TD SYNNEX

RSA Security

La protezione delle identità come elemento fondamentale della sicurezza

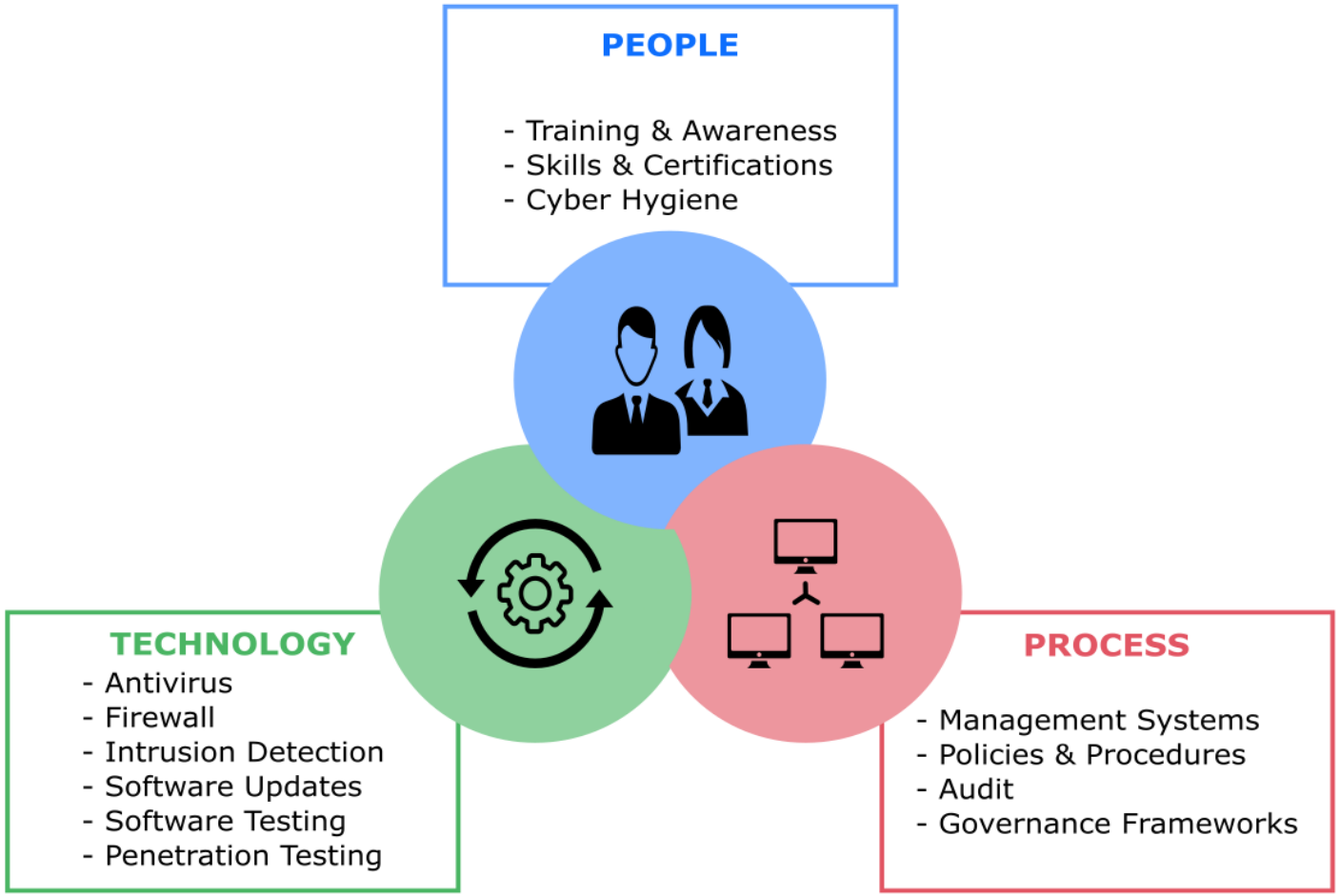
20 Dicembre 2024

Webinar

Roberto Branz – Channel Account Executive – RSA Security
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

