RSA

OWN YOUR IDENTITY.

Identity & AI Wave.

RSA Unified Identity Platform

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

Agenda

SECURITY SUMMIT 2023

- **Identity and major security concerns**
- **Why some tough GAPs**
- **IT Waves we see in the future**
- **The importance of a Unified Identity Platform**
  - How its foundational DNA should look like

Some Analysts sources and last updated Identity Risk Picture

- World Economic Forum Report
  - [Source: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf]
  - [Published on 18-Jan-2023 in collaboration with Accenture]

- Verizon 2022 Data Breach Investigations Report
  - [Source: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf]
  - [It's the 15th annual Verizon Data Breach Investigations Report with 23,896 security incidents analyzed, of which, 5,212 were confirmed data breaches]

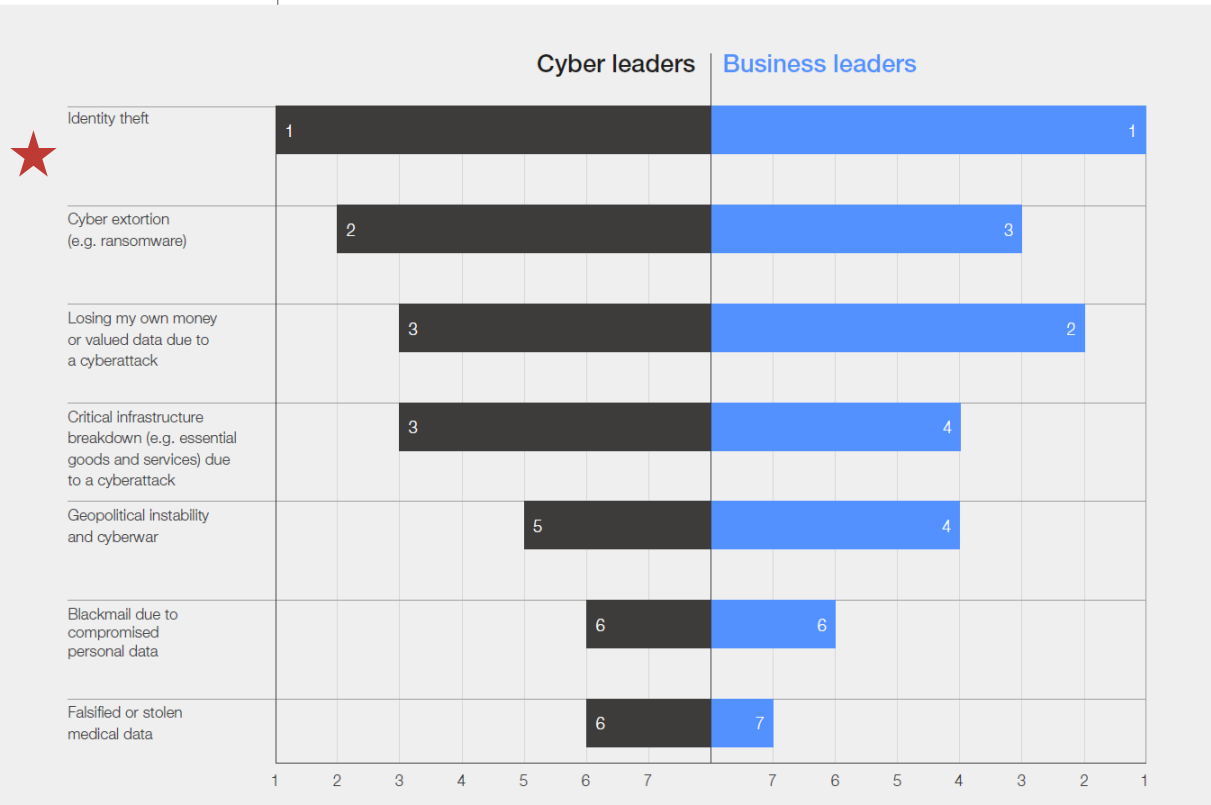
- Gartner Identifies Top Security and Risk Management Trends for 2022
  - [Source: https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022]
  - [Published on 7-Mar-2022]

- KuppingerCole 2022 Identity Governance and Administration Leadership Compass
  - [Source: https://www.rsa.com/resources/reports/kuppingercole-leadership-compass-identity-governance-and-administration/]
  - [Published on 25-Nov-2022]

Most concerning cyber risk

- "What cyber risk are you most concerned about"
  - [Source: "World Economic Forum Report" – Pag. 27 - https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf]
  - [Source: "Cost of a Data Breach Report 2022" – Pag.17 - https://www.ibm.com/downloads/cas/3R8N1DZJ

FIGURE 20 What cyber risk are you most concerned about when it comes to your personal cybersecurity?



