Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA

SECURITY SUMMIT

Security Summit

Verona, 24 ottobre 2024

Identity. Cosa sappiamo di non sapere

Luca Bechelli, CS Clusit
Roberto Branz | Channel Account Executive Italy, di RSA Security

24 ottobre 2024 orario 14 – 14.40

Luca Bechelli

COMITATO SCIENTIFICO

PARTNER @P4I – GRUPPO DIGITAL360

74%

Aziende che hanno rilevato un **aumento dei tentativi di attacco cyber**

A cosa è dovuto l'aumento?

76% **Effettivo aumento delle minacce**

Delle organizzazioni

48% **Miglior capacità di rilevazione degli attacchi**

Delle organizzazioni

43% **Maggior esposizione al rischio dell'organizzazione**

Delle organizzazioni

12%

Aziende che hanno subito **attacchi cyber con conseguenze tangibili**

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Campione Survey CISO 2023: 110 grandi organizzazioni italiane

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Innovazioni digitali che generano nuove **opportunità** o **minacce** alla **sicurezza aziendale *corrente***

Cloud

- **L'adozione di soluzioni cloud è sempre più rapida e inevitabile**
- Il Cloud si conferma il primo trend per impatto attuale anche nel 2023

Impatto attuale

Impatto futuro

Digital Identity

- Si consolida l'esigenza di **certificare l'identità degli utenti** e di definire **privilegi e modalità di accesso a dati critici**
- La Digital Identity si conferma il trend in maggior crescita nello scenario attuale

Impatto attuale

Impatto futuro

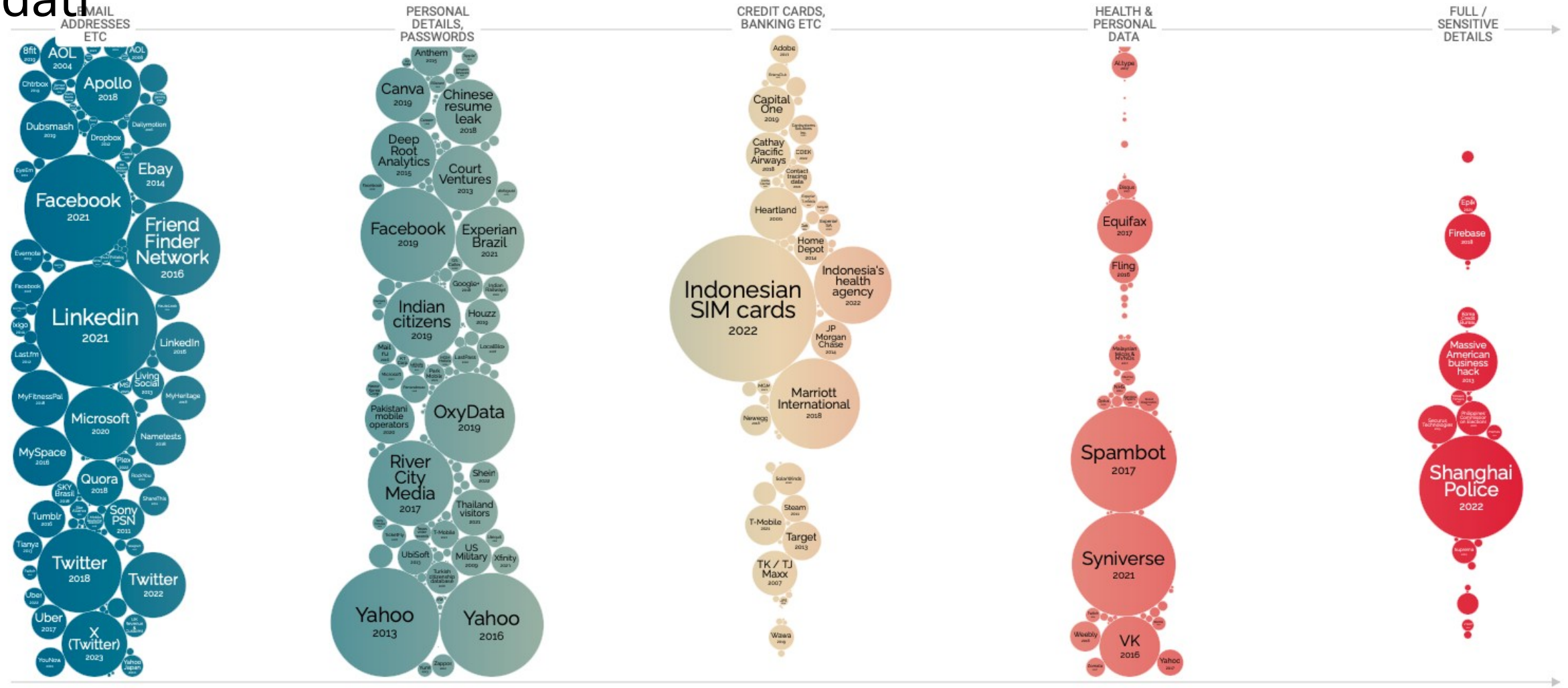
POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Campione Survey CISO 2023: 110 grandi organizzazioni italiane

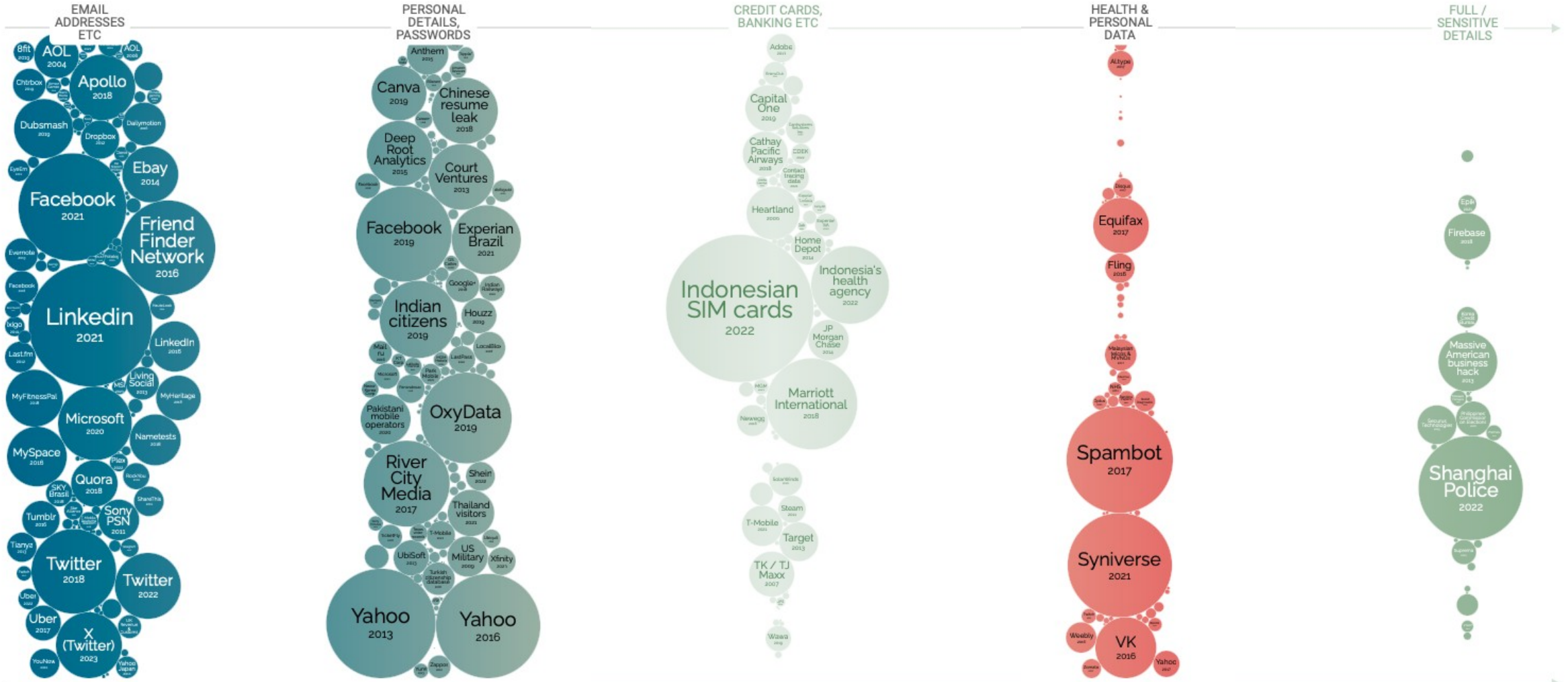
Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Data Breach per rilevanza dei dati



