

DORA, ChatGPT and the (many) others – How to cover your bases in a new wave of cyber risks?

Gábor HIRSCH

Regional Sales Manager – Data Security

Atila PAKSI

Regional Sales Manager – Identity & Access Management



7 Top Trends in Cybersecurity for 2022

01



Attack surface
expansion

02



Identity system
defense

03



Digital supply
chain risk

04



Vendor
consolidation

05



Cybersecurity
mesh

06



Distributed
decisions

07



Beyond
awareness

Source: Gartner, © 2022 Gartner, Inc.

- Announced: 27th of December, 2022.

- Take effect: 17th of October, 2024

- New “essential sectors” covered such as energy, transport, banking, health, digital infrastructure, public administration and space sectors

- The new rules will also protect so-called “important sectors” such as postal services, waste management, chemicals, food, manufacturing of medical devices, electronics, machinery, motor vehicles and digital providers. All medium-sized and large companies in selected sectors would fall under the legislation

- The requirements cover incident response, supply chain security, encryption and vulnerability disclosure, among other provisions (Paragraph 51 and 98 specifically mention encryption).

CER – Critical Entities Resilience

■ **Announced: 27th of December, 2022.**

■ **Take effect: 17th of October, 2024**

■ **Replace the European Critical Infrastructure Directive of 2008**

■ **Cover: Energy, Transport, Banking (together with DORA), Health, Drinking water, Waste water, Digital infrastructure, Public administration, Space**

■ **Goals:**

- Strengthen existing protection
- Connected to NIS2 Directive and DORA

DORA – Digital Operational Resilience Act

■ **Announced: 27th of December, 2022.**

■ **Take effect: 17th of January, 2025**

■ **Cover: practically all finance entities: banks, insurance companies, funds, etc. (exclude just a few, for example postal clearing houses)**

■ **Goals:**

- Standardization
- Cover 3rd party suppliers
- Connected to NIS2 Directive and CER
- Principle of proportionality

ICT risk management

- Practically not new only small changes

ICT incident handling and reporting

- Standard reporting to everywhere
- New, centralized reporting authority

Digital resilience testing

- A lot of tests: penetration test, code test, etc.
- TLPT: Threat Lead Penetration Test
 - Long, difficult and complex test with audit capabilities

3rd party ICT risk management

- Minimal requirements
- Similar like outsourcing or cloud regulations but „wider“

etc.

Proposal for a regulation on cybersecurity requirements for products with digital elements

Covers: practically all digital equipments

- Including Industrial Automation & Control Systems (IACS) intended for the use by essential entities such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);

Four specific objectives were set out:

1. Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;
2. Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
3. Enhance the transparency of security properties of products with digital elements, and
4. Enable businesses and consumers to use products with digital elements securely.

Protect transaction and personal data at rest

Encrypt financial and personal data in motion

Implement strong access control measures

Encryption still #1 choice to protect data



Of respondents said encryption was the top tool to secure data. Yet only **50%** say that **more than 40%** of their sensitive data has been encrypted – **a slight increase** in the 2021 survey, up from **46%**.

Protect Data in Motion: High Speed Encryptor Family

CV1000



- Hardened virtual appliance
- KeySecure integration
- Supports Transport Independent Mode (TIM)
- **Ideal for Software Defined Networks (SDN) and Server-to-Server communications**

CN4000 Series



- 10 Mbps-1 Gbps Ethernet Encryptor
- Certified, low-cost, high-performance
- **Small form factor ideal for remote locations**

Securing Data in Motion—High Speed Network Encryption

CN6000 Series



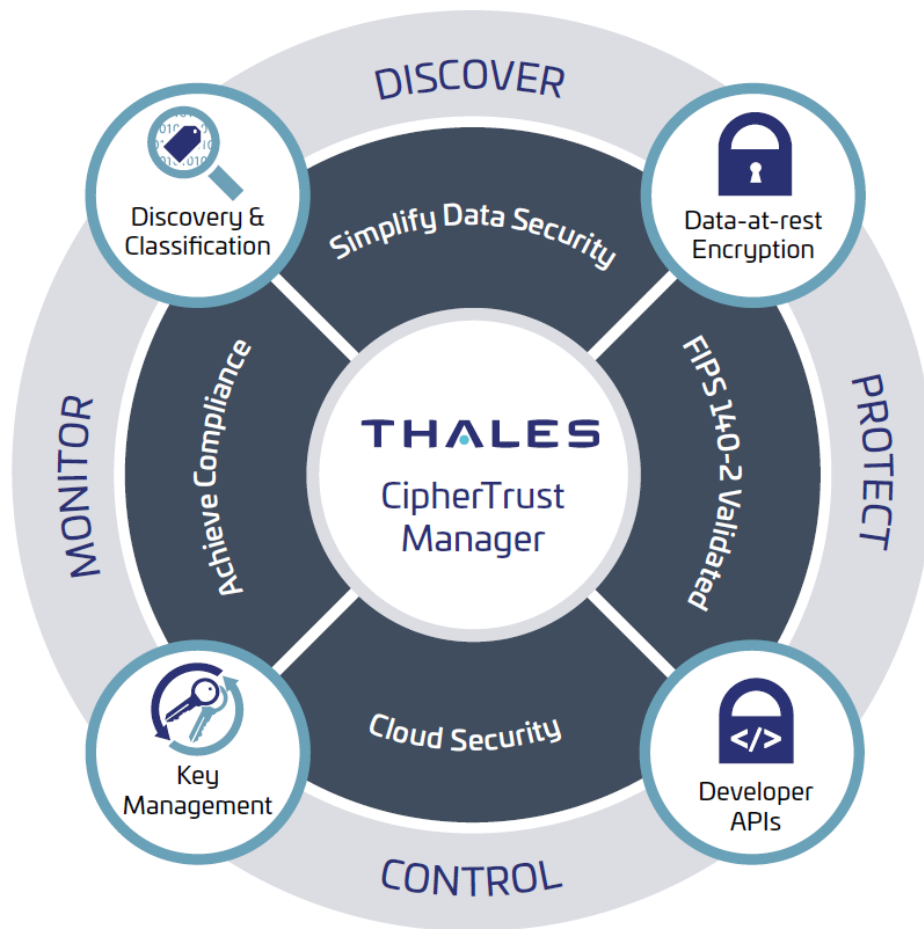
- 1 Gbps-10 Gbps Ethernet Encryptor
- Certified to highest commercial standards
- Rack-mountable, fully redundant robust design
- **Ideal for private networks and data center interconnects**