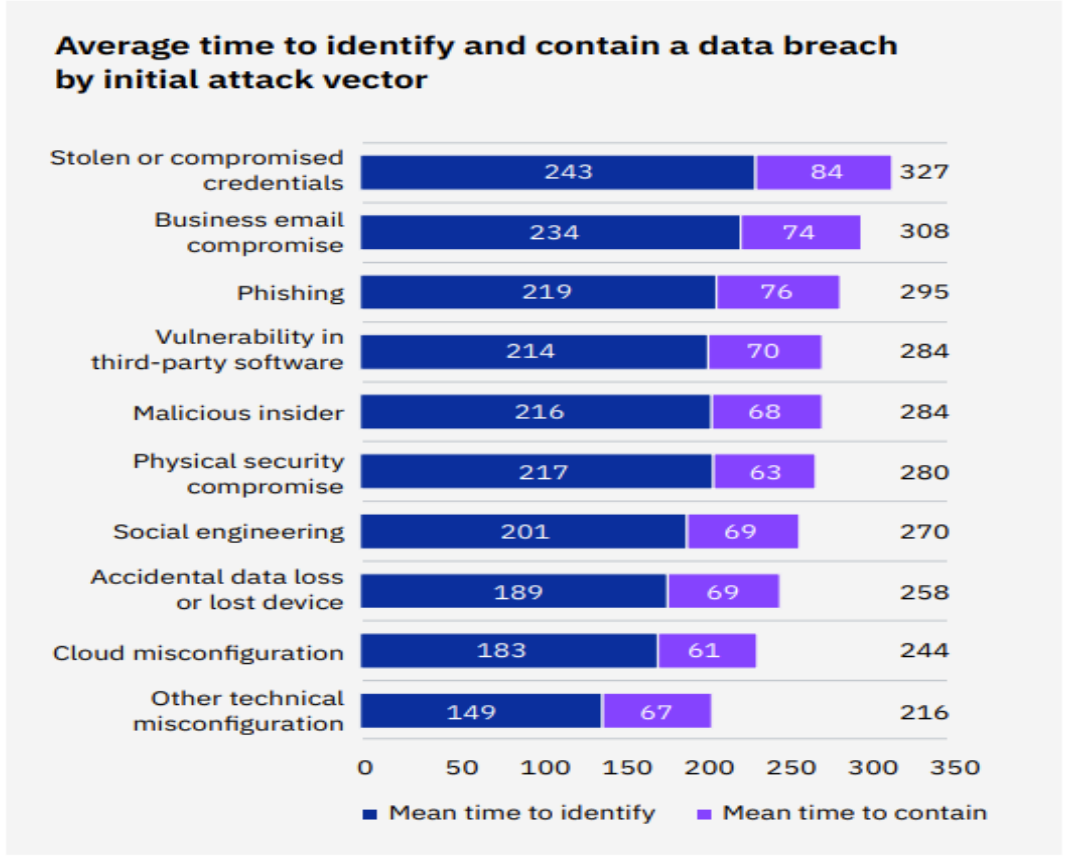


Figure 12: Measured in days

Most concerning cyber risk

- “The human element continues to drive breaches. This year 82% of breaches involved the human element”
- “It’s important to remember, Ransomware by itself is really just a model of monetizing an organization’s access”
  - [Source: ”Verizon 2022 Data Breach Investigations Report” – Pag. 7,8 - https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf]

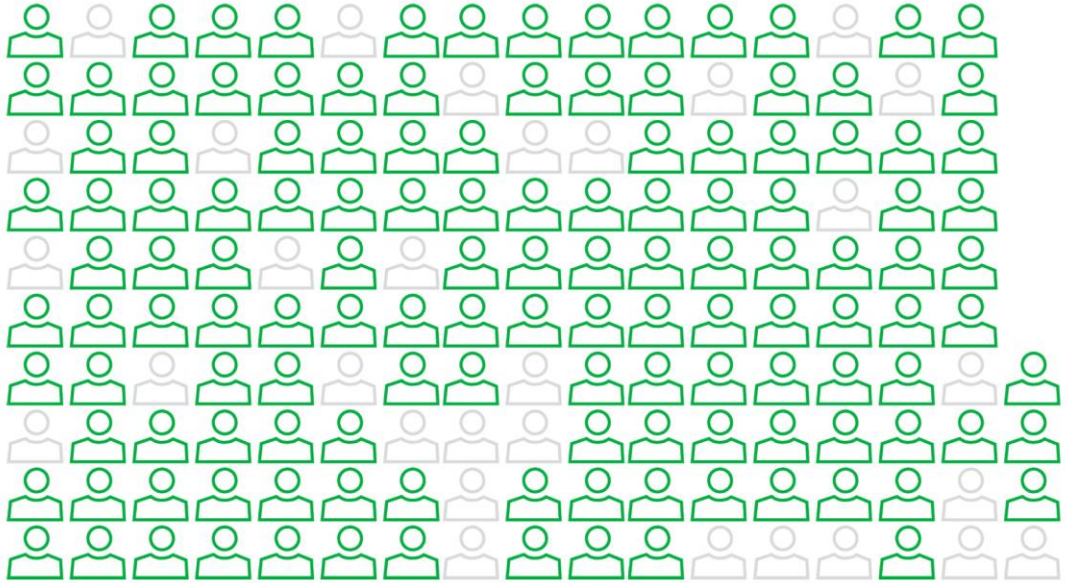


Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.

Please consider that there are four key paths leading

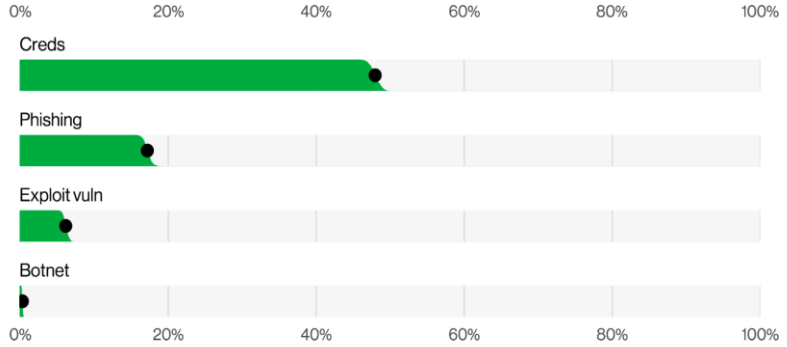


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

Internet without Identity Layer

Basically, Internet was built without a way to know who and what you are connecting to!!!!