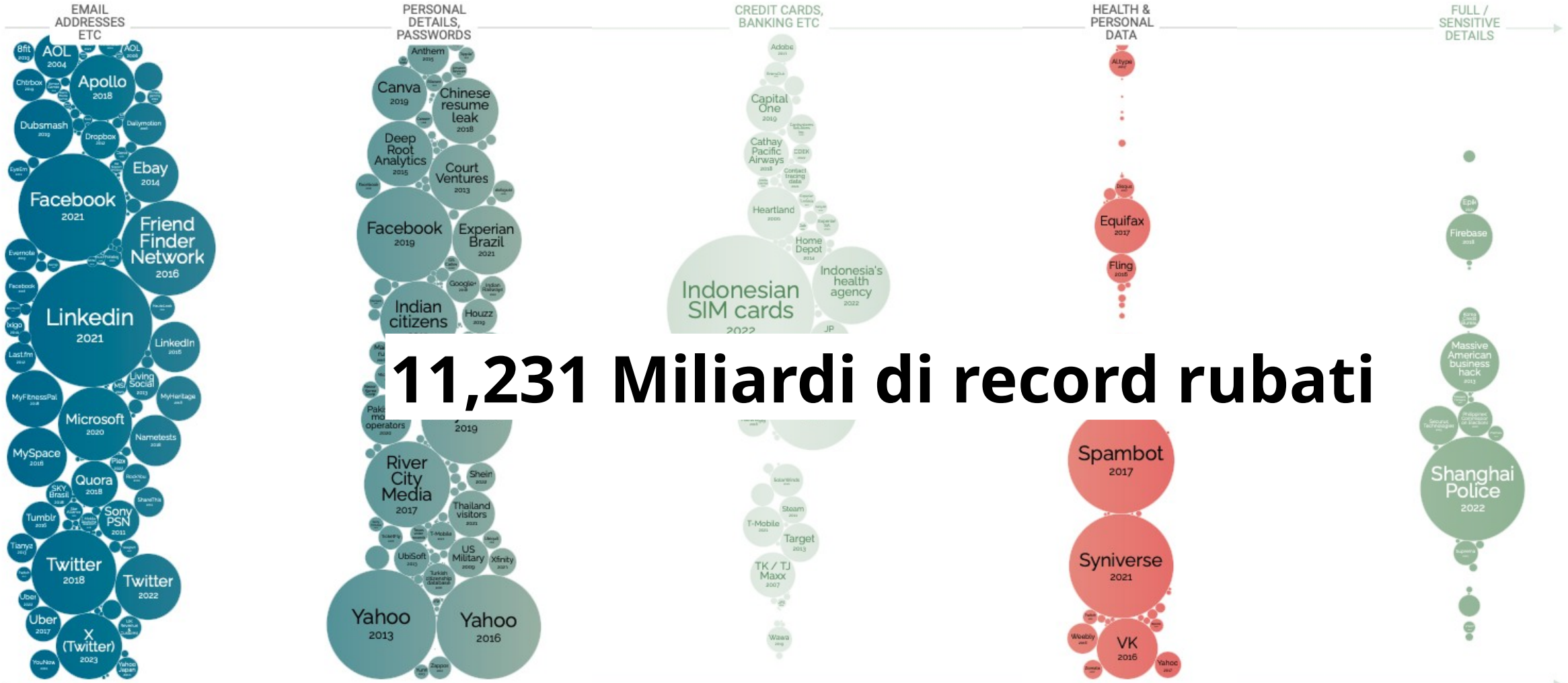
Data Breach per rilevanza dei dati



Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Data Breach per rilevanza dei dati



11,231 Miliardi di record rubati

Parliamo dei “fondamentali”

(89) I soggetti essenziali e importanti dovrebbero adottare un'ampia gamma di pratiche di igiene informatica di base quali principi zero trust, aggiornamenti del software, configurazione dei dispositivi, segmentazione della rete, gestione dell'identità e dell'accesso o sensibilizzazione degli utenti, organizzare per il loro personale una formazione e sensibilizzarlo alle minacce informatiche, al phishing o alle tecniche di ingegneria sociale. Inoltre, tali soggetti dovrebbero valutare le loro capacità di cibersicurezza e, se del caso, perseguire l'integrazione di tecnologie per il rafforzamento della cibersicurezza quali l'intelligenza artificiale o i sistemi di apprendimento automatico, per migliorare le loro capacità e la sicurezza dei sistemi informatici e di rete.

