



Trust **Your Digital** User

BEHAVIORAL-BASED THREAT & FRAUD PROTECTION

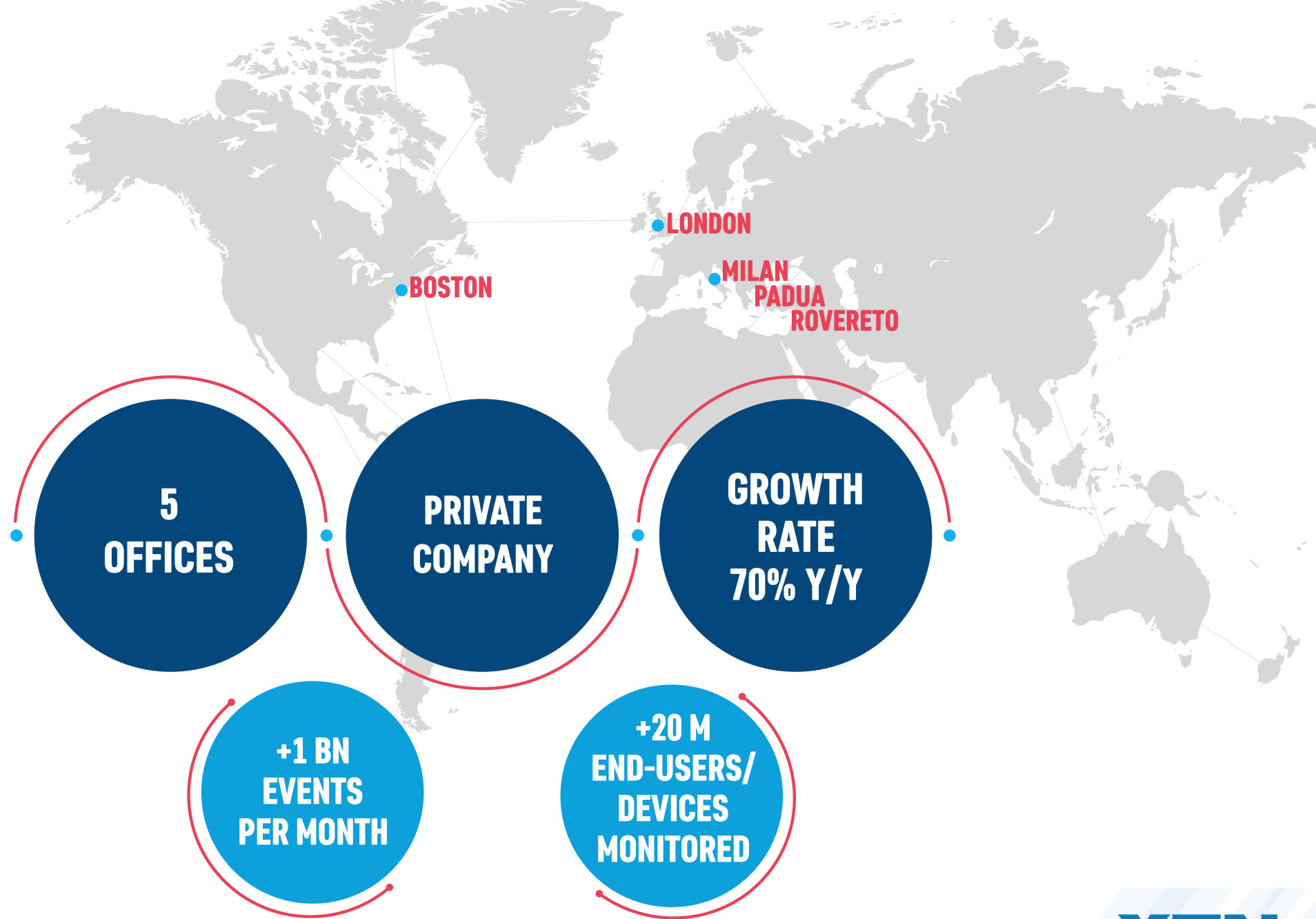
XTN is a provider of Behavioral-based **Threat and Omnichannel Fraud Protection** solutions designed to defend digital businesses, avoiding any impact on user experience.