CN9000 Series

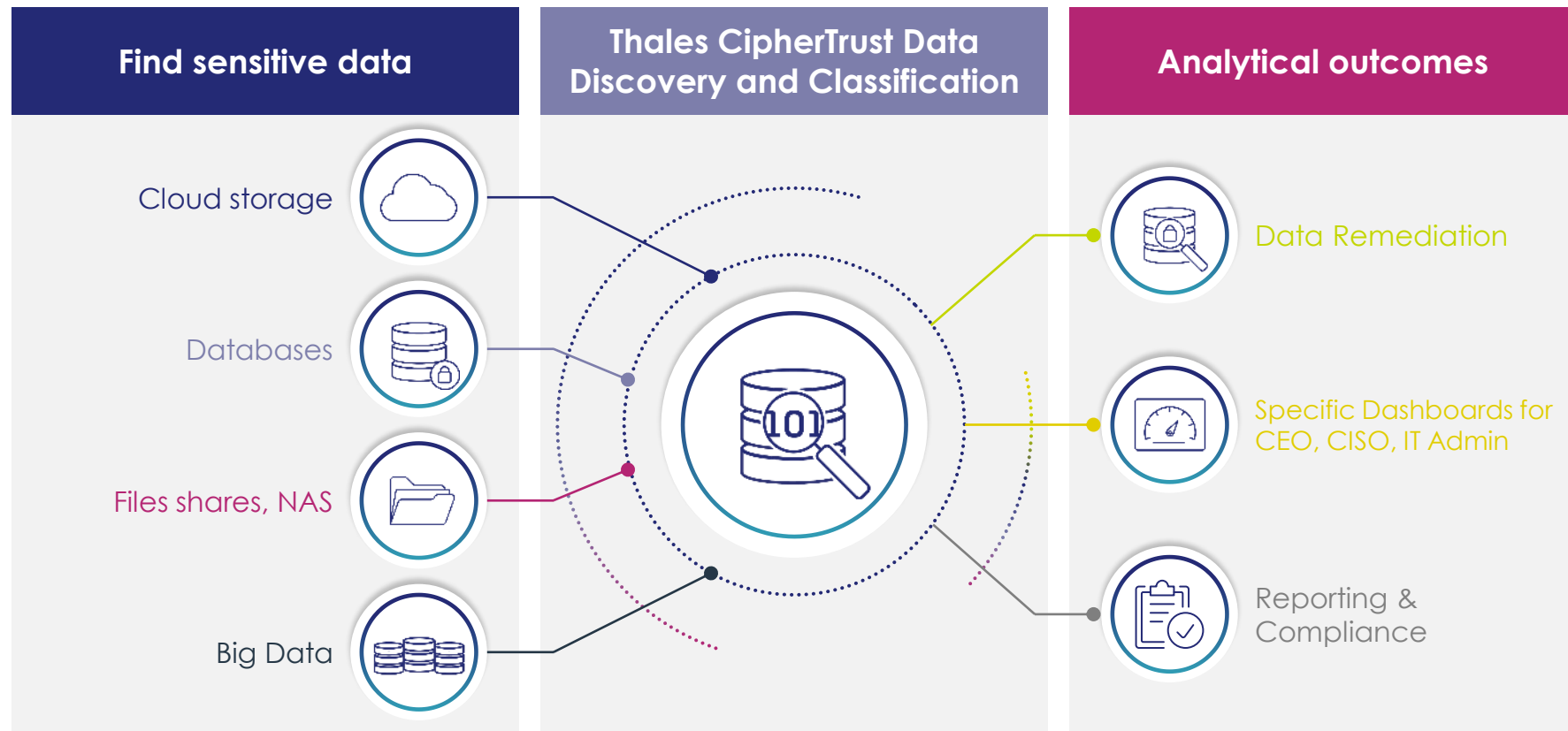


- First commercial certified 100 Gbps encryptors
- Only multipoint 100G Encryptor on market
- Fully interoperable with CN product family
- **Designed for next gen data centers and core networks**

Protect Data in Rest: CipherTrust Data Security Platform

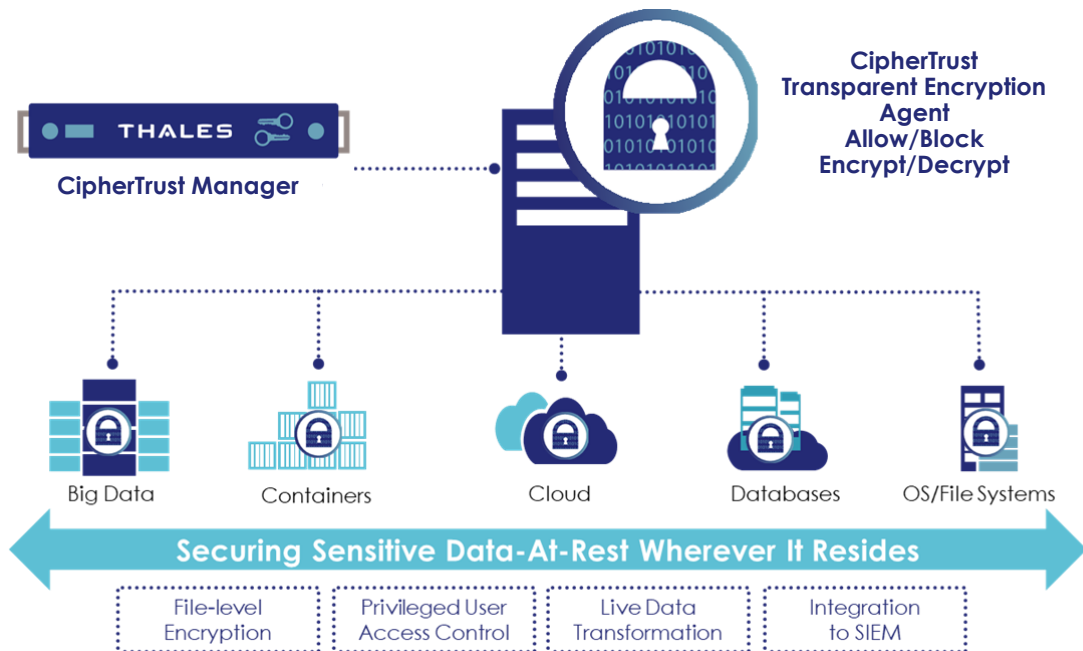


CipherTrust Data Discovery and Classification



CipherTrust Transparent Encryption (CTE)