Considerando 89, Direttiva NIS2

Roberto Branz
Channel Account Executive Italy

RSA

Identità digitali
Cosa non sappiamo di non sapere

Branz Roberto

Channel Accaut Executive – Rsa Security

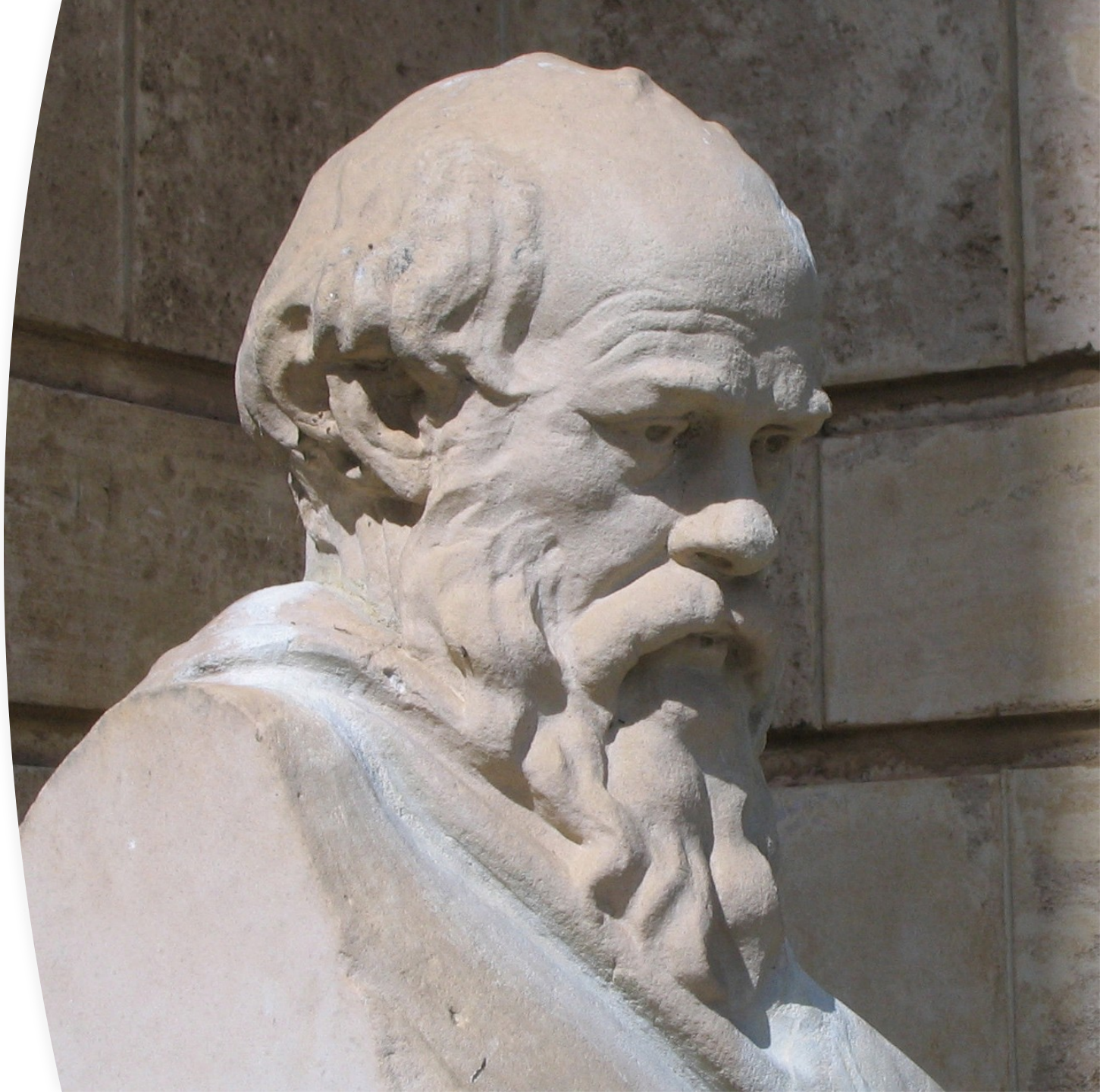
Roberto.branz@rsa.com

+39 3316453193

OWN YOUR IDENTITY.

La Sicurezza !

Termine che deriva dal latino «sine cura», cioè senza preoccupazione, può essere definita come la **«conoscenza che l’adozione di un sistema non produrrà stati indesiderati»**, in altri termini che «quello che faremo» non provocherà danni.



Why enterprises need phishing-resistant for the future of work

Human element

68% of breaches involved the human element in 2024

Source: Verizon

63% of breaches

In financial services are caused by phishing in 2024

Source: Verizon

Costly & difficult

Employees lose 11 hours each resetting passwords. 40% of all help desk calls are password resets

Source: Bloomberg

4000 attacks

Password attacks per second

Source: Microsoft

Global Mandates

Mandates the deployment of phishing-resistant MFA and Zero Trust Architecture

Utente è l’anello debole

- Forse non è tutta colpa sua !

Nemmeno l’umano dell’help desk, se la passa meglio !

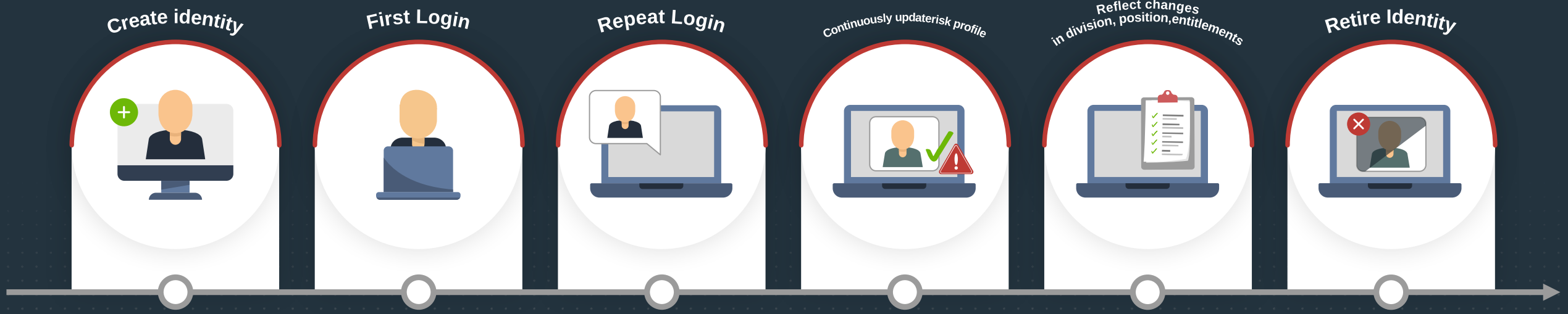
Servizio | Cybersicurezza

Attacco ai casinò MGM: danno da 100 milioni di dollari

A fine settembre la storica catena di sale da gioco americane era stata presa di mira da pirati informatici.