TD SYNNEX

Cyber Security Pillars



CyberSec – Alcuni numeri

>30%
Increase in cyber threats in 2024

88%
Data breaches caused by compromised identities

>$1B
ransomware payments maid in the US alone in 2023

$5.2T
Estimated cost of cybercrime in 2024

~7.2B
Records stolen in 2023, more than one per person on earth

TD SYNNEX

Perché le azienda hanno bisogno di proteggere le identità

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

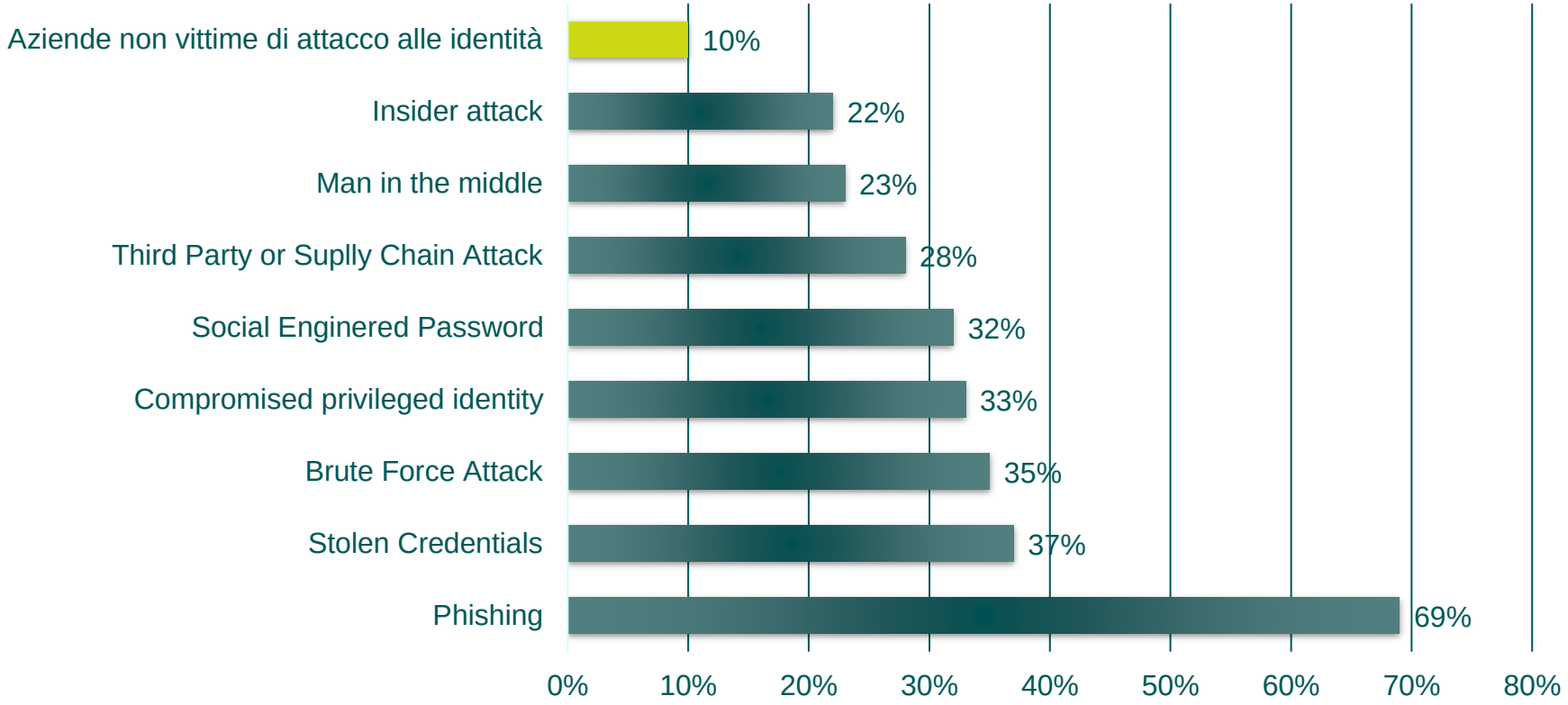
Gestione delle identità

4,88 M $

Il costo medio globale di una violazione dei dati nel 2024 è aumentato del 10% rispetto allo scorso anno ed è il più alto di sempre.