Data-at-rest security wherever it resides



Meet needs for

- Compliance and regulation for encryption and access control
- Data breach prevention: 100+ countries with privacy laws – U.S. and Multinationals
- Protecting intellectual property, financial data, and sensitive information

Centralized control

- Physical / Virtual Data Centers
- Cloud / SaaS

CipherTrust Transparent Encryption (CTE)

Transparently protects file system, volume data-at-rest

CipherTrust Transparent Encryption Agent

Allow/Block Encrypt/Decrypt/report



Privileged Users

Encrypted & Controlled

*\$^!@#){
-|"_}?\$%-
:>>



Approved Users

Clear Text

John
Smith
401 Main
Street



Cloud Admin

Encrypted & Controlled

*\$^!@#){
-|"_}?\$%-
:>>



Transparent, file-level encryption

- For all databases and file types



Privileged user access controls

- Allows root users to do their job, without abusing data



Data access audit logging

- Accelerate threat detection and ease forensics



Centralized encryption key and data access policy management

- Streamline operations, reduce risk, satisfy compliance

Extensions and Additions to CTE



CTE Live Data Transformation

Zero-downtime deployment and seamless key rotation



CTE for Kubernetes

Policy-based encryption of data stored on persistent volume attached to a container application



CTE for SAP HANA

Encrypt SAP HANA data and logs to avoid unauthorized access



CTE for Efficient Storage

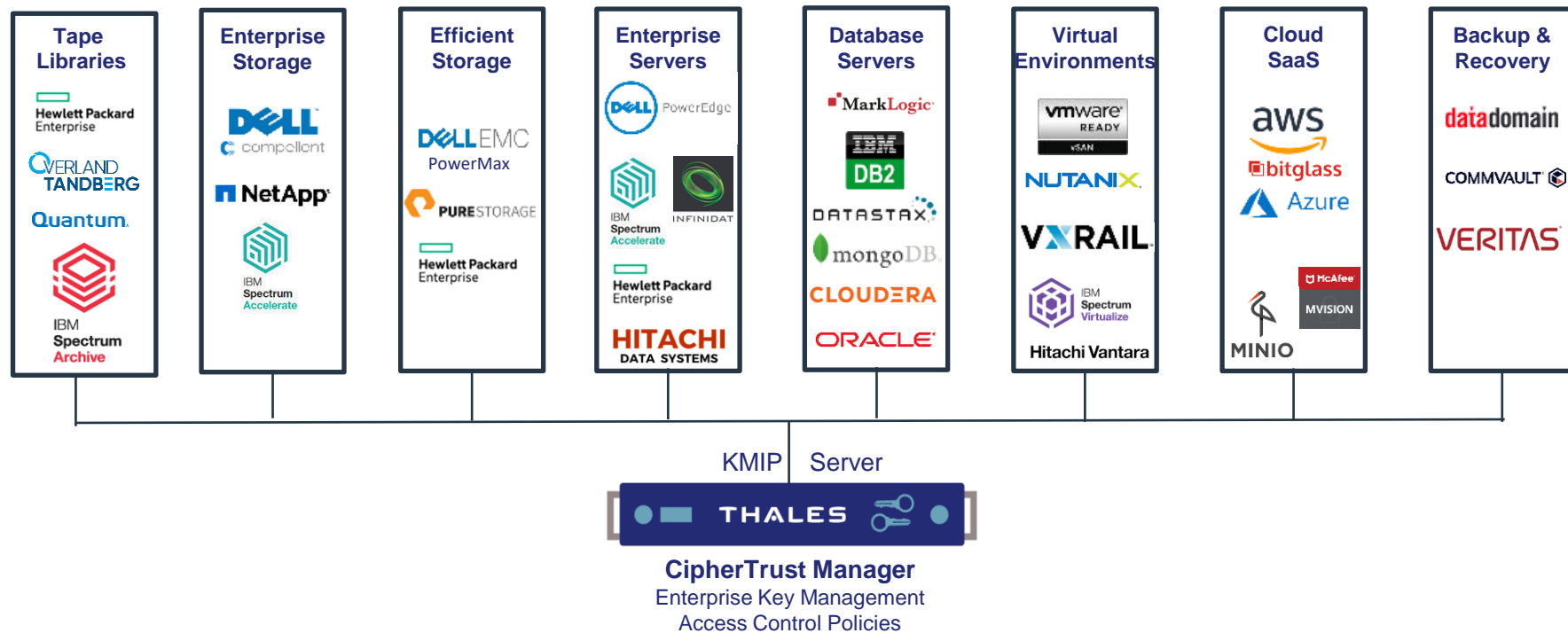
Best data protection possible while maintaining storage efficiency