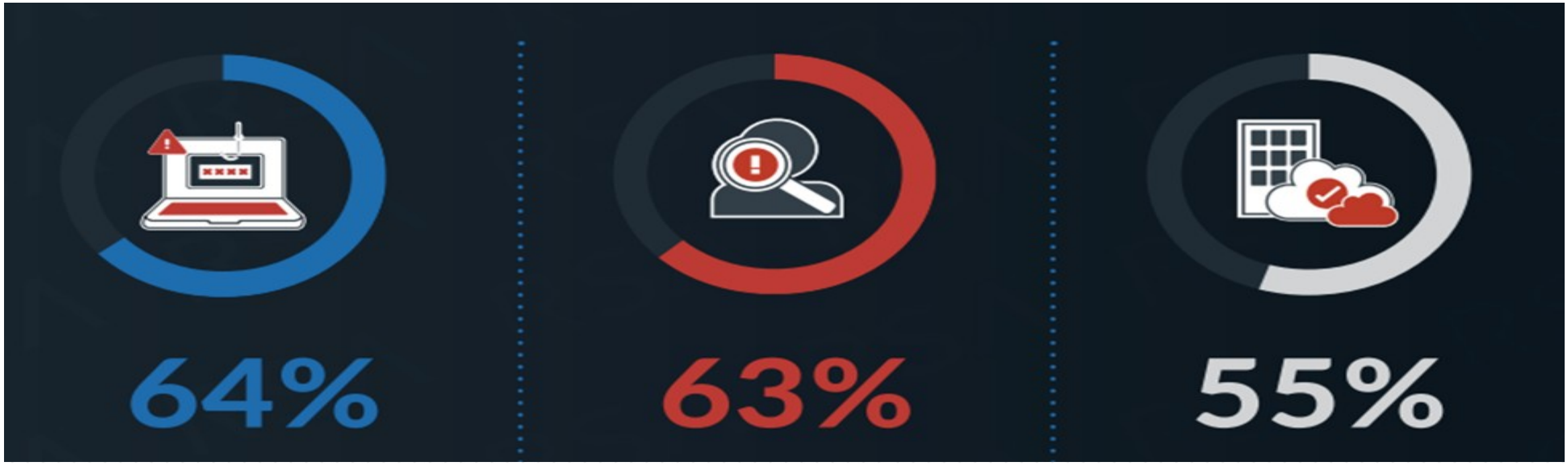
6 ottobre 2023

Managing millions of identities and billions of identity entitlements and events is complex



Protecting identities throughout their lifecycle is critical to mitigate risk

IQ Identity Test



Il 64% non ha selezionato le tecnologie di best practice come strumento per mitigare il phishing

Il 63% non conosceva quali fossero le componenti di identity security necessarie per indirizzare la strategia Zero Trust

Il 55% non ha compreso a pieno l’importanza della gestione dell’identity per innalzare la postura di sicurezza di un’organizzazione

Maggiori dettagli

- Rapporto Clusit 2024 : https://clusit.it/rapporto-clusit/ da pagina 191

Market and Customer Trends

1. **Cyberthreats and Regulatory mandates**
   Governmental and zero trust mandates = MFA for everyone
2. **Cloud Adoption/IT modernization**
   Complexity of managing identities across cloud, APIs, DevOps
3. **Passwordless/FIDO**
   Improving security and user productivity
4. **Adaptive Zero Trust**
   Static rule-based access ineffective in a dynamic world
5. **Platform Convergence**
   Customers seeking Identity Security Platform not point products
6. **Digital Experiences**
   Need to protect identities for workers, external users & customers

We look at identity security differently

Risk-based Security Beyond Access Control

Accelerate Zero Trust Maturity

Built for Highly Regulated Industries

Flexibility & Control

Future-proof Security

Solving the Identity Crisis involves more than just MFA

WHO
is the user

Authentication

Phishing
MFA fatigue
Brute force

WHAT
can they access

Access

Excess privilege
Shared accounts
Shadow IT

WHERE
is it managed

Directory

Weak enrollment
Password reset
Credential recovery

WHEN
can they use it

Lifecycle

Manual processes
Privilege escalation
Rubber stamping

WHY
do they have it

Governance

Orphaned accounts
Inappropriate access
SoD violations

RSA Unified Identity Platform

Identity: The Foundation of a Zero Trust Approach

Identity Challenges

WHO
is the user

- Users
- Devices

WHAT
can they access

- SaaS Apps
- On-Prem
- Privileged

WHY
do they have access

- Role
- Entitlement
- Dynamic

WHEN
and for how long

- New User
- Temp User
- J-M-L

HOW
are they managed

- Employee
- Partner
- Customer

ID Plus Solution

Authentication

- Multi-factor
- Passwordless
- Behavioral

Authorization
coming in June

- RBAC/ABAC
- Adaptive Access
- Single Sign-On

Governance
now in cloud

- Reviews
- Relevancy
- Policy

Lifecycle
now in cloud

- Birthright
- Requests
- Provisioning

Directory
in development

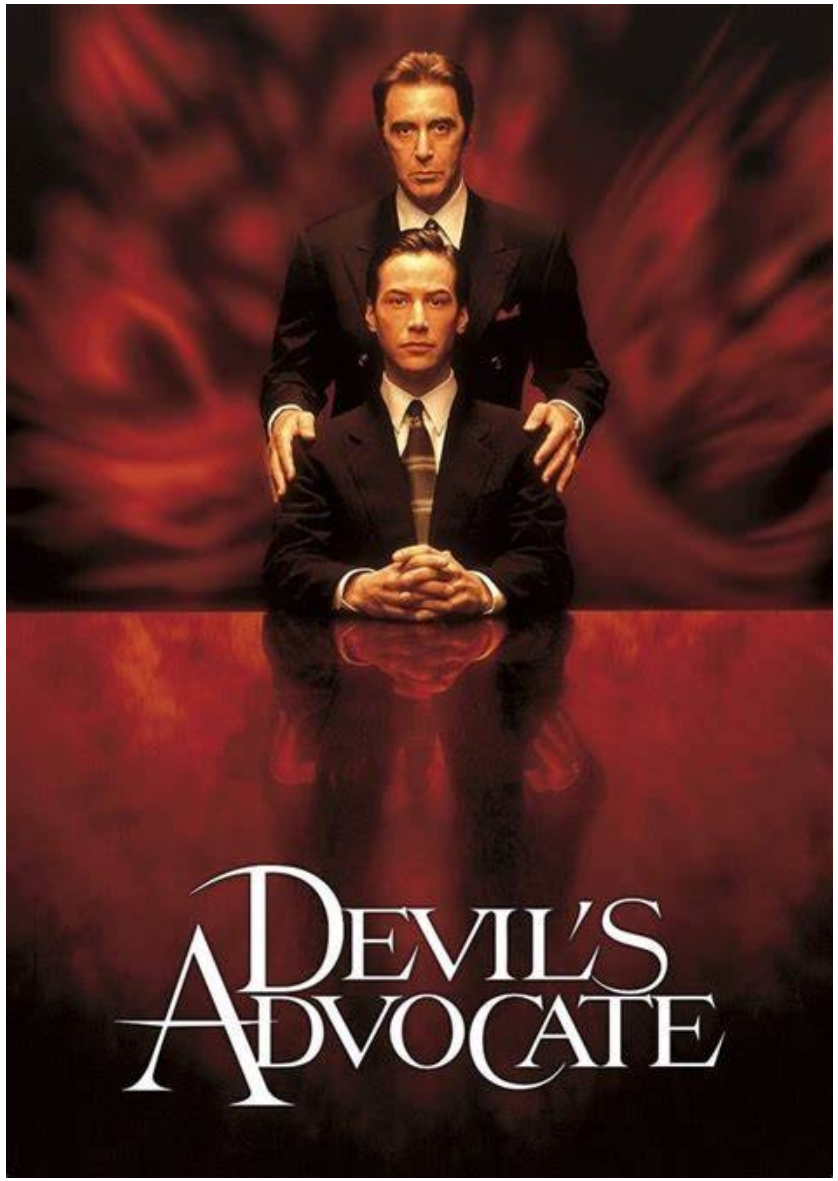
- AD/LDAP
- Cloud users
- DB/proprietary