Fonte: IBM

Tipi di attacchi alle identità subiti lo scorso anno



Fonte: IDSA Alliance

Utenti e Password

L’utente è l’anello debole

Ma forse non è tutta colpa sua!

E i colleghi dell'Help Desk?

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

Password e violazioni

Password	Time to Crack	Utilizzo
123456	<1 second	3.018.050
123456789	<1 second	1.625.135
12345678	<1 second	884.740
password	<1 second	692.151
qwerty123	<1 second	642.638
qwerty1	<1 second	583.630
111111	<1 second	459,730
12345	<1 second	395.573
secret	<1 second	363.491
123123	<1 second	351.576

Fonte NordVPN

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Dove le password hanno fallito

NIST Guideline 2024

- Attivare Show Password
- Utilizzare Password Manager
- Usare Hashing per lo store delle password
- Anti Brute Force Policy
- 2FA – MFA
- Politica di cambio password (!)
  - Non cambiare spesso le password
  - Riduzione dell'importanza della complessità
  - Monitoraggio delle password Dictionary
  - No Password Hint
  - Utilizzare Passphrase

Perché affidarsi alle sole password può essere pericoloso:

- L'utilizzo da parte di un attaccante di una password non è controllabile
- Password utilizzate più volte
- Le politiche di sicurezza password portano ad una gestione poco sicura
- Password usate per scopi privati e lavorativi

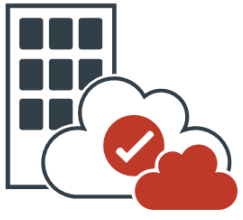
MFA non è più opzionale

Perché MFA è Necessaria

- 88% dei Data Breach passano da password rubate o poco sicure
- Gli utenti aziendali riutilizzano la stessa password in media 13 volte per applicazioni differenti
- Un attaccante può violare una password standard in meno di due ore

Vantaggi delle politiche di MFA

- Rischio di compromissione dell'account ridotto di circa il 99,9%
- Aggiunta di un livello di sicurezza (Qualcosa che conosco, Qualcosa che ho, Qualcosa che sono)
- Integrazione nativa con i sistemi