Our security solutions are **Cognitive** using proprietary AI algorithms. We also employ **Behavioral Biometric Analysis**, both to guarantee complete user profiling, and to evaluate and block anomalies and threats in real-time.



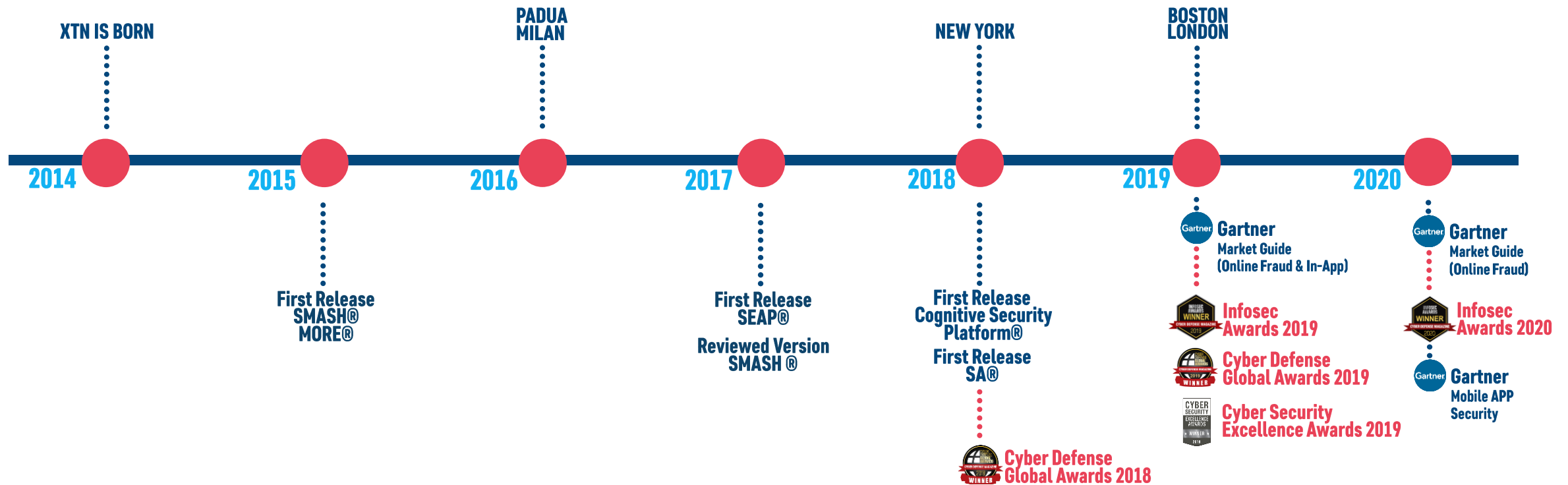
XTN

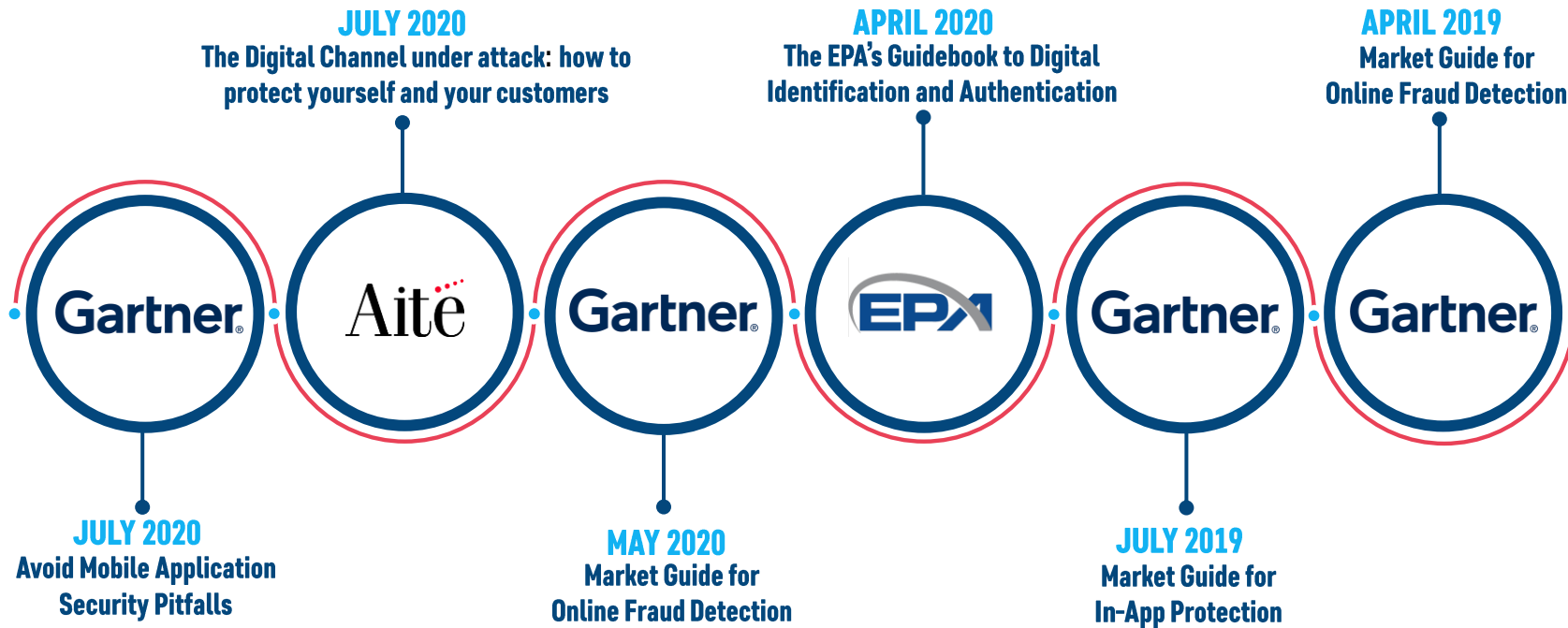
**WHO
WE
ARE**



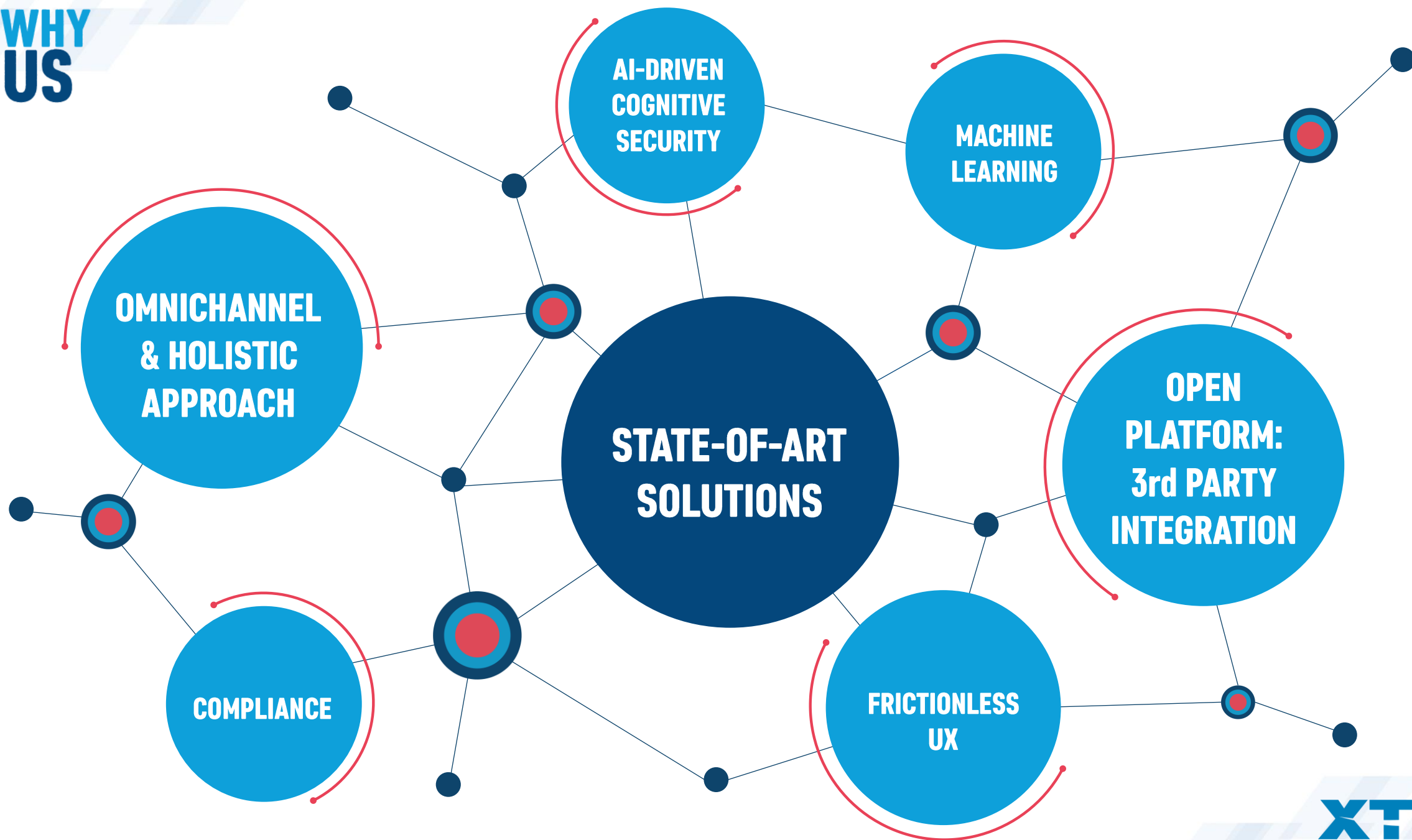
XTN

OUR MILESTONES





**WHY
US**



XTN

COGNITIVE SECURITY



BEHAVIORAL BIOMETRICS

OUR APPROACH

Our collective experience in cybersecurity is **ENCODED** into our products. We transformed our **HUMAN SKILLS** into artificial intelligence.

Continuously refining methods and processes, the system learns to anticipate threats and generates **PROACTIVE RESPONSES**.

COGNITIVE SECURITY

Learning algorithms enable us to process and analyze in real-time huge volumes of data and **IDENTIFY THREATS** impossible for a human to detect.

= SMART SOLUTIONS

- EASY TO USE
- EFFECTIVE
- FAST ROI

OUR APPROACH

BEHAVIORAL BIOMETRICS

CONTINUOUSLY EVALUATING

the anomalies in interacting with the service,
allowing the countermeasures to be dynamic,
saving your user from unnecessary friction.