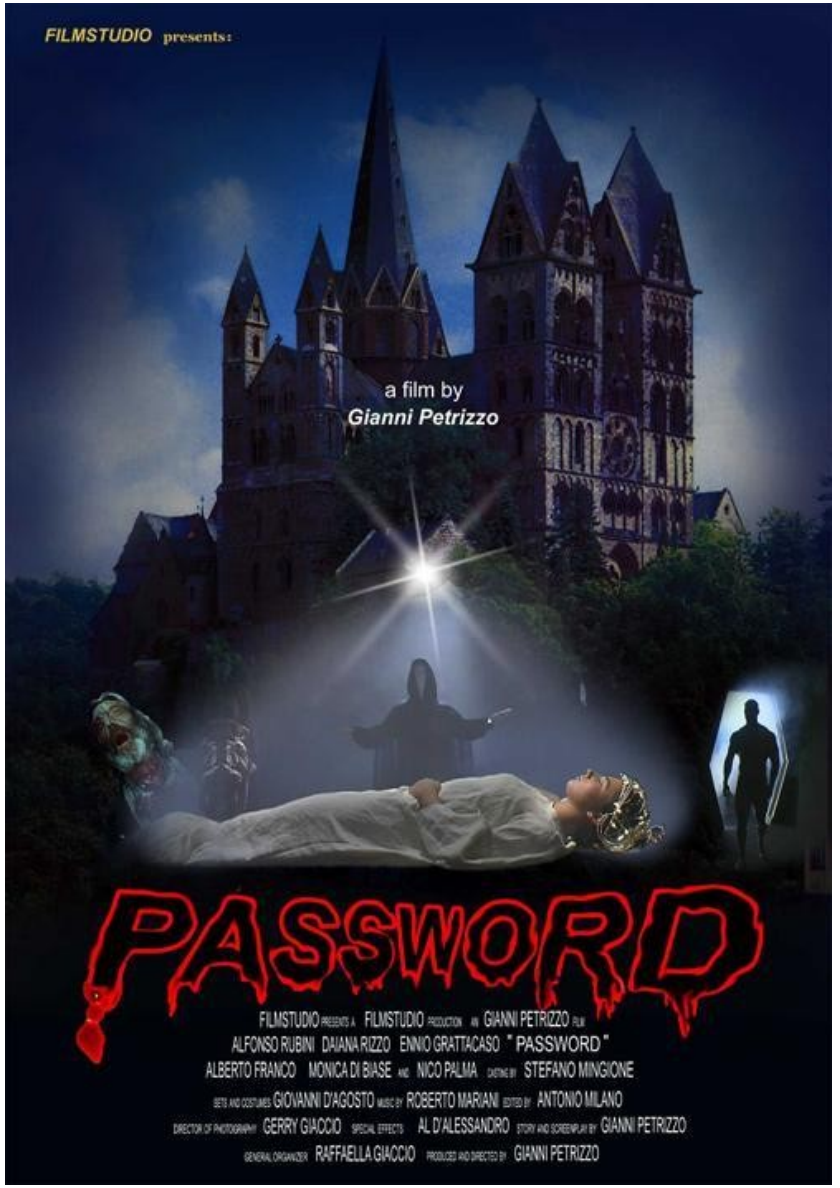
3 cose sull’identitv

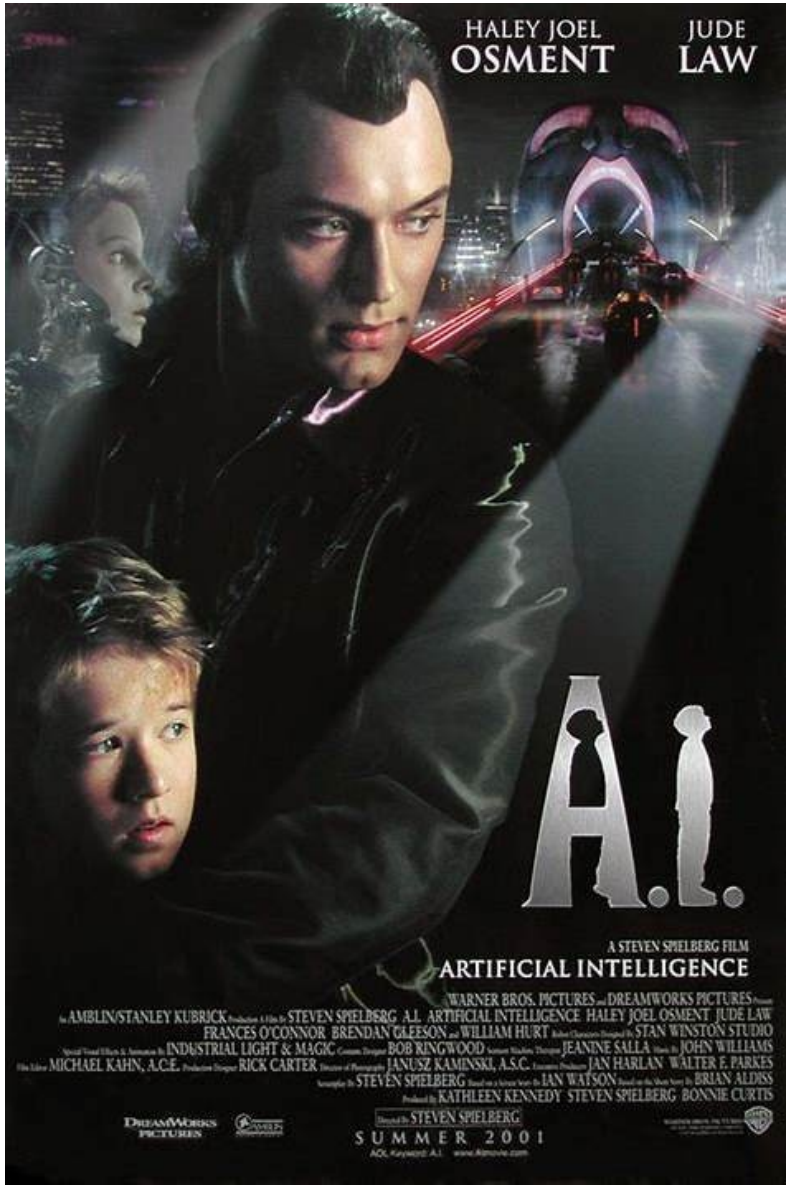
Basta password

Normative e best practice (NIS2 e Zero Trust)