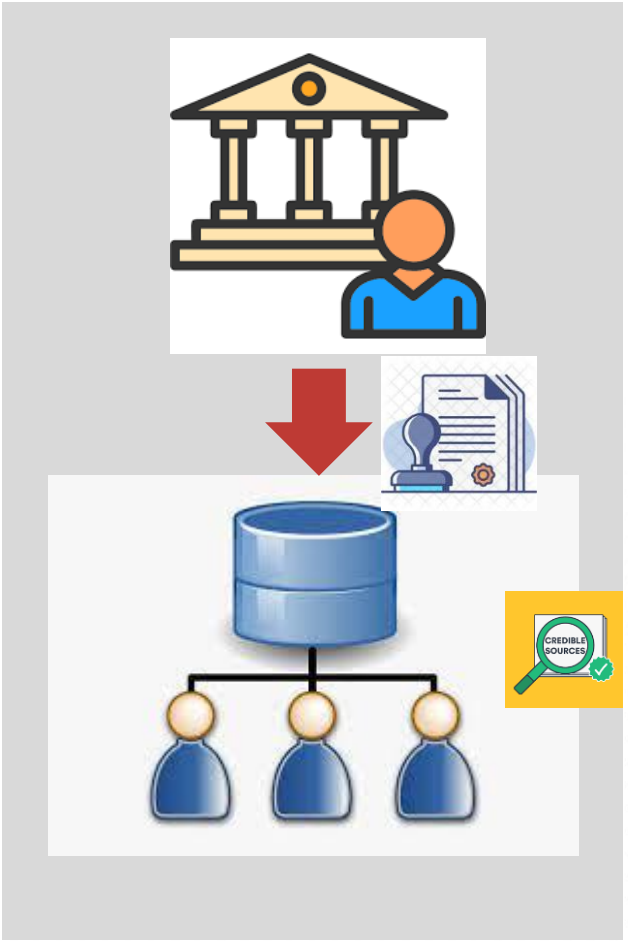
With the TCP/IP networking protocol you might only know the address of the machine you are connecting to.

IDENTITY FRAMEWORK

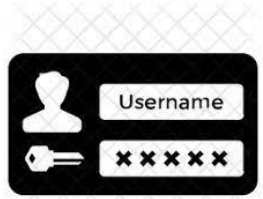
You know nothing about the person or the organization or the thing behind that specific machine

Evolution of Identity: from Centralized Model to…

Centralized Identity Model is a system in which a single authority or organization is responsible for managing and verifying user identities.



Provide a convenient and efficient way to manage user identities



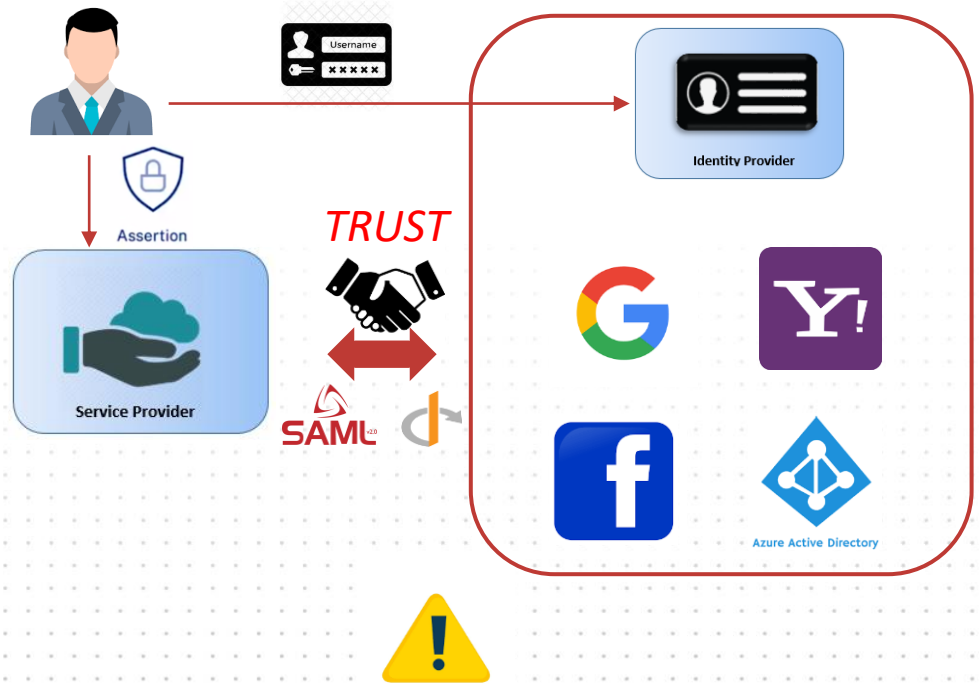
Single point of failure

If a centralized identity system is compromised, the personal information of all users could be at risk

It may be vulnerable to abuse by governments or other entities that seek to use user data for surveillance or other purposes

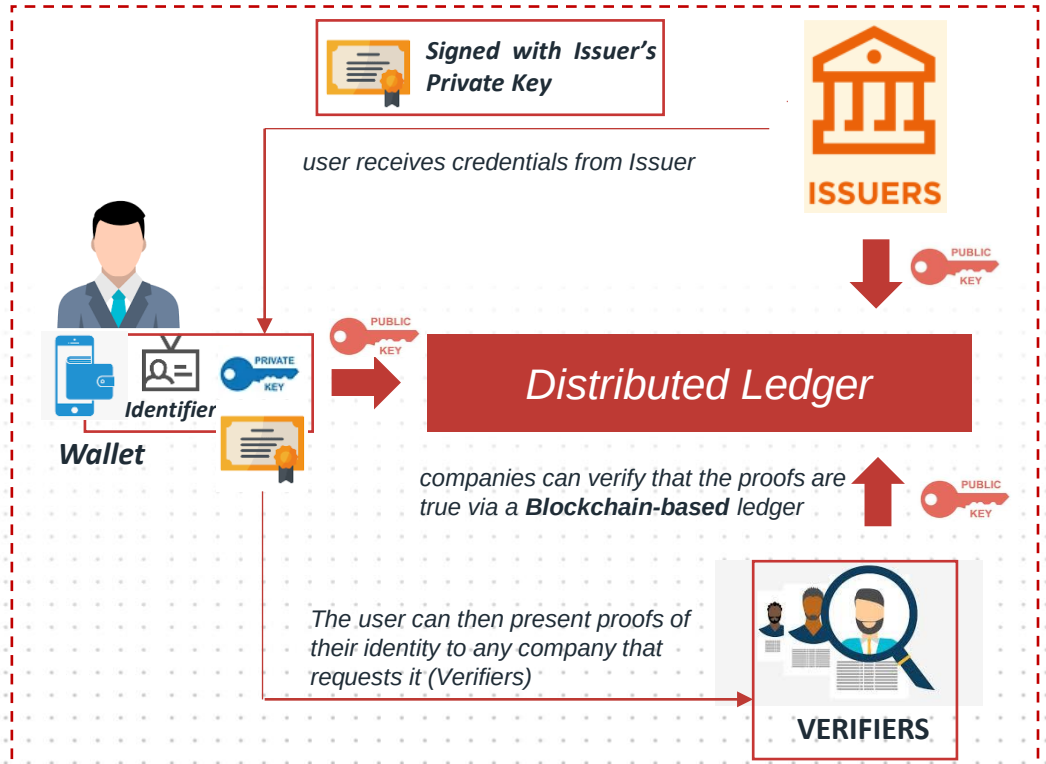
Identity Model: Federated and Decentralized

Federated Identity Model is a system in which multiple organizations (**SP**) agree to trust each other's identity systems (**IDP**) and share user authentication and authorization information.