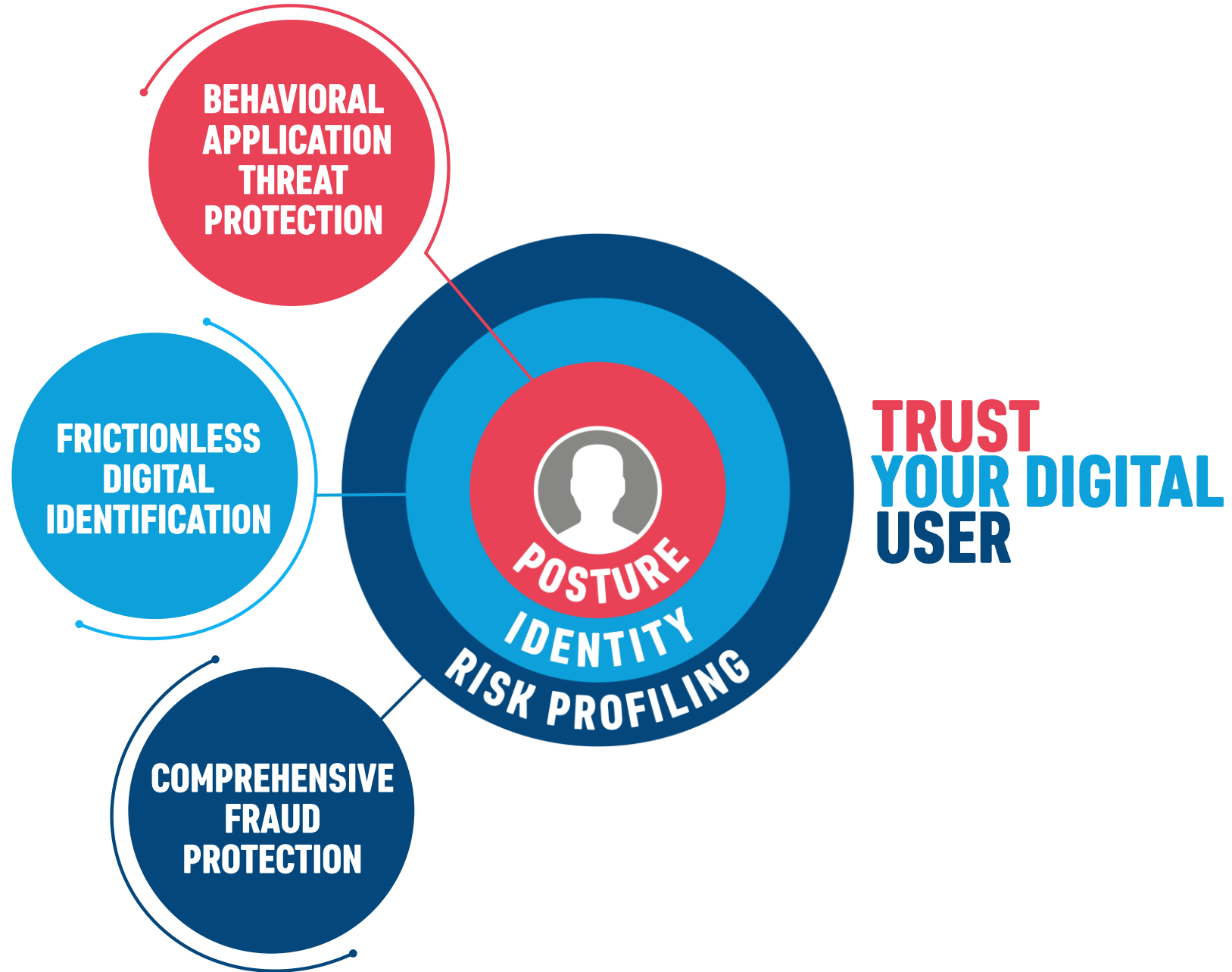
• allows you to

IMPROVING SECURITY POSTURE
without disrupting your users' experience
and without hardware requirements.

= PROTECT

your digital services from
identity-related **FRAUD** and
MALWARE-BASED or **BOT ATTACKS**.