Fatevi aiutare Da RSA. (e anche dall’AI)


DEVIL'S ADVOCATE


FILMSTUDIO presents:
a film by
Gianni Petrizzo
PASSWORD
FILMSTUDIO PRESENTS A FILMSTUDIO PRODUCTION AN GIANNI PETRIZZO FILM
ALFONSO RUBINI DAIANA RIZZO ENNIO GRATTACASO "PASSWORD"
ALBERTO FRANCO MONICA DI BIASE AND NICO PALMA CASTING BY STEFANO MINGIONE
SETS AND COSTUMES GIOVANNI D'AGOSTO MUSIC BY ROBERTO MARIANI EDITED BY ANTONIO MILANO
DIRECTOR OF PHOTOGRAPHY GERRY GIACCIO SPECIAL EFFECTS AL D'ALESSANDRO STORY AND SCREENPLAY BY GIANNI PETRIZZO
GENERAL ORGANIZER RAFFAELLA GIACCIO PRODUCED AND DIRECTED BY GIANNI PETRIZZO


HALEY JOEL OSMENT
JUDE LAW
A.I.
A STEVEN SPIELBERG FILM
ARTIFICIAL INTELLIGENCE
WARNER BROS. PICTURES and DREAMWORKS PICTURES Present
A KUBRICK/SPIELBERG A.I. ARTIFICIAL INTELLIGENCE HALEY JOEL OSMENT JUDE LAW
FRANCES O'CONNOR BRENDAN GLEESON and WILLIAM HURT
INDUSTRIAL LIGHT & MAGIC BOB RINGWOOD JEANINE SALLA JOHN WILLIAMS
MICHAEL KAHN, A.C.E. RICK CARTER JANUSZ KAMINSKI, A.S.C. JAN HARLAN WALTER F. PARKES
STEVEN SPIELBERG IAN WATSON BRIAN ALDISS
KATHLEEN KENNEDY STEVEN SPIELBERG BONNIE CURTIS
DreamWorks PICTURES
STEVEN SPIELBERG
SUMMER 2001

NIS2 - Risk Management Measures

- 17 October 2024, the Commission shall adopt implementing acts
- Policy on Risk analysis and Information Systems
- Incident handling
- Business Continuity
- Supply Chain Security
- Security in Network and Information systems acquisition, development, maintenance, vulnerability handling
- Assessing effectiveness of processes and procedures
- Basic cyber hygiene and training
- Use of cryptography
- use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity
- human resources security, access control policies and asset management

Recommendation: adopt a wide range of basic cyber hygiene practices, such as **zero-trust principles**, software updates, device configuration, network segmentation, identity and access management