Hybrid Work

Adoption of more cloud applications

Increase in 3rd party relationships

Additional mobile devices & machine identities

RSA Unified Identity Platform

Workforce — External — Customer — Non Human

Automated Identity Intelligence

Authentication | Access & SSO | Governance & Lifecycle

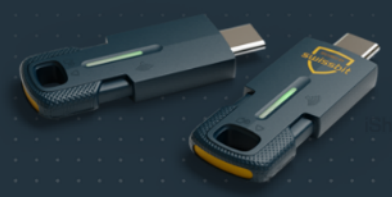
RSA Ecosystem

On-Premises — Hybrid — Multi-Cloud

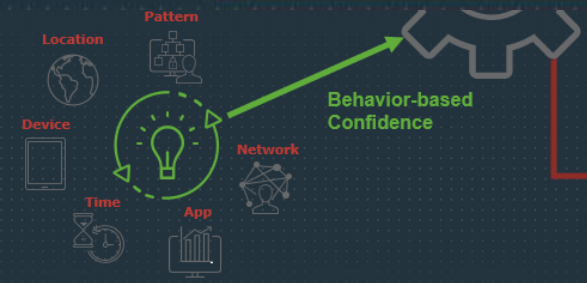
Security-First

Mobile Lock

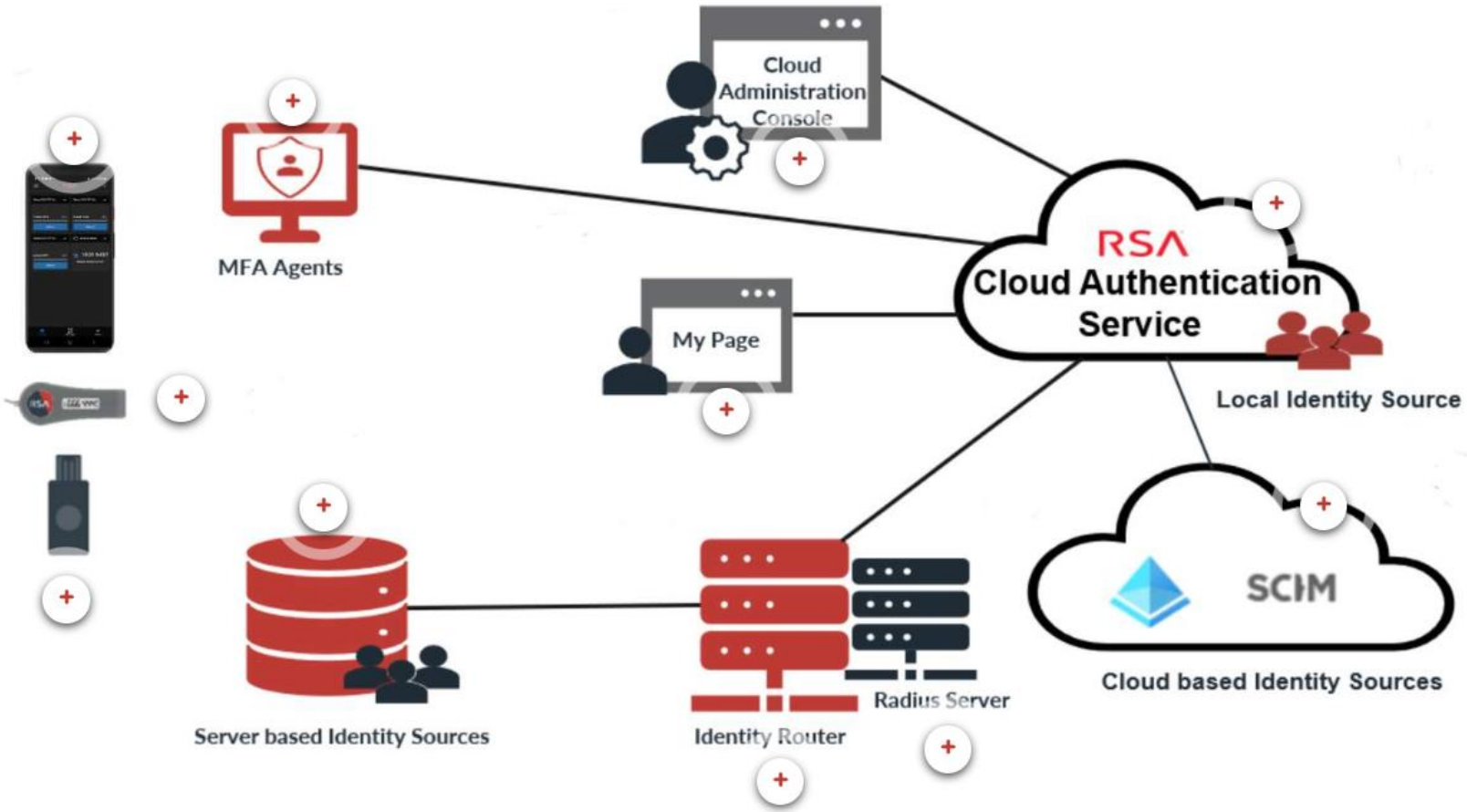
Passwordless multi-use authenticator: FIDO passkey (device-bound), OTP, and PIV smartcard