Risks about the centralization of power and potential privacy and data protection violations

Decentralized Identity Model is a system in which users control their own identity information and can choose to share it with trusted parties as needed.



What identity model is the best?

P Best identity model

There is no one-size-fits-all answer to the question of the best identity model, as the appropriate model depends on the specific needs and risks of the application or system in question.

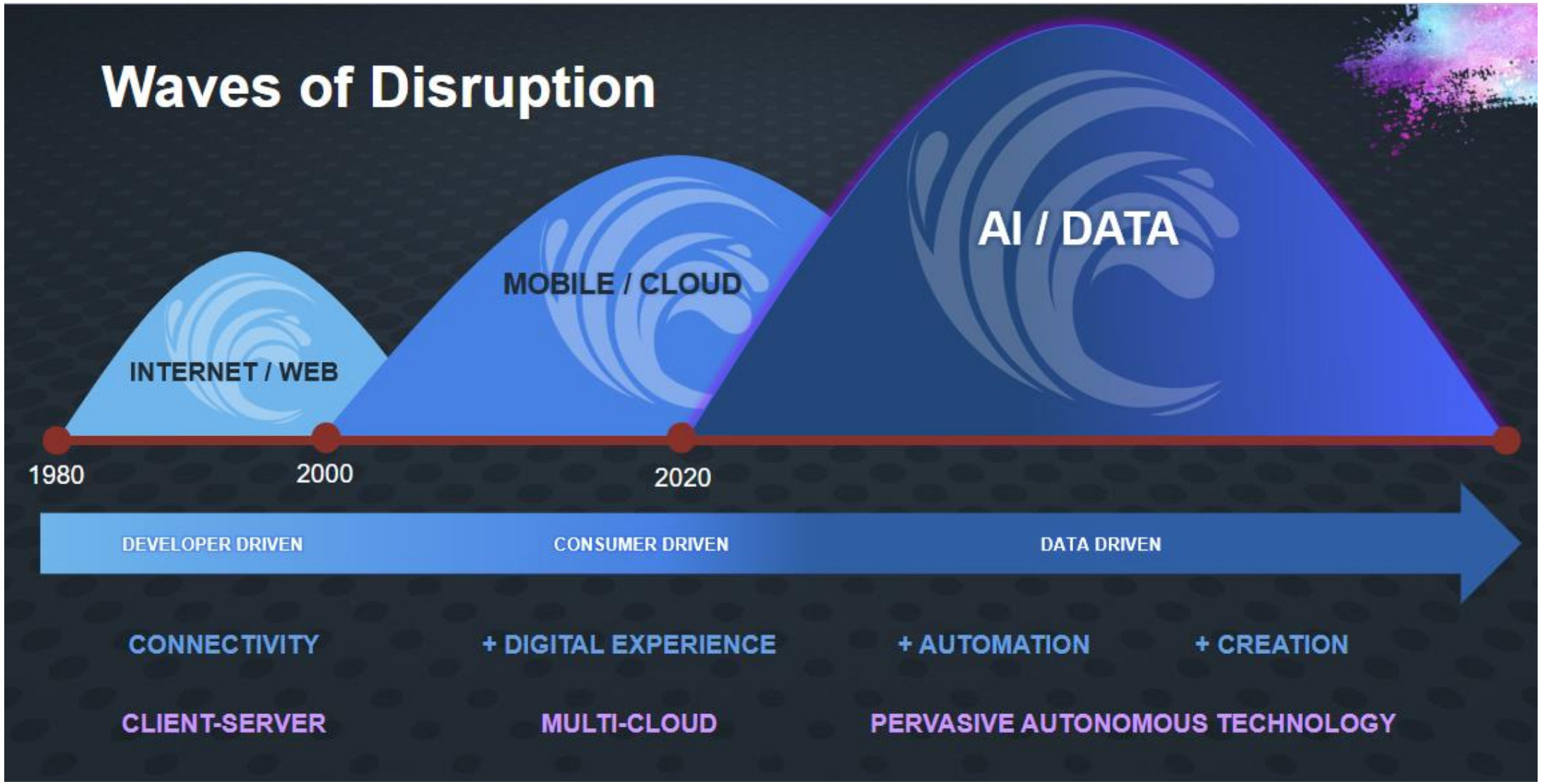
Centralized identity models offer convenience and efficiency in managing user identities, but they also raise concerns about privacy and security. If a centralized identity system is compromised, the personal information of all users could be at risk.

Federated identity models offer a compromise between convenience and security by allowing multiple organizations to trust each other's identity systems and share user authentication and authorization information. However, this model does rely on trust between the organizations involved, and there are concerns about the centralization of power and potential privacy violations.