ID Plus: Passwordless Experience

A modern, intuitive, and frictionless experience **FOR EVERY USER**

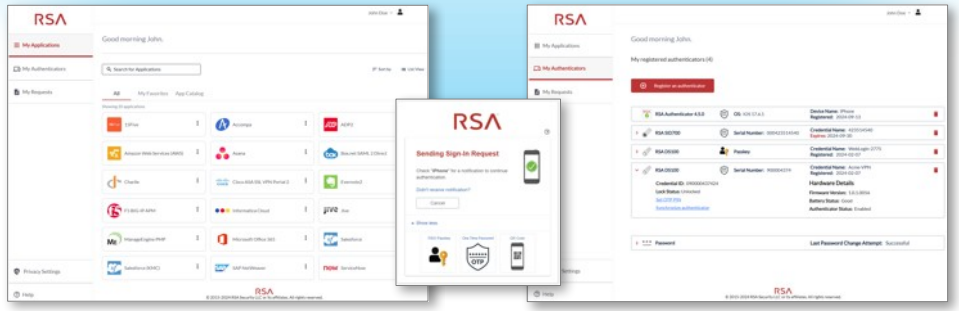
RSA DS100

iShield Key 2 Series

RSA Authenticator App
for iOS / Android

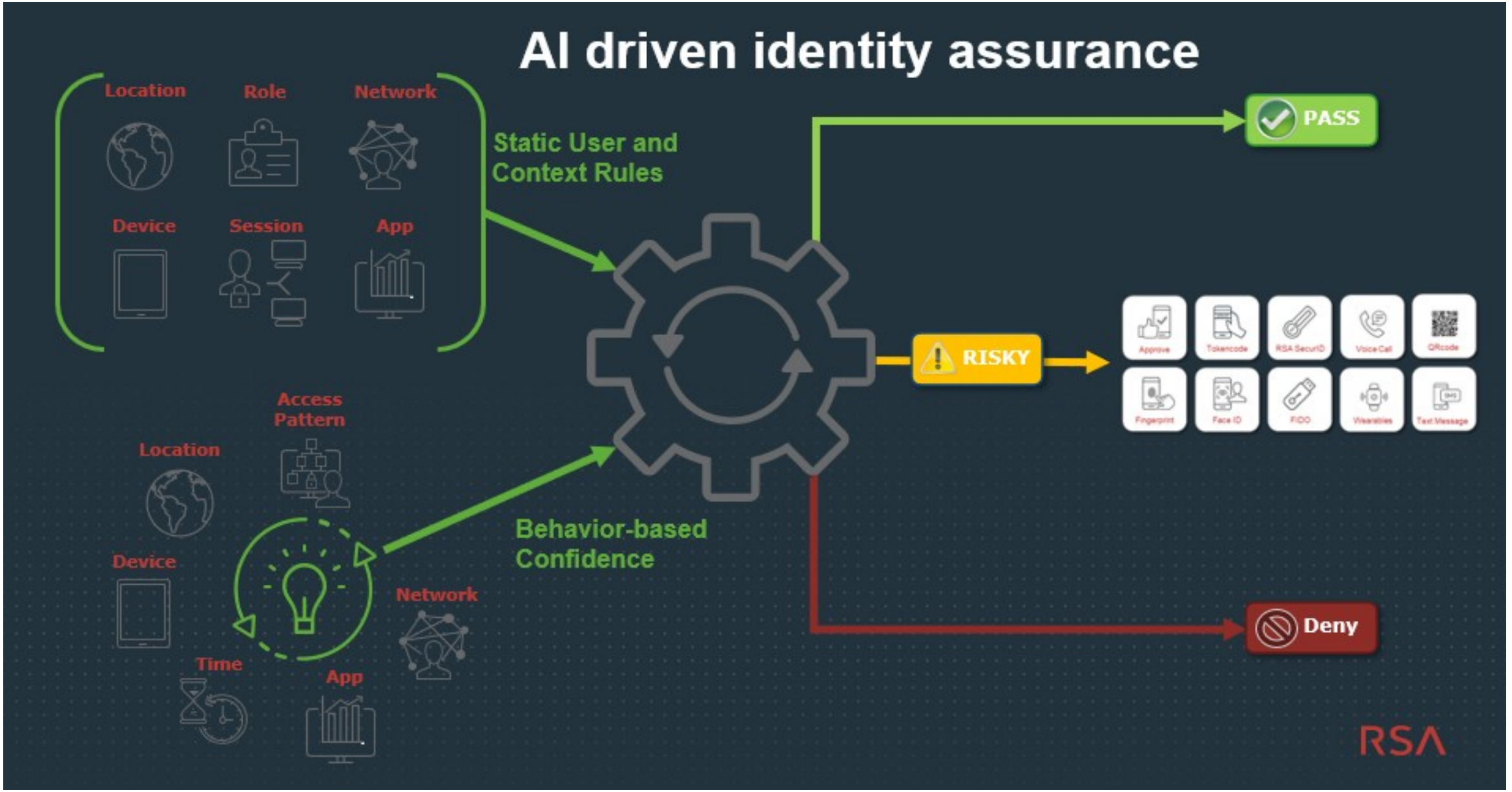
Secure passwordless made easy

- Self-service enrollment & recovery
- Risk-based single sign-on
- Single solution for SaaS / web & legacy apps

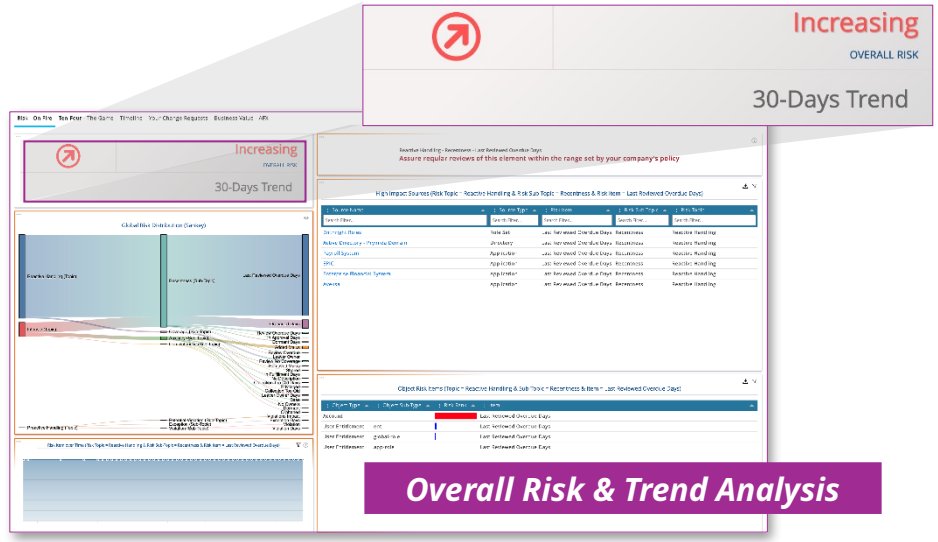


Zero Trust security beyond FIDO

- ID Verification (gov't-issued ID / mobile match)
- Identity Intelligence (Risk AI / Mobile Lock)
- Risk-based governance & lifecycle automation

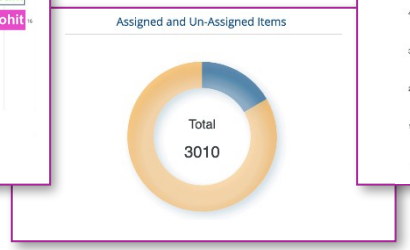

AI driven identity assurance
Location
Role
Network
Device
Session
App
Static User and Context Rules
PASS
RISKY
Approve
Tokencode
RSA SecurID
Voice Call
QRcode
Fingerprint
Face ID
FIDO
Wearables
Text Message
Access Pattern
Location
Device
Network
Time
App
Behavior-based Confidence
Deny
RSA

Risk AI: Governance-Based Risk Intelligence & Insights

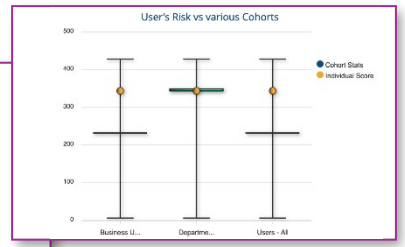


Overall Risk & Trend Analysis

Gamification



Review Status



Risky Users

Benefits and Features

- **Improve speed and quality of decision making** through data analysis & visualization
- **Reduce cost of audit-readiness** through intelligent discovery and evidence collection
- **Increase user compliance** through an enhanced experience and in-product gamification
- **Customize and build new dashboard elements** with full support for actionable drill down

RSA + elementity
WHEN SUBJECT EXPERTISE MATTERS

(Now Available in G&L 8.0)

NEW Risk Engine

What is it?

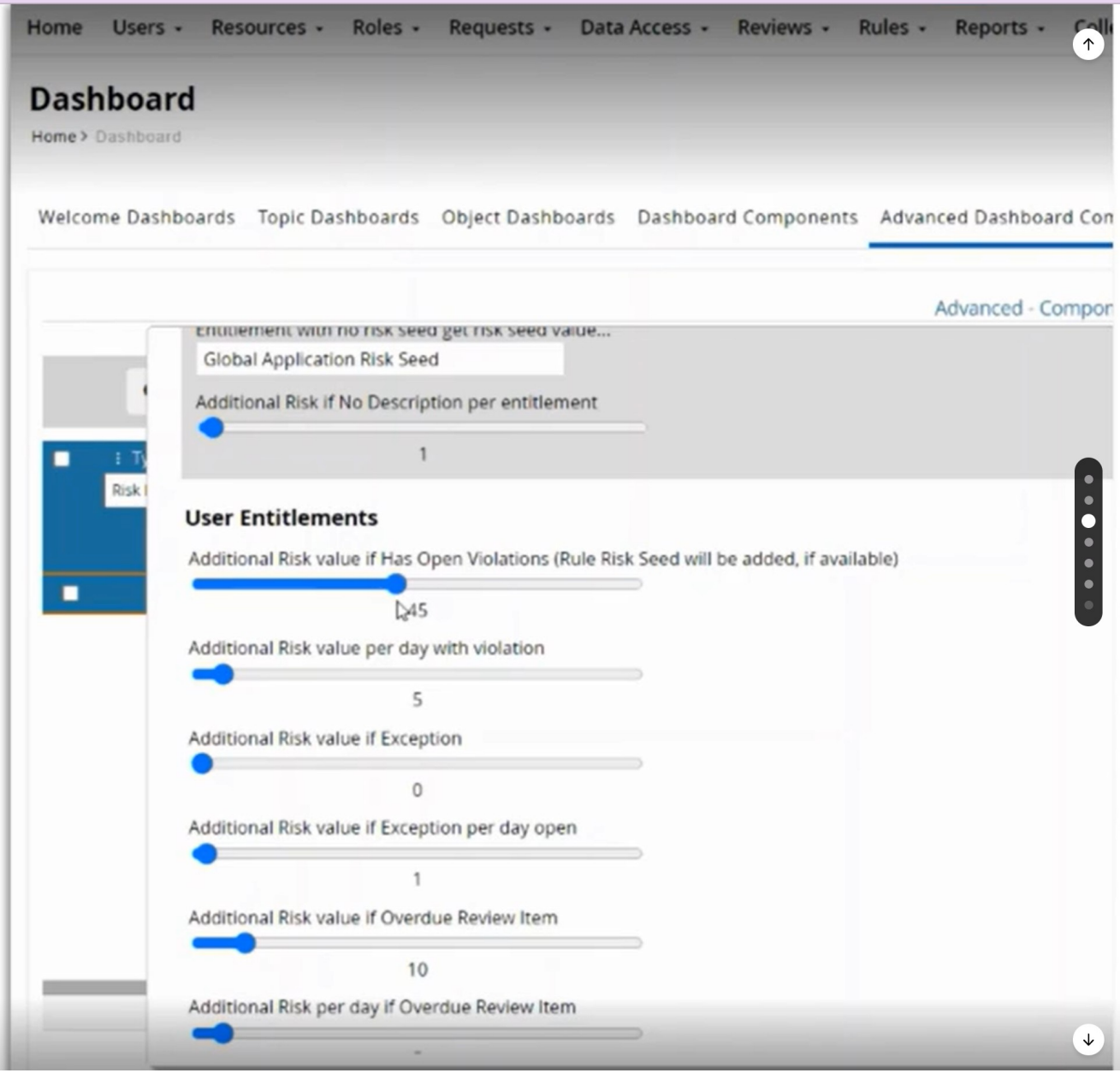
A configurable engine that helps uncover risk insights such as orphaned accounts, policy violations, over-entitled identities and more.