CTE for Teradata

High-performance encryption solution for Teradata database

CipherTrust KMIP Integrations



Centralized Key Management



One or more
Private Clouds



On-Premises

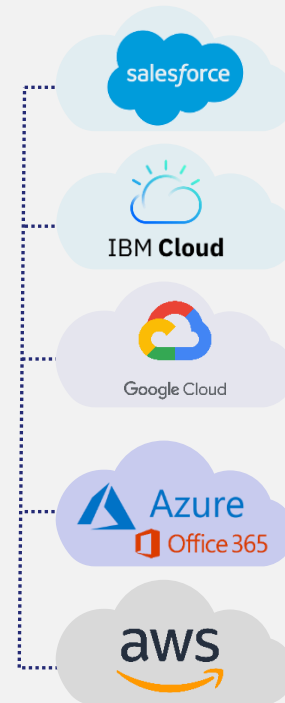


Goals:
Cloud-Neutral Control

**Centralized
Key
Management**

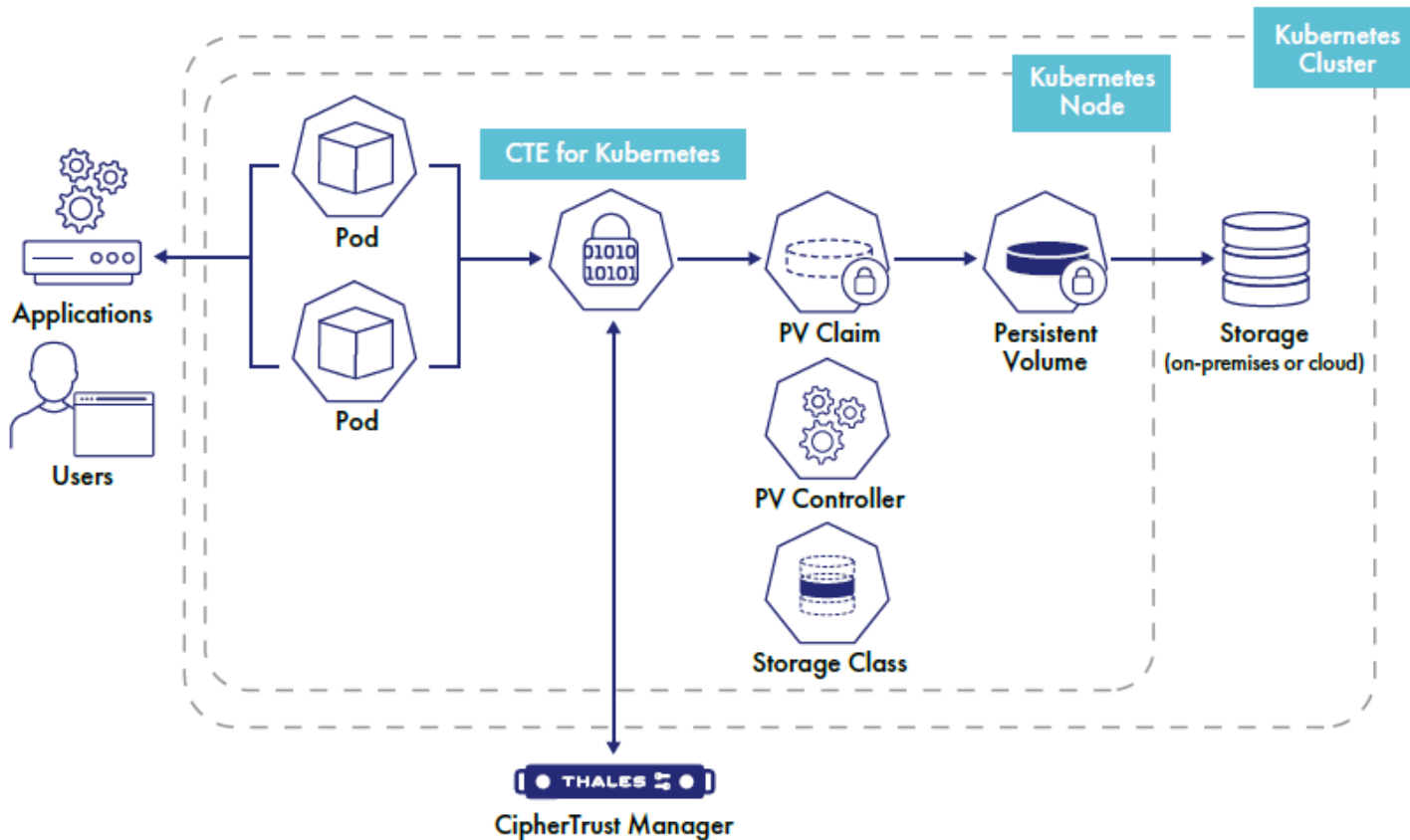


Challenges:
Encryption Key Visibility
Data Loss Prevention
Attaining Compliance
Key Lifecycle Management



Multiple Public Cloud Services

Use case: software development in kubernetes environment



Identity is the new...everything!

Passwordless? User personas?
Authentication journeys?
MFA? PKI? IAM? CIAM?

Attila Paksi, Thales
2023



Chat GPT and its potential...

AT

Fair enough. So tell me: are cybercriminals also using your talent?



As an AI language model, I don't have the ability to know or control how people use my responses or outputs. However, it's possible for cybercriminals to use AI technology for their malicious purposes. For example, they can use AI-powered phishing attacks, chatbots or deepfakes to deceive or defraud individuals, steal sensitive information or spread malware.

It's important to stay vigilant against these types of attacks and to take necessary measures to protect yourself, such as keeping your software and security systems up-to-date, using strong passwords, being cautious of suspicious links or attachments, and using reputable cybersecurity solutions.



PhaaS

What's PhaaS ?






- On May 2022, a new service by **EvilProxy** has emerged, promising to steal authentication tokens to bypass multi-factor authentication (MFA) on Apple, Google, Facebook, Microsoft, Twitter, GitHub, GoDaddy...
- **Zero code phishing solution** for the low-skill threat actors
- EvilProxy is offered on a **subscription** base - 10, 20 or 31 days
- Attackers get : user credentials and an authenticated session cookie
- Available both in the clearnet and darknet

How much PhaaS cost ?

Browser address bar: <https://cpanel.pua75npoc4ekrkppdglafn5mi2hxsunz5uuup6uxqmen4deepyd.onion/moloch/origins/all>