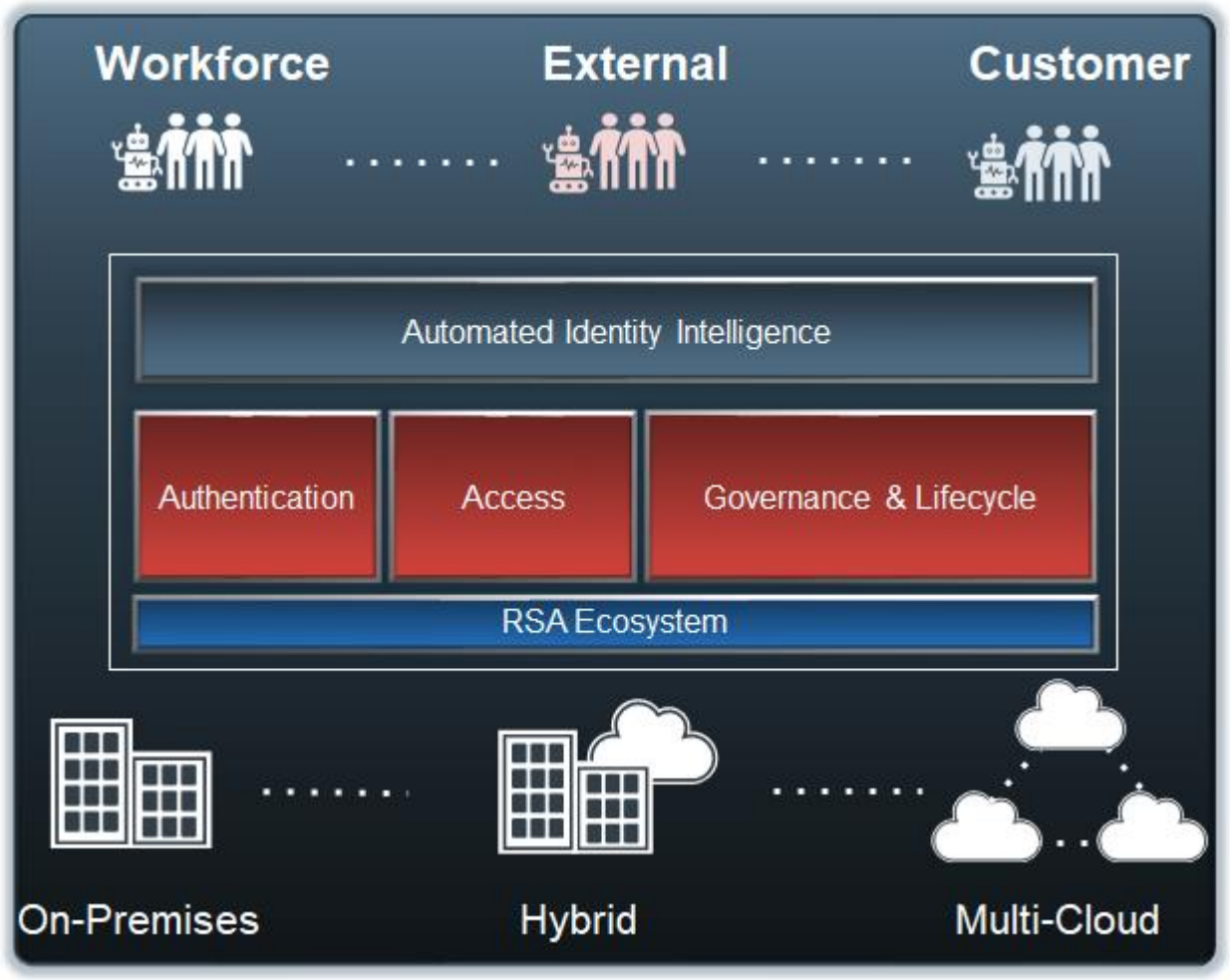
Decentralized identity models give users control over their own identity information and can be achieved using technologies such as blockchain and self-sovereign identity. This model gives users greater control over their privacy and security, but there may be more friction in establishing trust between parties and the user experience may be less convenient.

Ultimately, the best identity model depends on the specific needs and risks of the application or system. It is important to consider factors such as the level of security required, the importance of user privacy, the need for interoperability and convenience, and the potential risks and benefits of the chosen model.