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



Sistemi Cloud – On Prem – Ibridi



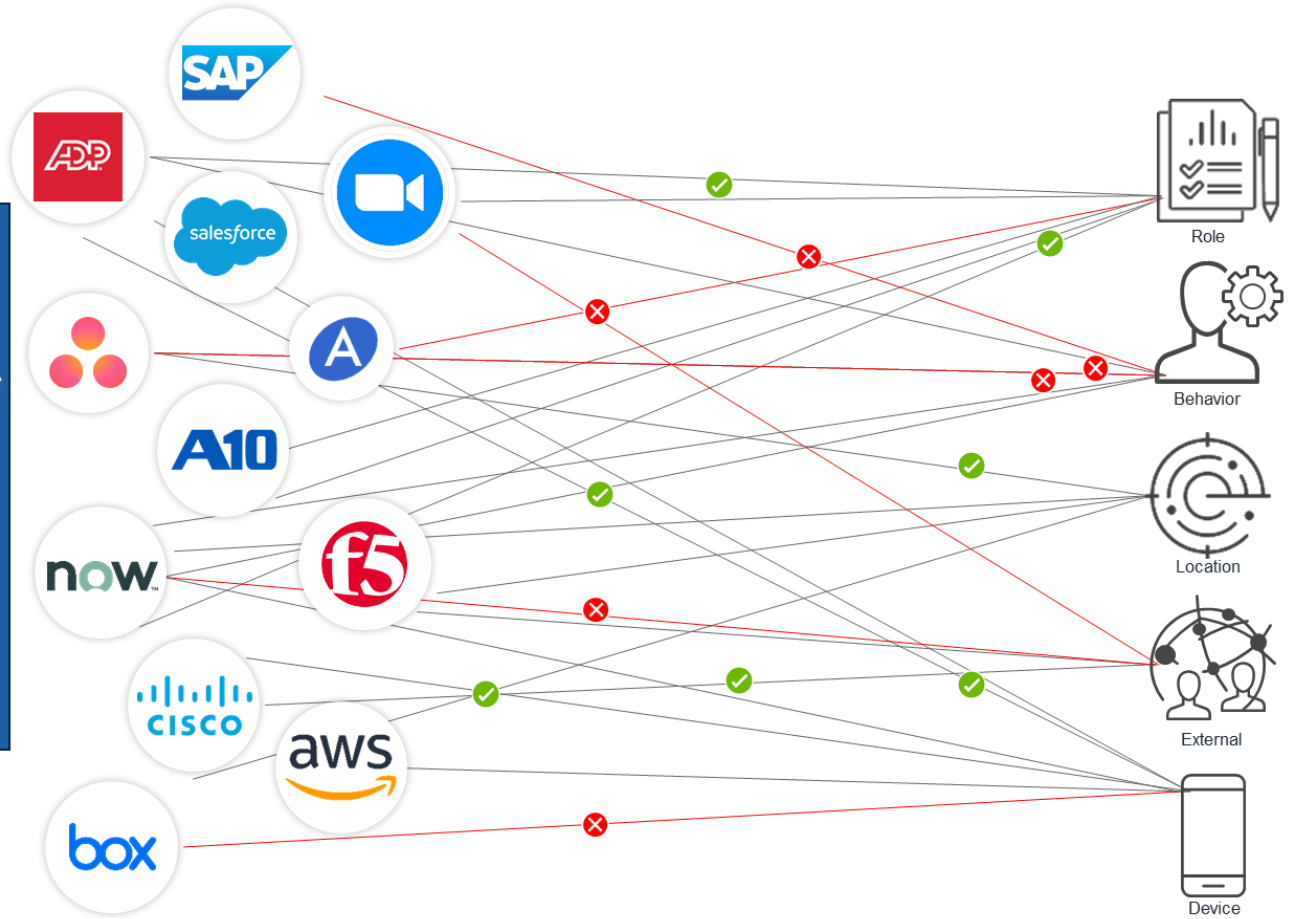
La sfida di un mondo che cresce

Forrester:

"Large organizations (20k+ employees) use

367 software apps and systems,

on average"



Admins are wasting time trying to secure the *unknown!*

La soluzione: Risk AI

- Simplifies policy management with dynamic risk-based decisions.
- Increases identity confidence through continuous learning and real-time risk scoring.
- Enhances security by adapting to changing threat landscapes.
- Reduces administrative overhead by automating complex access decisions.
- Provides transparency and control with explainable AI.