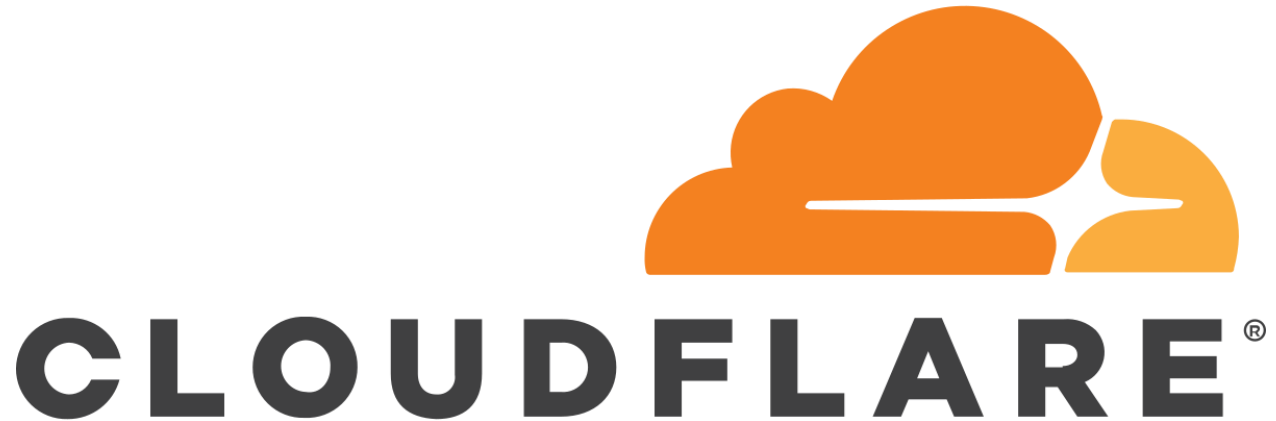
Contacts: evilproxy | Available Services & Prices | Account Balance: 400

Search for

Bundle	Entry Scopes	Data Collected	Price
 dropbox	dropbox.com	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 rubygems	rubygems.org	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 yandex	yandex.ru	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 yahoo	yahoo.com	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 microsoft	xbox.com		
	skype.com		
	onenote.com		
	office.com	✓ login	10 days - 150\$
	microsoftonline.com	✓ password	20 days - 250\$
	microsoft.com	✓ session cookies	31 days - 400\$
	live.com		
bing.com			
		✓ login	10 days - 150\$

Who's Cloudflare

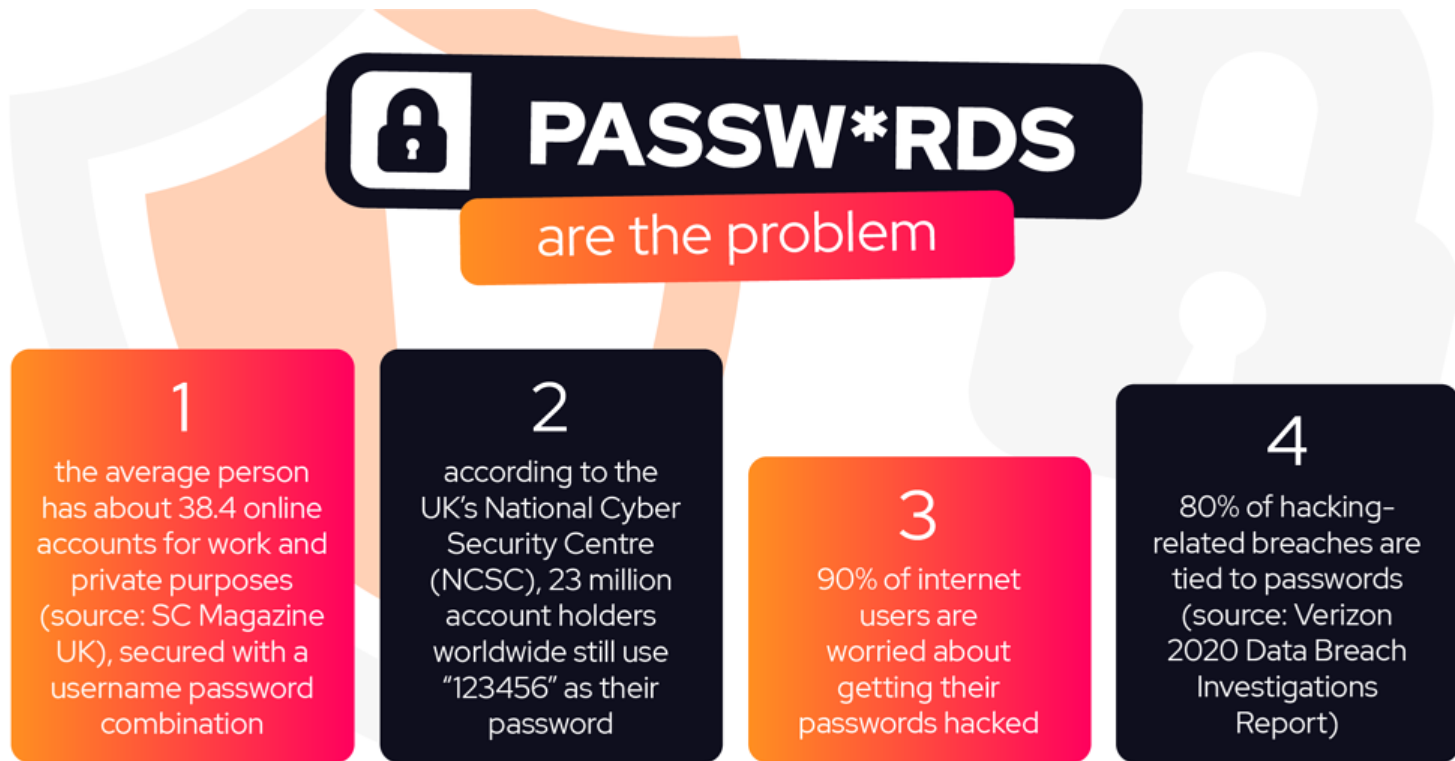
- Based in San Francisco
- An American content delivery network and DDoS mitigation company
- It primarily acts as a reverse proxy between a website's visitor and the Cloudflare customer's hosting provider