Identity and Wave AI



RSA Unified Identity Platform

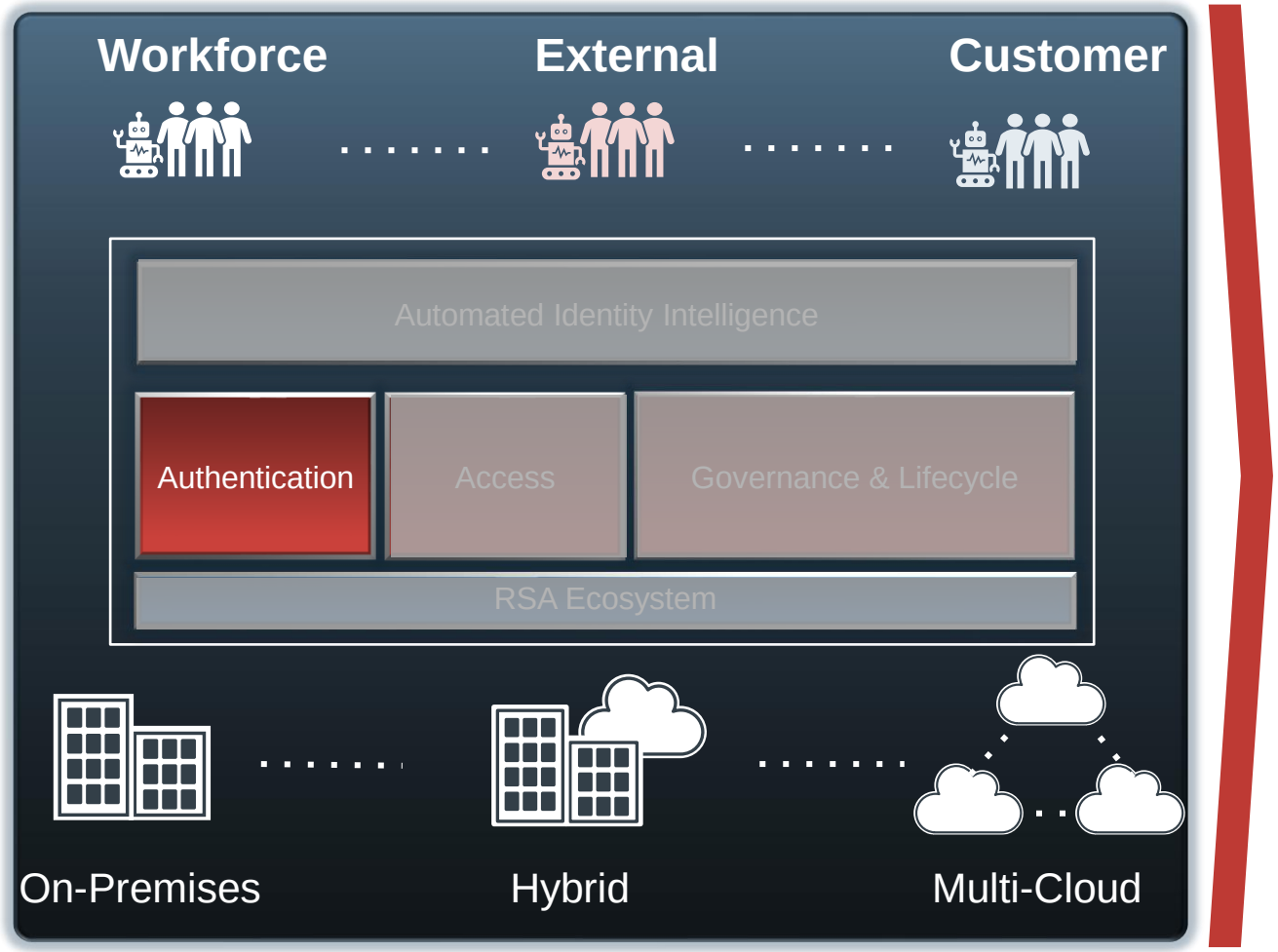


Security-First

Intelligent

Open

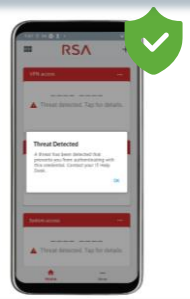
RSA Unified Identity Platform - Authentication



Modern MFA

- Approve
- Tokencode
- RSA SecurID
- Voice Call
- QRcode
- Fingerprint
- Face ID
- FIDO
- Wearables
- Text Message

Threat Detection

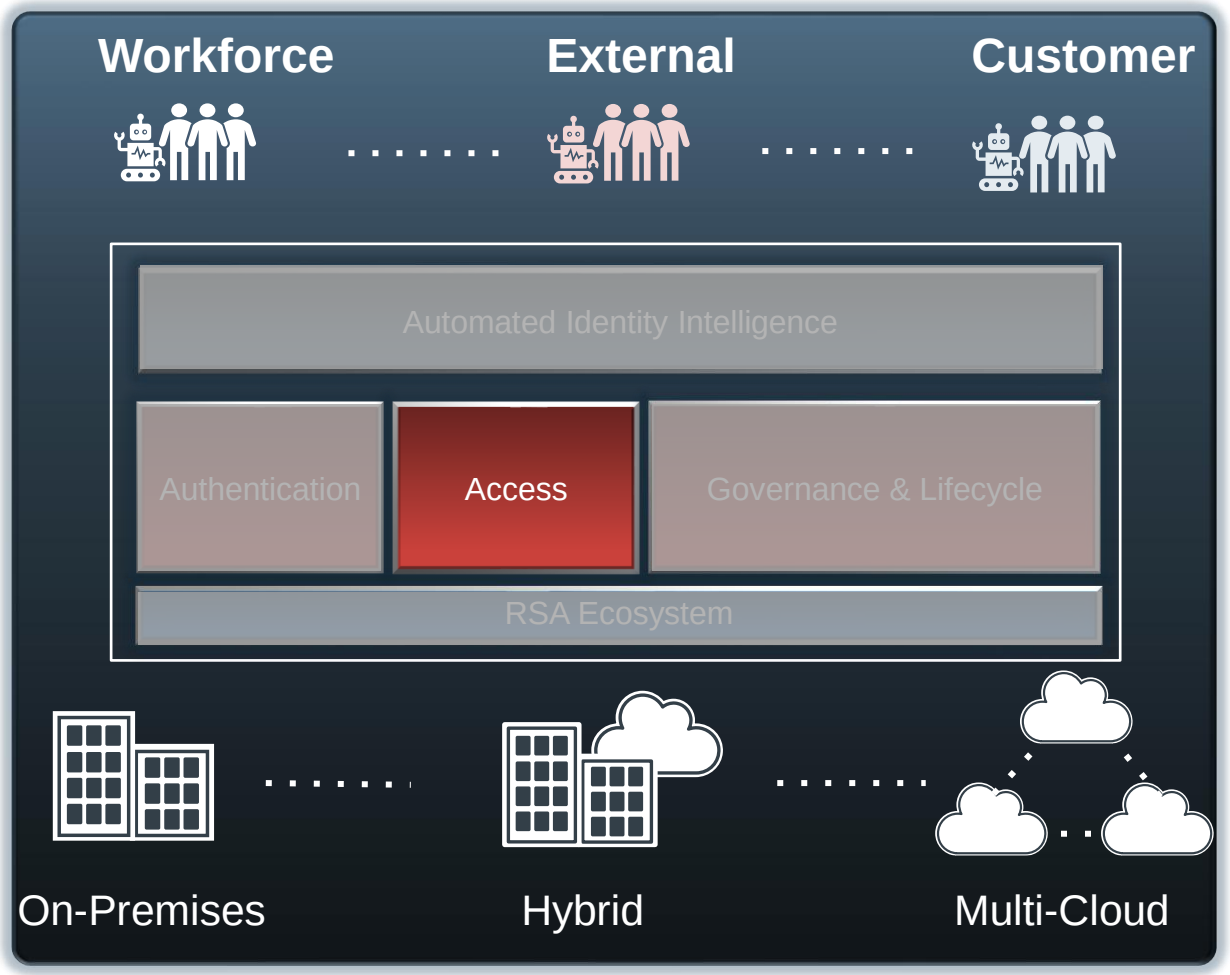


- Detect threats on mobile devices
- Establish trust in unmanaged mobile devices
- Restrict authentication to protect resources
- Leave other device functions unaffected

