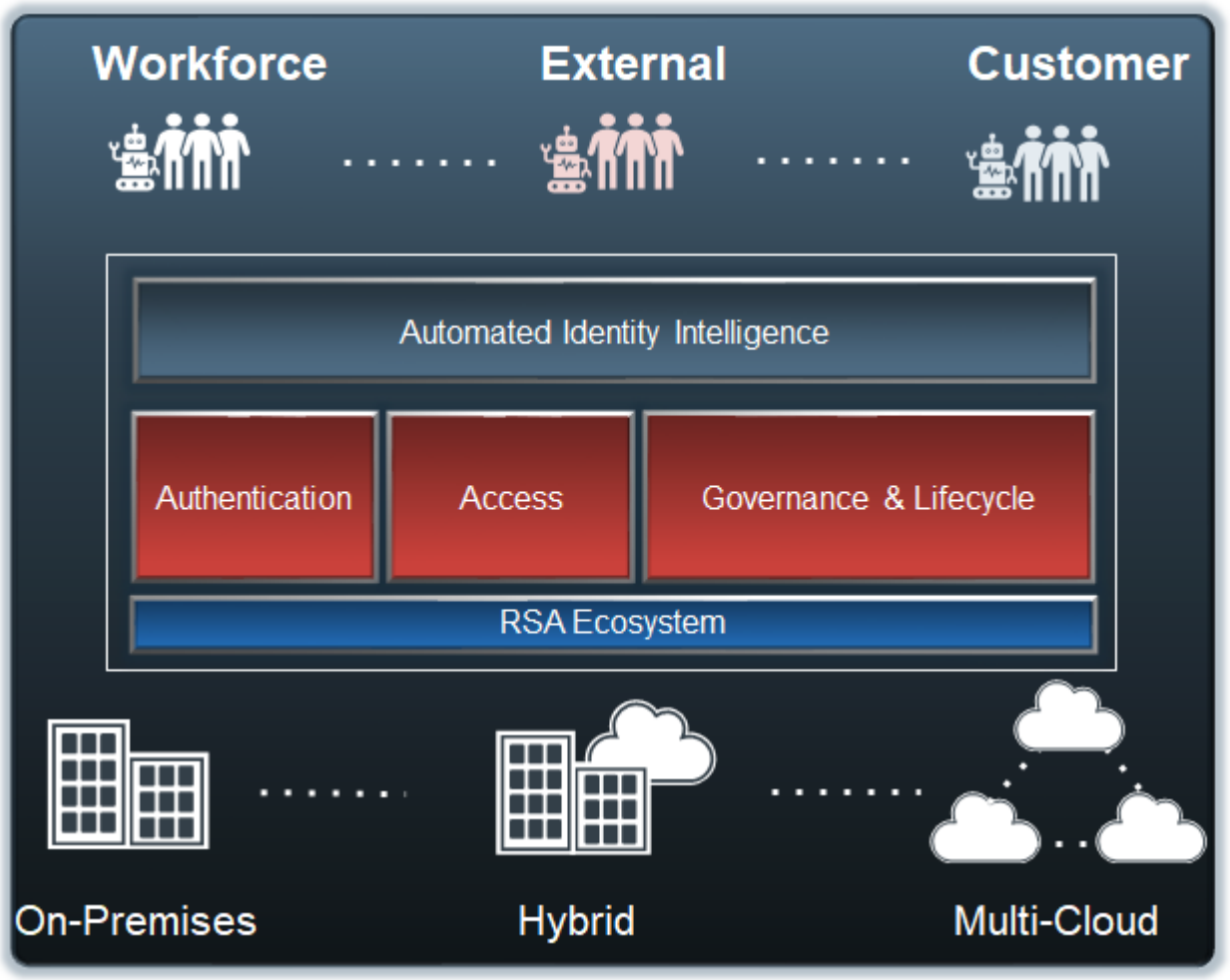
October 6, 2023 09:53 AM 1



Live user verification, ID Verification

…Regardless, AI will change the World for better or worse…

RSA Unified Identity Platform

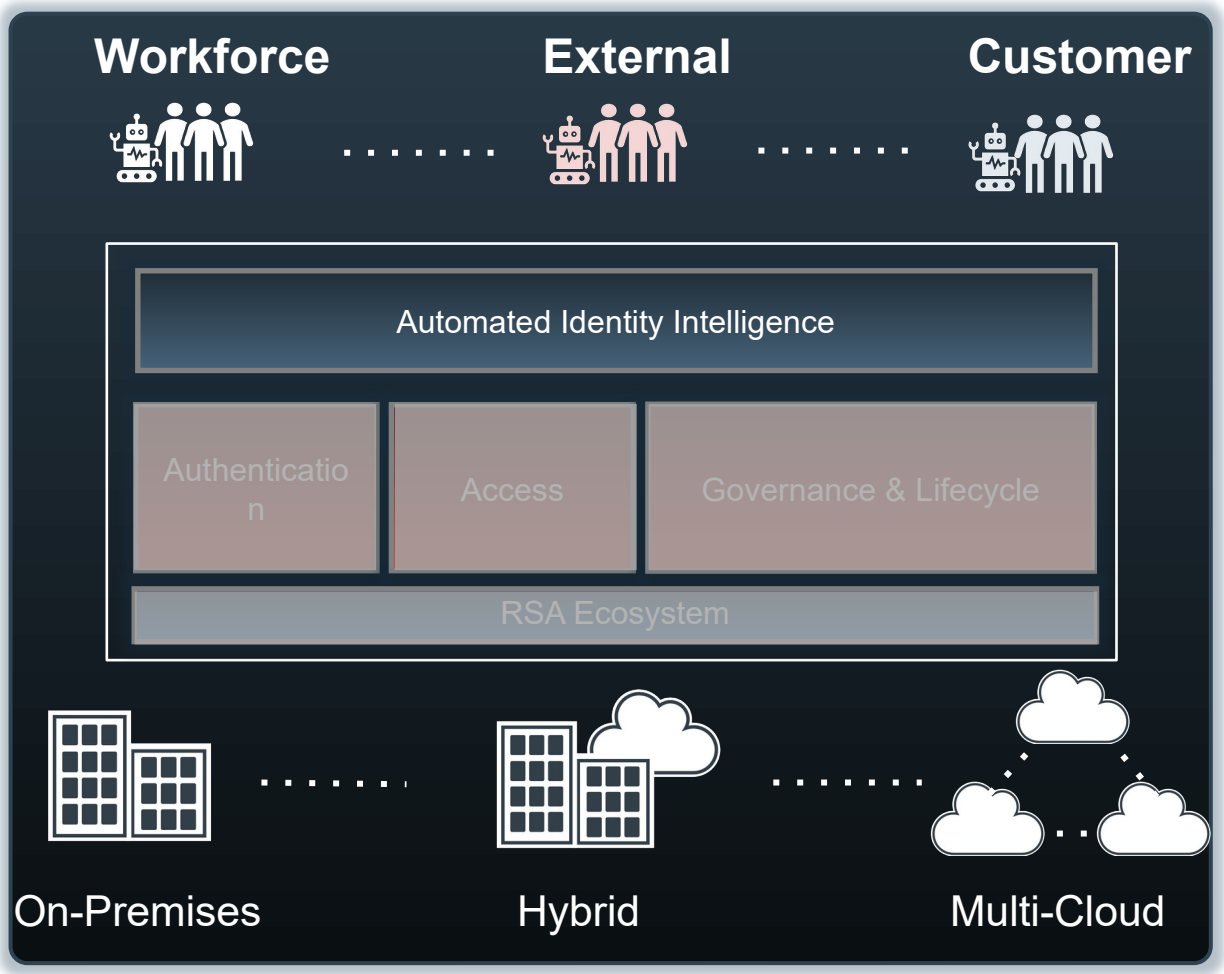


Security-First

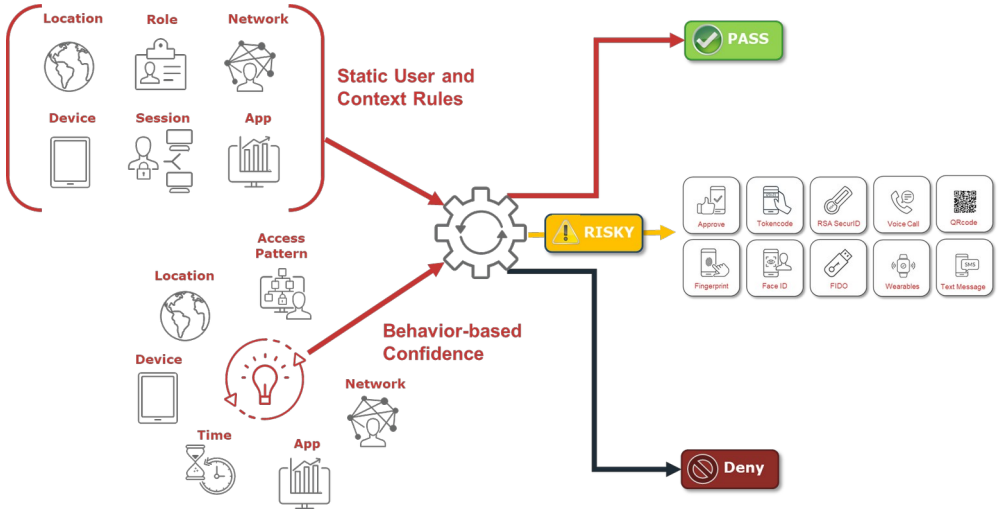
Intelligent

Open

RSA Unified Identity Platform – AI



AI RISK ENGINE



- Based on the user's behaviour
- Reduce step-up Authentication (only with low risk)
- Improve user experience

Per concludere…

- L’identità risulta ancora il vettore di attacco più usato, il più difficile da identificare e contenere e tra i quelli a maggior impatto economico per un’azienda;
- L’impatto dell’AI provocherà (sta già provocando) un aumento della numerosità degli attacchi e degli impatti che avranno sui target colpiti;
- L’AI ha bisogno di molti dati e di qualità per poter creare modelli sempre più efficaci. La protezione delle informazioni all’interno dell’azienda diventa un requisito ancora più cruciale;
- A valle di questo, una rivisitazione delle priorità sui controlli di sicurezza, forse sarebbe opportuno farla, ponendo maggiore attenzione sui Threat Vector più impattanti e frequenti come l’Identity;
- Una ***Unified Identity Platform*** che copre tutti gli aspetti di protezione dell’identità supportata da funzionalità di AI, siamo convinti che potrà contribuire a mitigare i rischi più importanti.

OWN YOUR
IDENTITY.

Thank You

RSA