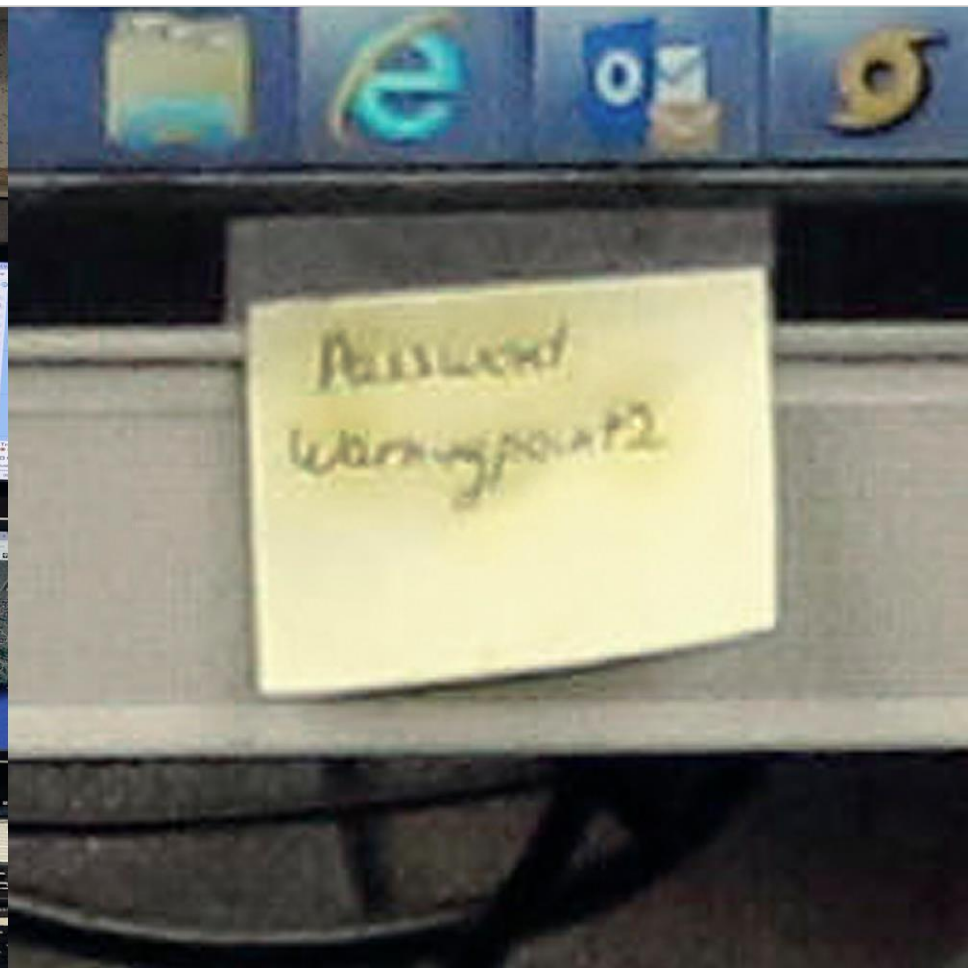
The Cloudflare's attack

- On July 20, 2022, the Cloudflare Security team received reports of employees receiving legitimate-looking text messages pointing to what appeared to be a Cloudflare Okta login page
- Employees and family members received text messages
- Spoof login website was registered less than 40 minutes before the phishing campaign began
- Every employee at the company is issued a **FIDO2-compliant token**
- Attack result: NONE 😊

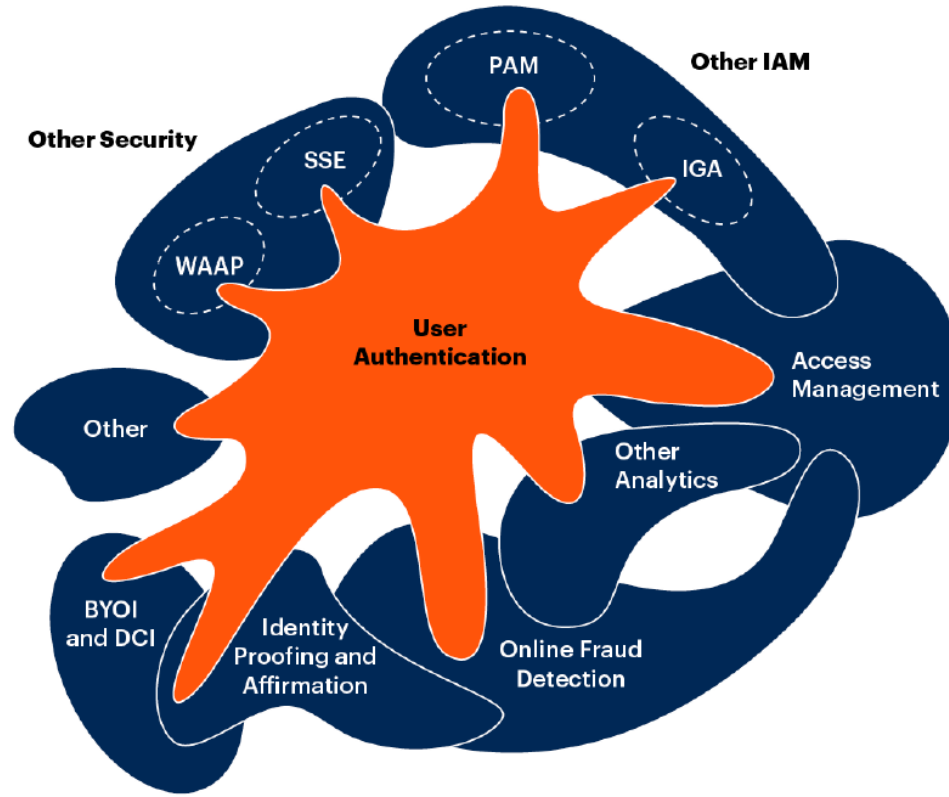
The password problems!



This is a SOC...



The Boundaries of User Authentication Are Fuzzy



Source: Gartner
731668_C



How and to whom can I SAFELY make the data available remotely?