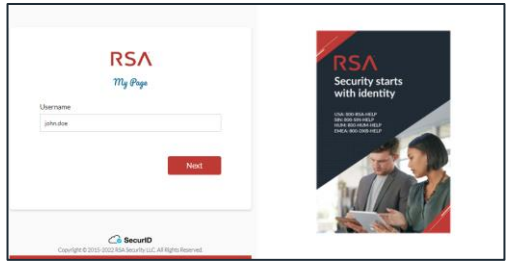
MFA Fatigue Attack

- To limit the number of MFA requests
- To choose the MFA method that works best

RSA Unified Identity Platform - Access

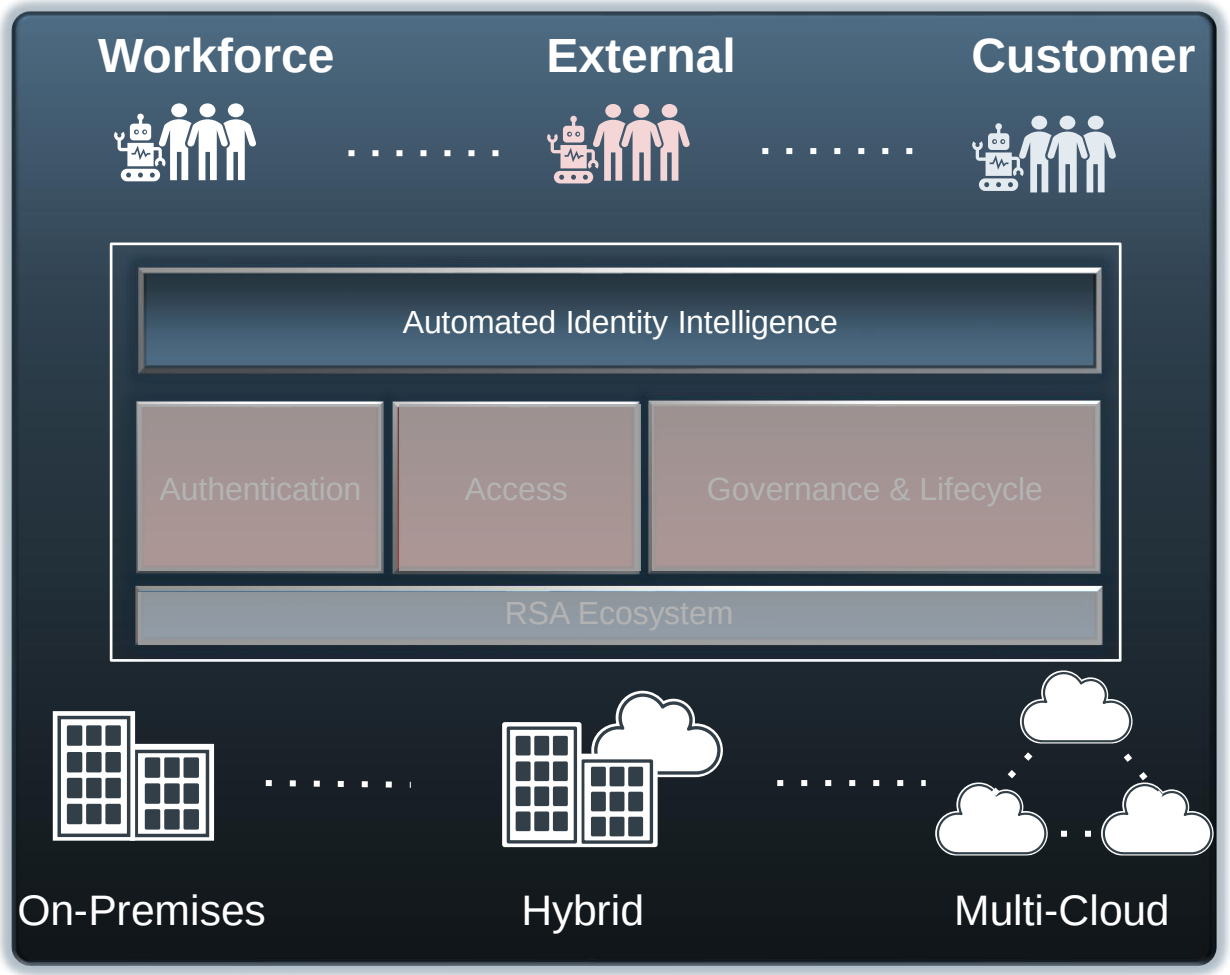


One Unified Experience – Off and On-site

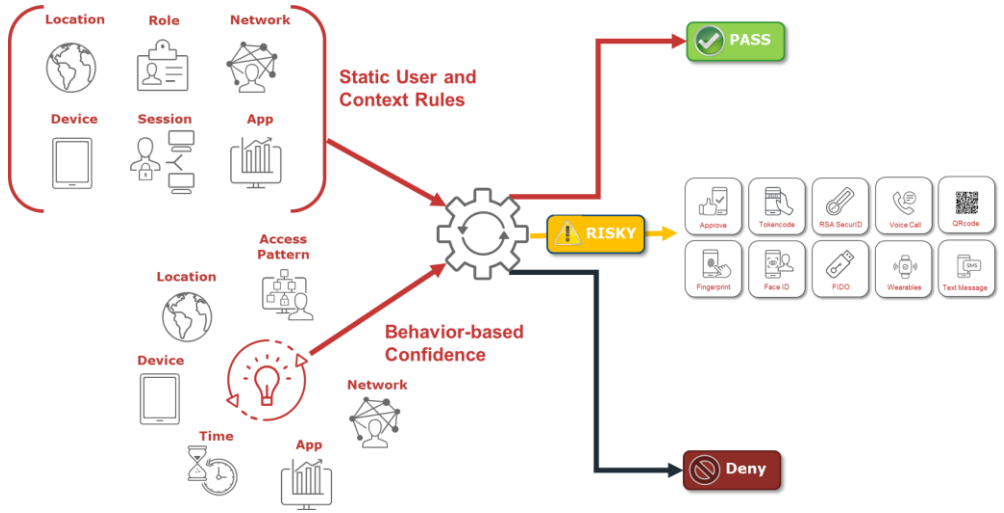


- **Self Service Device Management**
- **Single Sign On**
- **Password Management (Recovery, Reset, ecc.)**
- **Customizable**
- **Open (SAML, OIDC, SCIM. ecc.)**