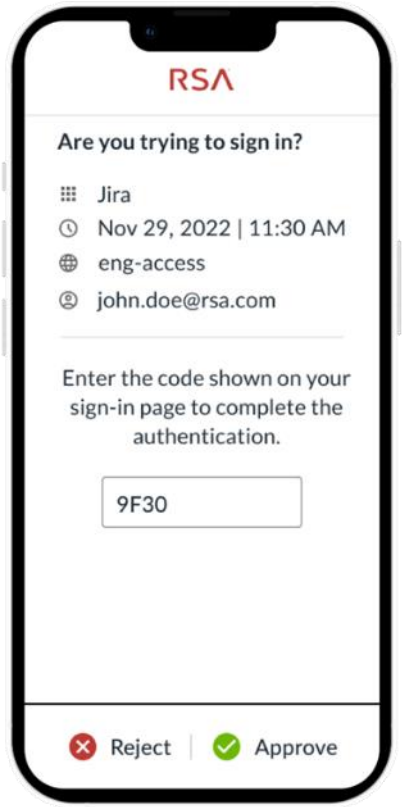
Sfida dei dispositivi MFA Mobili

Users are **reluctant to install Corporate Security Solutions** on their personal devices.

Mobile Devices are **vulnerable to multiple types of attacks** such as Malware and Spyware.

Fragmentation of the Android OS ecosystem makes it **more difficult to secure.**

Soluzioni per ogni utilizzo



RSA Authenticator App

GET IT ON Google Play

Download on the App Store

DS100 & iShield Key 2 Series

FIDO2 Certified, OTP & Phishing Resistant

Mobile Lock

Anomalous Behavior

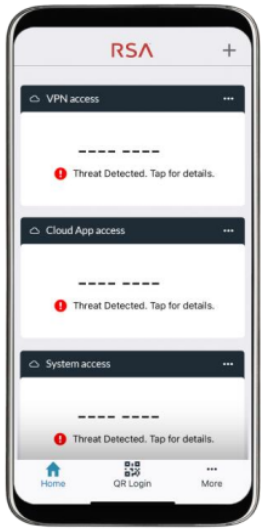
Identifies a critical threat

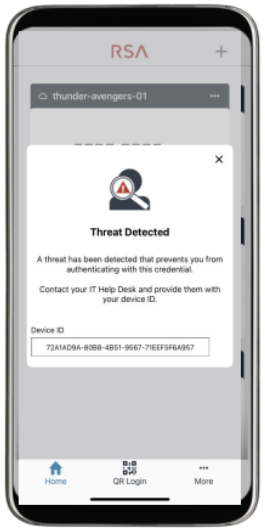
RSA Mobile Authentication Restricted

Informs user about the threat on their mobile authenticator app; Organization informed about the threat