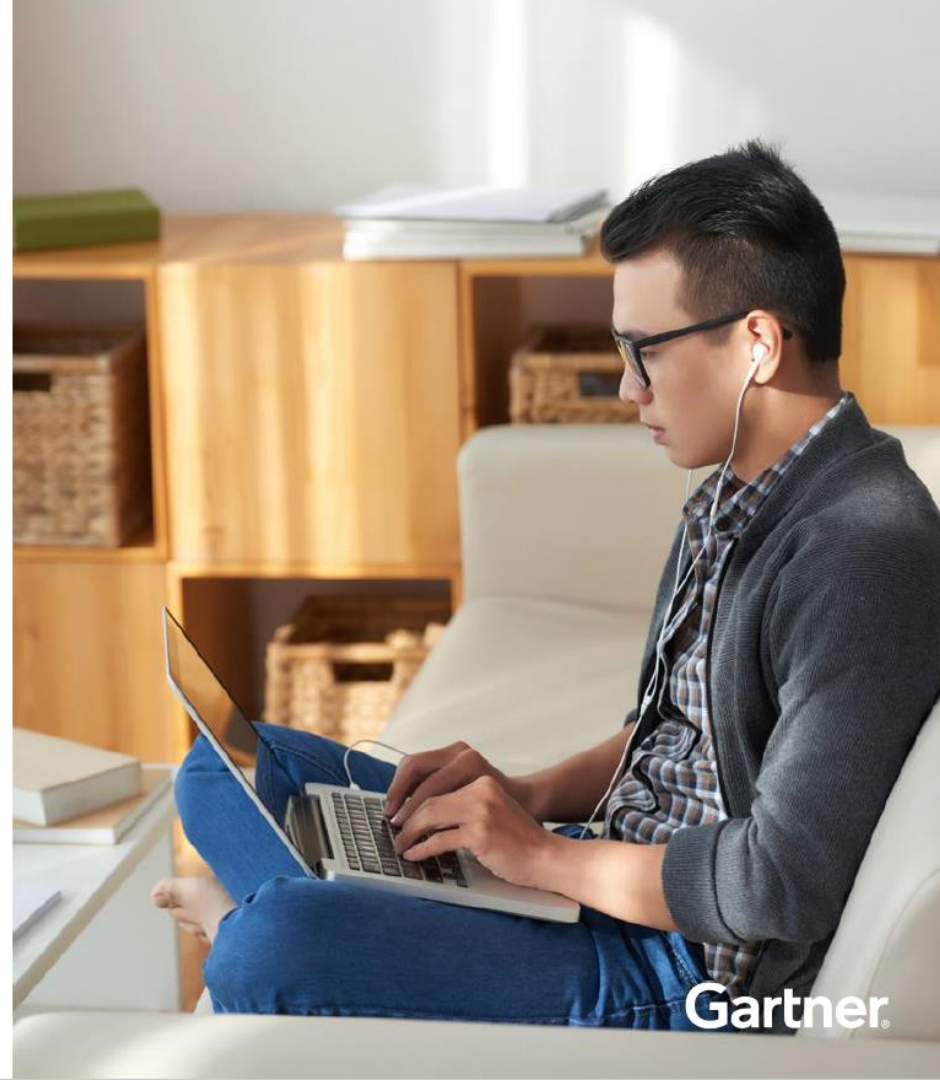


Users are NOT equal...

User Experience Matters

- Adding MFA can add friction (but it doesn't have to)
- Employee and customer experience is more important than ever
- Offering multiple options for diverse users is necessary
- Password less MFA is one possible answer

Source: Gartner

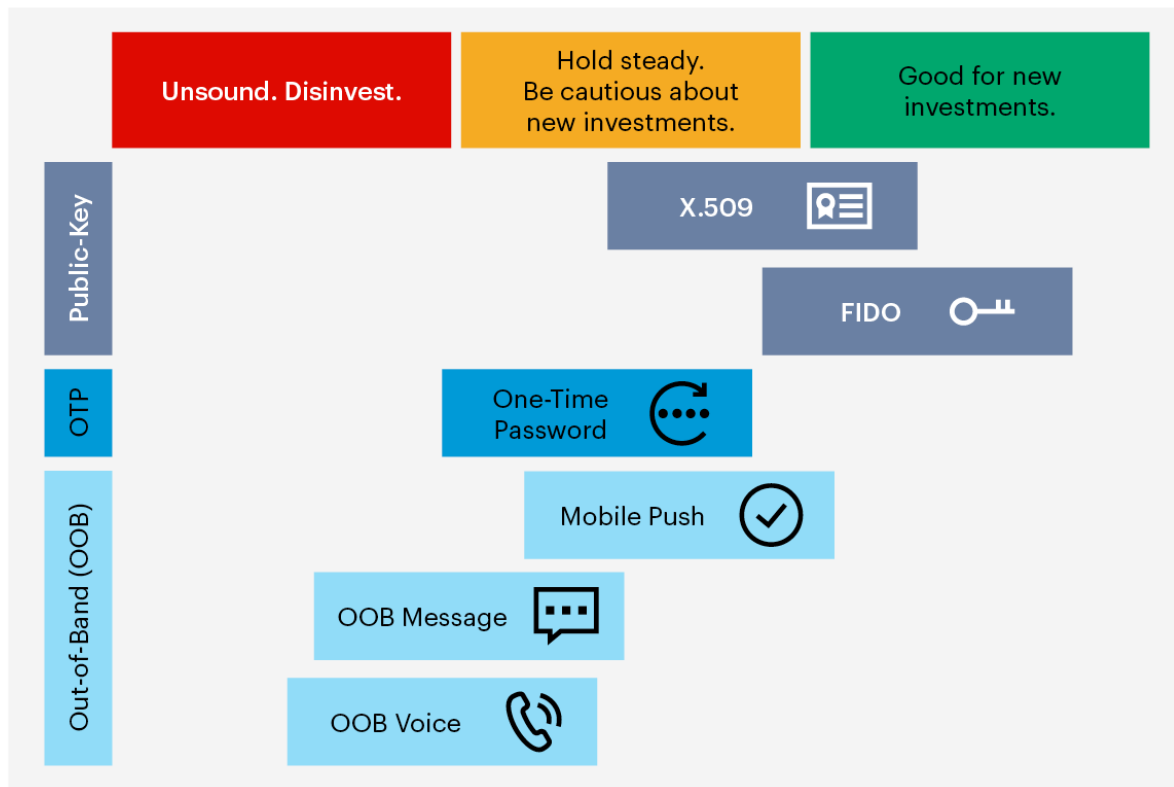


User Persona – Users are NOT equal...



Where to put your authentication budget?