Why will customers & prospect care?

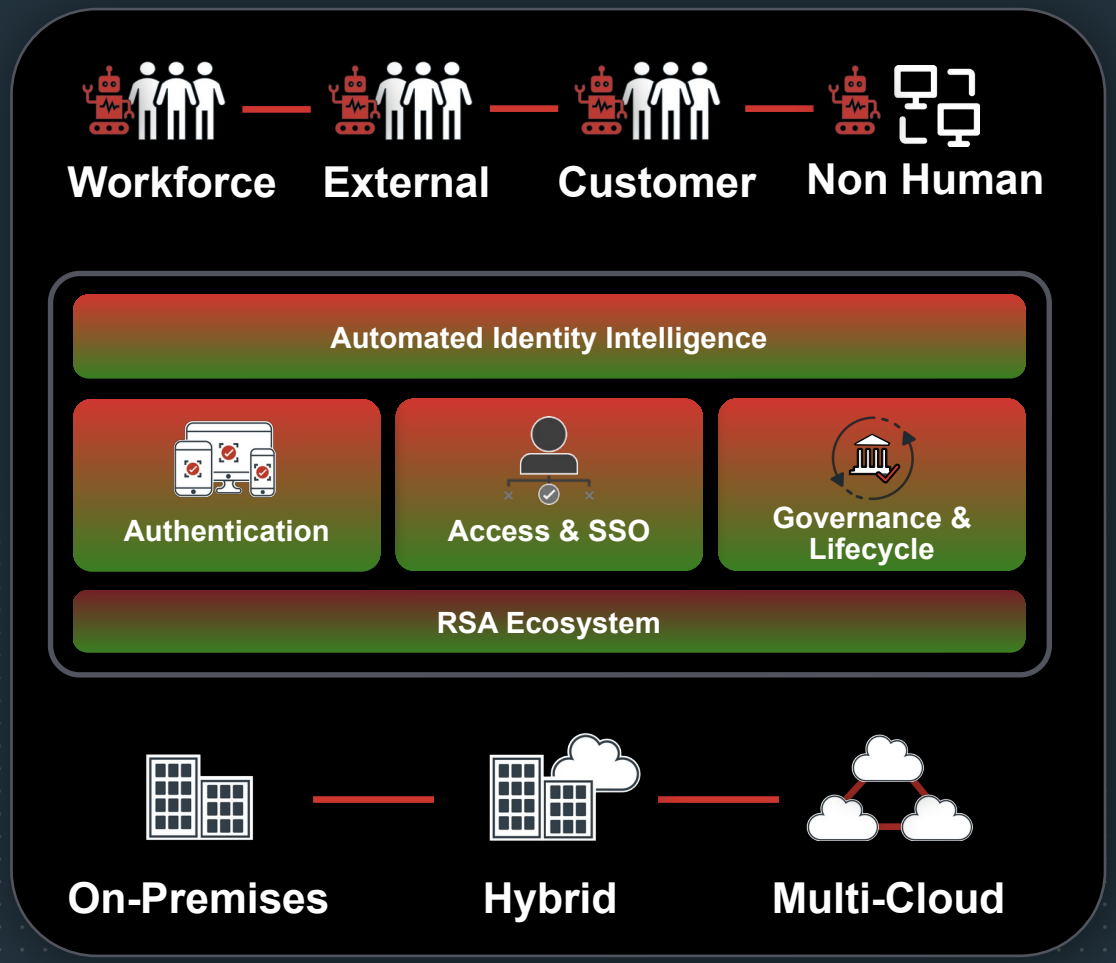
- Uses our Advanced Dashboards to visually depict and interact with the data, it's easy for administrators to identify problematic areas.
- Provides recommendations to mitigate identified risk.
- Includes a quick view that describes how overall risk has been trending over the last 30 days.

How does it work?

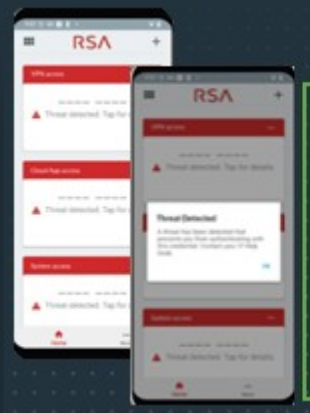
Customize the Risk Engine with sliders based on company policy.



RSA Unified Identity Platform



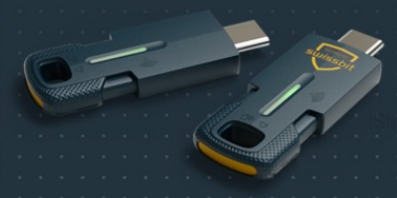
Security-First



Mobile Lock

- Detect threats on mobile devices
- No separate installation required
- Establish trust on mobile devices
- Leave other device functions unaffected
- Restrict authentication to protect resources

Passwordless multi-use authenticator: FIDO passkey (device-bound), OTP, and PIV smartcard



- Secure Password-less hardware authenticator
- Fido + OTP + PIV
- FIPS 140-3 (level 3) validated crypto module
- USB-A or USB-C and NFC
- Upgradable

Fidarsi é bene

ma la tecnologia é meglio

cit. Dr. Selena Milanovic