Reduced Window for Threat Actors

Maintain security of business systems and data

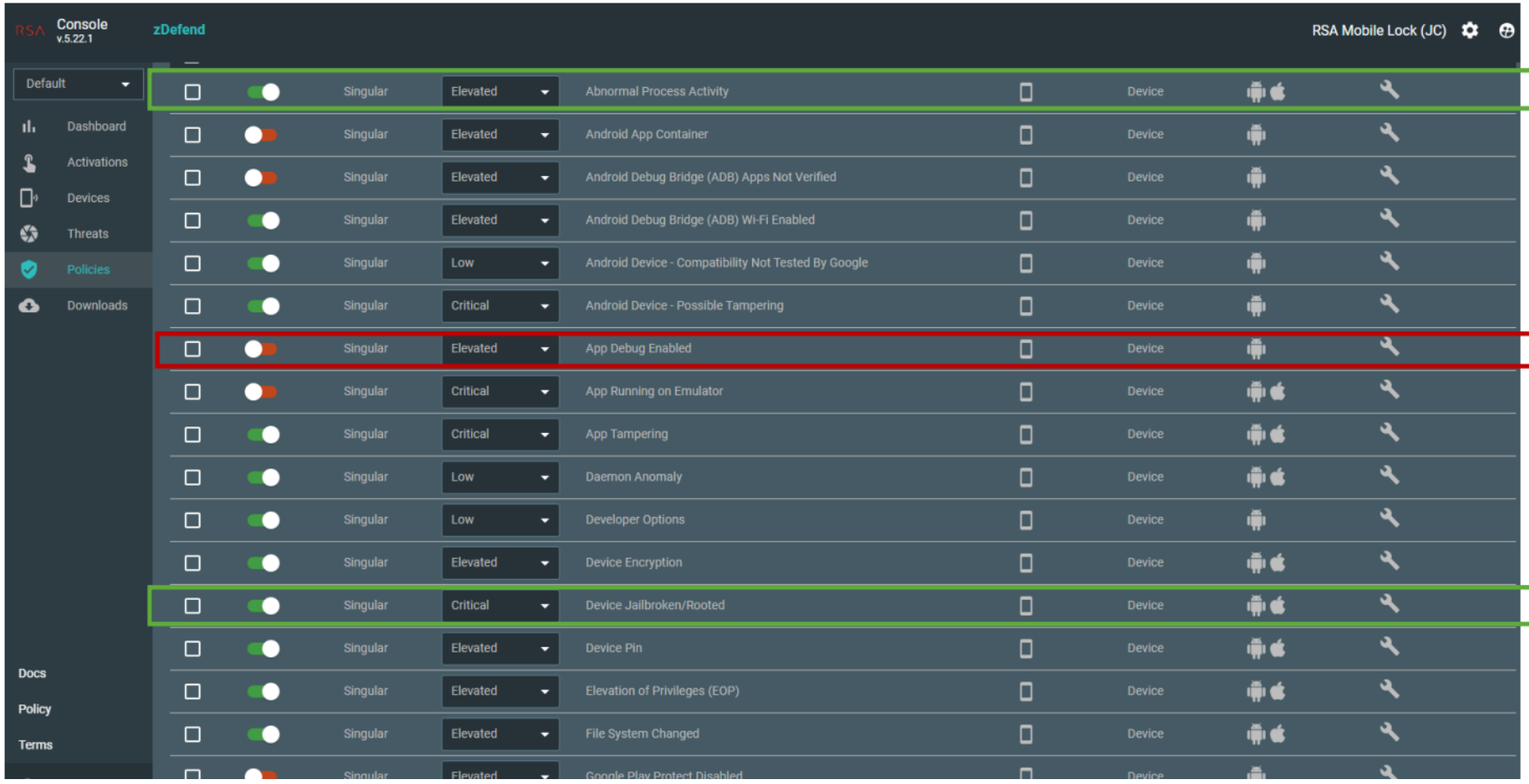




Benefits and Features

- ✓ Establish trust in mobile authenticator, no separate installation required.
- ✓ Restrict authentication to protect resources.
- ✓ Leave other device functions unaffected.
- ✓ Prevent threats from spreading during investigations.

Mobile Lock – Admin Console



Threat enabled for Detection & Reporting In Console, No impact on end users

Threat Disabled: No Detection, no reporting, No impact on end users

Threat Enabled and Classified: **"Critical": Detection and Reporting In Console, Block Authentication when Detected**