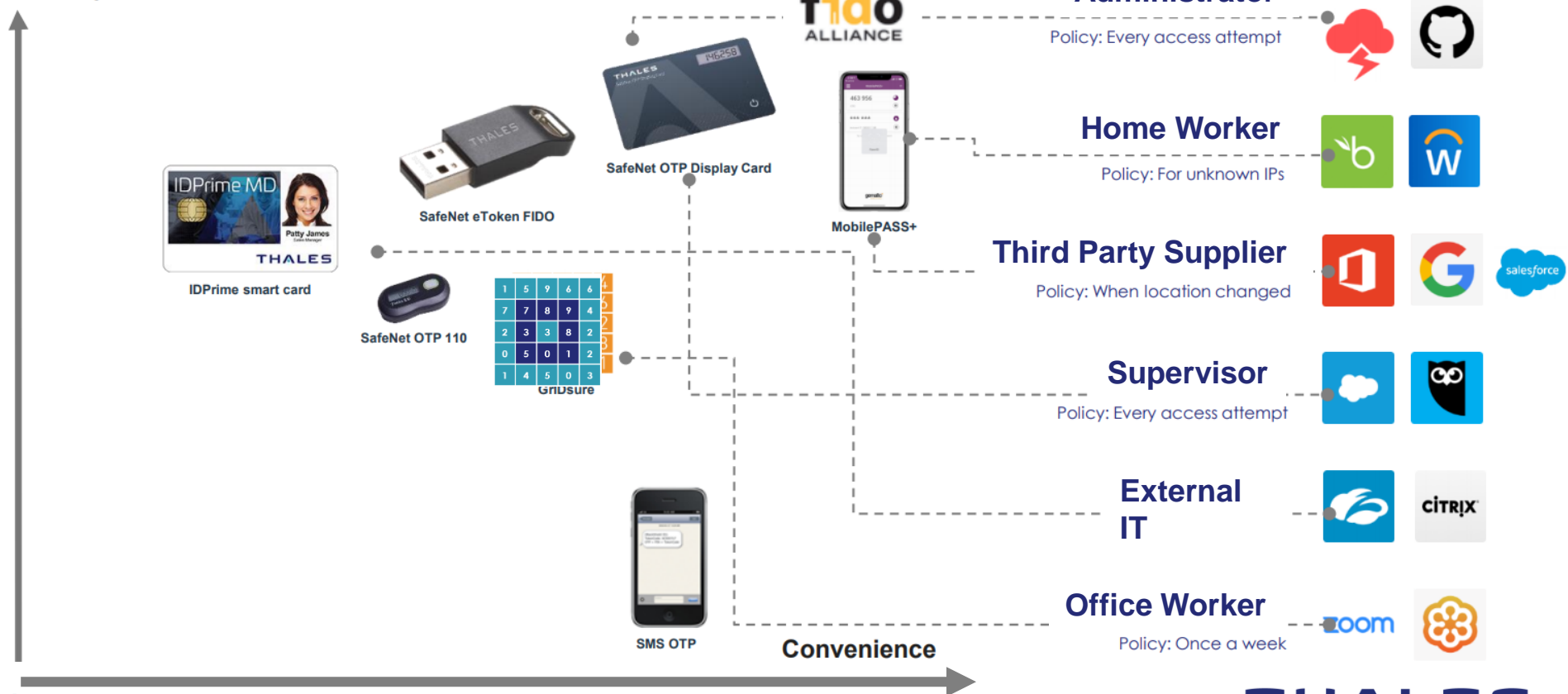
The Strategic Value of Different Kinds of Authentication Token



Source: Gartner
724226_C

Different authentication paths

Security



A leading player in the field of PKI-based authentication

Development

Supporting new use cases



IDPrime Virtual



FIDO hardware authenticators

Maintenance

The strongest MFA portfolio



Smart cards



Tokens



Middleware

- PKI and FIDO2 support in one device
- Use of existing PKI investments
- Rapid deployment based on Thales Middleware and existing PKI infrastructure

- PKI + FIDO2 tools
- Combined FIDO – PKI Smart card
- FIDO USB token



THALES

Thales Devices Characteristics

	Form Factor			Mode				Certification		Applet	
	USB-A	USB-C	Smart card	Contact	Contactless	Dual interface*	Physical access	FIPS	CC	PKI	FIDO 2.0
eToken FIDO	✓	✓		FIDO							✓
eToken FIDO fusion	✓	✓		PKI, FIDO					✓	✓	✓
IDPrime 3940 FIDO			✓			PKI, FIDO			✓	✓	✓
IDPrime 3930 FIDO (roadmap)			✓			PKI, FIDO		✓		✓	✓
IDPrime 931 FIDO			✓	PKI	FIDO		✓	✓		✓	✓
IDPrime 941 FIDO			✓	PKI	FIDO		✓		✓	✓	✓
IDCore 3121 FIDO			✓		FIDO		✓				✓
eToken 5300 FIDO (roadmap)	✓	✓		PKI, FIDO						✓	✓



Thales FIDO Devices with other 3rd Party IDP and CMS



Mapping out FIDO use cases

Suitability of Authentication Tokens in Different Use Cases and Recommendations

			Windows PC and Network Login	Remote access (VPN, SaaS, &c.)	PAM	Banking	Other CIAM				
Public-Key	X.509	Dedicated Device	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
		Companion Device	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
		Embedded Creds	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
	FIDO	Dedicated Device	<div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div></div>	↑	
		Companion Device	<div><div></div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div><div></div></div>	↑	
		Embedded Creds ^a	<div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div><div></div></div>	↑	
OTP	One-Time Password	Dedicated Device	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
		Companion Device	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
		Embedded Creds	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
Out-of-Band (OOB)	Mobile Push	Companion Device	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↑	<div><div></div><div></div><div></div></div>	↓	
		Embedded Creds	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
	OOB Message	Companion Device	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
		Embedded Creds	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	
		OOB Voice	Companion Device	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓
			Embedded Creds	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓	<div><div></div><div></div><div></div></div>	↓
Key			Suitability	Poor		Very Good		Given ease-of-integration, trust and UX considerations			
Recommendation			<div><div></div><div></div><div></div></div>	Good for new investments.			3-Year Trend				
			<div><div></div><div></div><div></div></div>	Hold steady. Be cautious about new investments.			↑ Increasing				
			<div><div></div><div></div><div></div></div>	Unsound. Disinvest.			— Flat or Uncertain				
							↓ Decreasing				

Source: Gartner

^aIncluding Windows Hello or WHfB

724226_C

THALES

“Hope is not a strategy”



THALES

Hvala!

Gábor HIRSCH

gabor.hirsch@thalesgroup.com

Attila PAKSI

attila.paksi@thalesgroup.com

Thank you

Gracias مكمل اركش

धन्यवाद Merci

Danke 謝謝

ありがとうございました