RSA Unified Identity Platform – AI

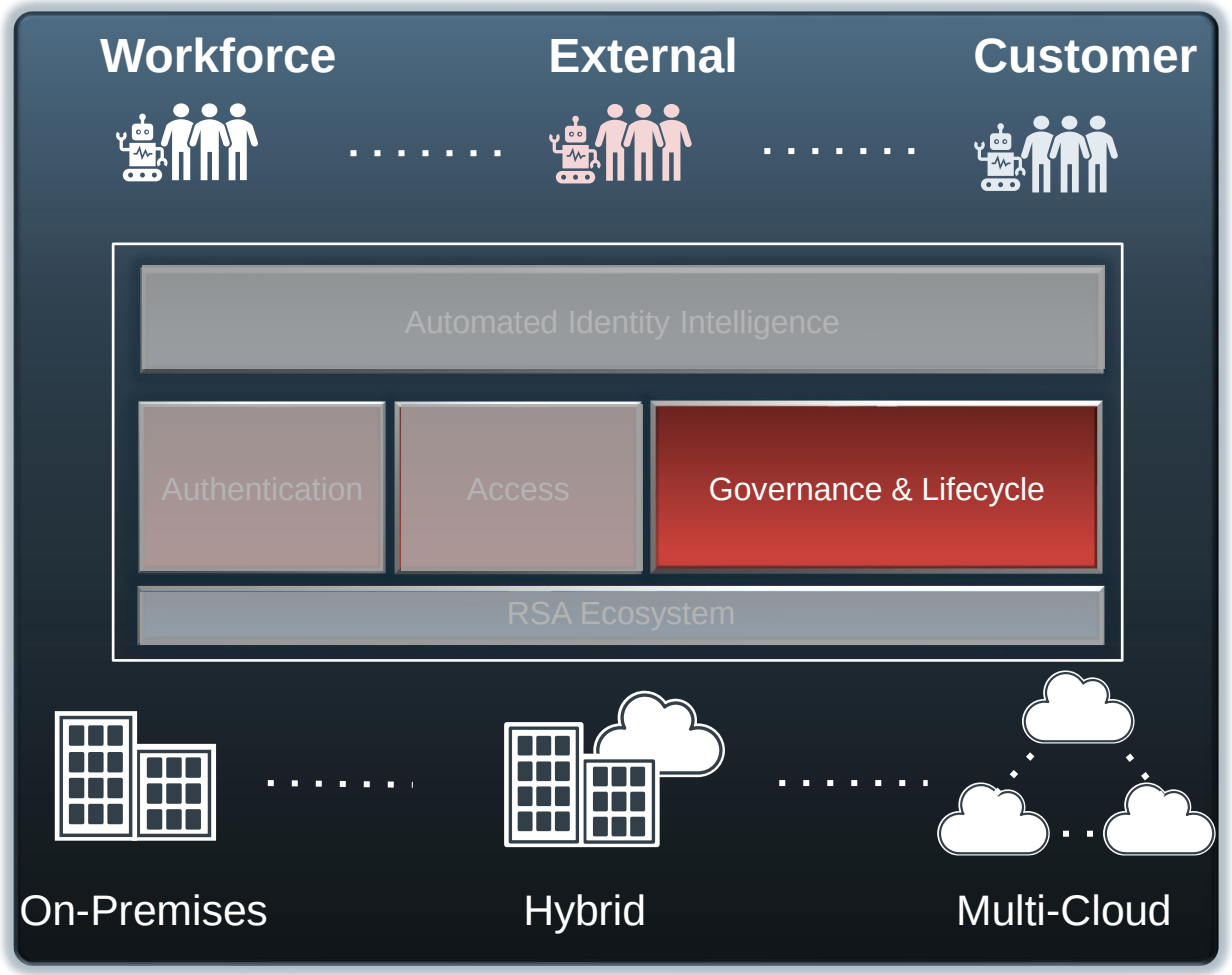


AI RISK ENGINE



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

RSA Unified Identity Platform – G&L



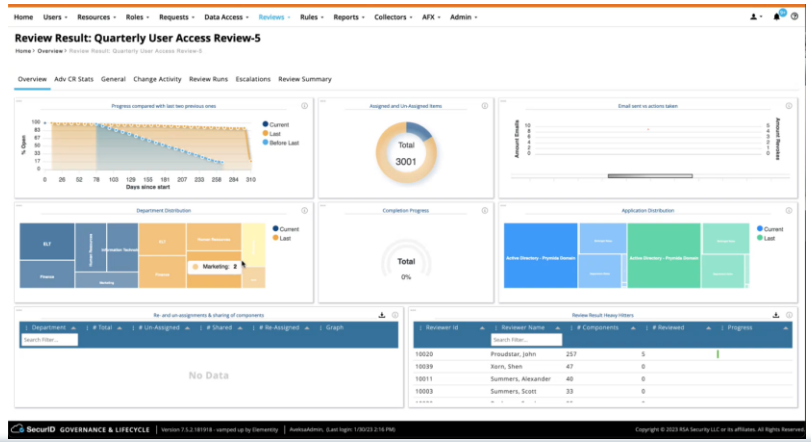
Reduce Identity Risks - Evolving Workforce

Identity Governance

Act with insight to prioritize access decisions (access visibility, compliance, SoD, Orphan Accounts)

Identity Lifecycle

Ensure users have timely access to the right applications (JML automated provisioning)



To Wrap Up…

- We know there are valid reasons why proper end-to-end Identity Management is a tough Business and Security Challenge

- Complexity and missing gaps (remind that we miss an Identity layer over Internet) simply make Identity the most consequential Attack Vector and the main Analysts out there cruelly highlight highlight that

- That being noted, probably, Customers should also revise the prioritization of the security controls that are going to mitigate Risks and focus on the most impacting Threat Vectors if their probable frequency is high

- A solid and **Unified Identity Platform** focusing on a “Security-First” dna, “Augmented with AI” and “Open” to Standards for effective interoperability, will make to job in mitigating the most important Risks

OWN YOUR IDENTITY.

Thank You

RSA