Destinazione Passwordless

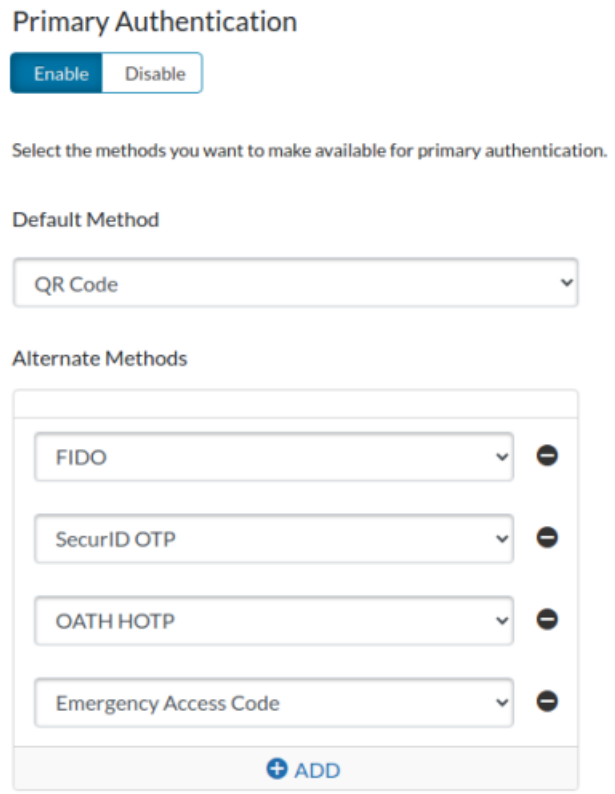
L’obiettivo è di un mondo IT non dipendente dalle password

Ad oggi si usa MFA come doppia autenticazione di una password

Con Passwordless:
- Facilità di uso
- Nessuna password porta l’utente ad essere meno attaccabile sull’identità
- Basata su MFA

Il Passwordless deve essere l’obiettivo a cui arrivare e deve essere usata nel quotidiano

RSA offre il miglior modo per iniziare il percorso con varie possibilità di MFA
- (PIN+) OTP (Device + PIN)
- QR Codes (Device + Biometrics)
- OATH HOTP (Device + PIN)
- FIDO (Device + PIN)



Perchè i servizi di autenticazione gestita

Accresci il tuo personale

Raccogli più sfide, distibuisci in maniera più efficiente e veloce, e fatti trovare pronto a competere in un mercato più importante senza incidere sui tuoi costi del personale

Aumenta il portfoglio di prodotti e soluzioni

Accresci in maniera rapida la tua offerta con un accesso veloce ai nostril servizi e fatti trovare pronto per le sfide di domani.

Accresci la tua profittabilità

Crea un nuovo modello di business concentrandoti sui servizi e non sulla sola vendita di prodotti, fidelizza il cliente e fornisci supporto di ottimo livello

Un unico partner

Crea maggiore efficienza scegliendo e consolidando le tue relazioni con un Service Provider di comprovata esperienza a livello globale.

I nostri servizi sono pensati per accrescere la fiducia di canale

TD SYNNEX

“Hackers don’t brake in, they log in”

https://www.rsa.com/
https://community.rsa.com/s/education-services
https://github.coventry.ac.uk/pages/CUEH/245CT/1_Introduction/SecurityConcepts_Pillars/
https://nis2directive.eu/
https://www.ibm.com/reports/data-breach
https://www.beyondtrust.com/blog/entry/the-state-of-identity-...
https://www.idsalliance.org/white-paper/2024-trends-in-securing-digital-identities/
https://nordpass.com/most-common-passwords-list/
https://www.linkedin.com/pulse/why-multi-factor-authentication-longer-optional-businesses-2024-uwulc/
https://pages.nist.gov/800-63-3/sp800-63-3.html
https://www.auditboard.com/blog/nist-password-guidelines/
https://fidoalliance.org/

TD SYNNEX

Q&A

Your Opinion Counts!

PROSSIMI APPUNTAMENTI

17 GENNAIO: Road to Win10 EOS

https://events.tdsynnex.it/cyber-unit-missione-protezione/

https://forms.office.com/r/B8pN50j9f3

TEAM SECURITY: security.it@tdsynnex.com
SPEAKERS: andrea.pezzoni@tdsynnex.com
roberto.branz@rsa.com +393316453193