**WHAT
WE
DO**

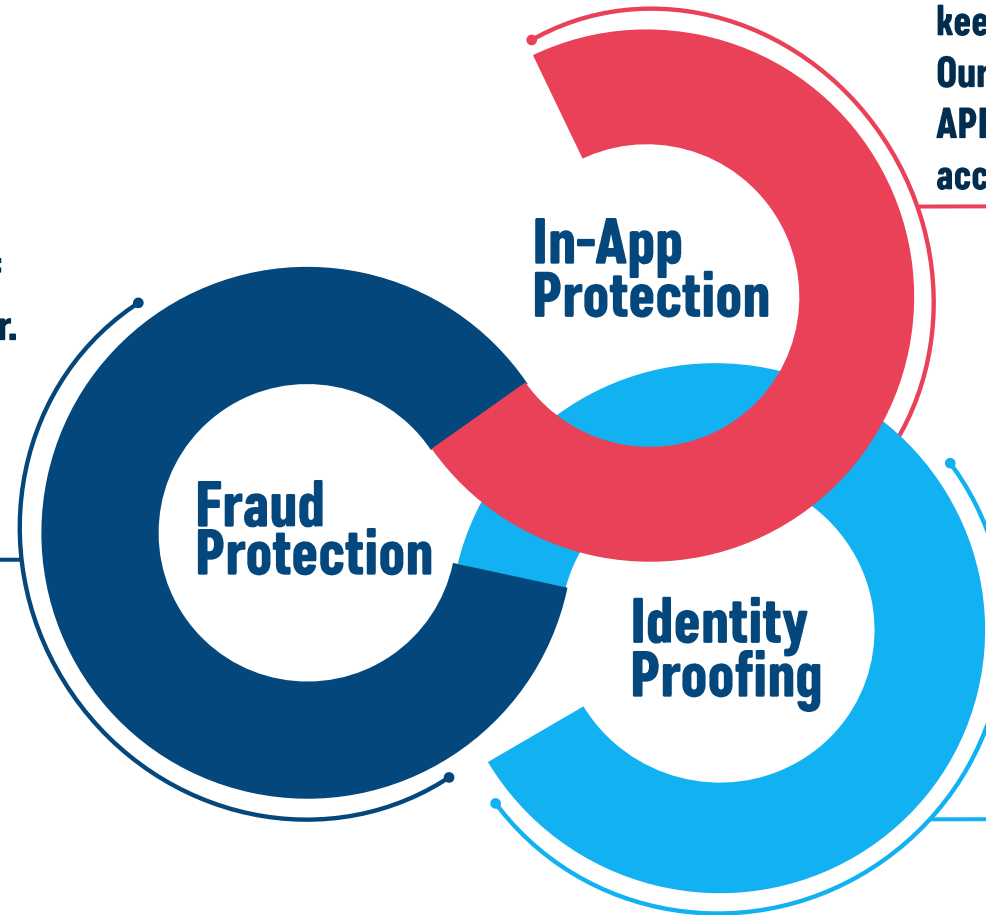


XTN

WHAT WE DO

PROTECT YOUR ONLINE PAYMENTS

Our solution learns to recognize users of online services and their usual behaviour. We use machine learning techniques to analyze and correlate hundreds of parameters determining in **real-time a risk score** for every transaction.



KEEP YOUR APPLICATIONS SECURE

Our **Behavioral In-App Protection** solution lets you keep your applications secure from the inside. Our **comprehensive and innovative vision** considers APP hardening, behavioural analysis of the user who accesses the service, and the service itself.

EFFECTIVE USER PROFILING

We generate an effective profile of your customers' digital identity using **dynamic digital indicators** and guaranteeing high levels of security, and a **fluid user experience**.

COGNITIVE SECURITY PLATFORM®

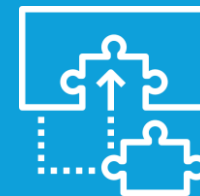




**HOLISTIC
APPROACH**



**OPEN
PLATFORM**



**THIRD-PARTY
SOLUTIONS
INTEGRATION**

KNOW YOUR CUSTOMER

USER BEHAVIOUR

We learn users' behavior and we identify suspicious events.

REAL-TIME ANALYSIS

We aggregate multiple customer interactions and channels and also analyzing hundreds of touch points in real-time.

MACHINE LEARNING

AI supported by several machine learning algorithms to provide the best solution for specific challenges.

BEHAVIORAL BIOMETRICS

We use passive biometrics to correlate and match the device to the specific end-user.

HOLISTIC APPROACH

THREAT ANALYSIS

Our behavioral biometrics solutions allow you to detect and block zero-day threats on apps (account takeover, malware, etc.)

CUSTOMER ID

Through an advanced profiling activity, we provide a strong end-user identification to prevent multiple threats and guarantee secure transactions.

FRAUD ANALYSIS

We proactively detect frauds: using real-time information we react ever and wherever required. This is pre and not post fraud analysis.

HOW WE DO IT

EASY INTEGRATION

**CLIENT &
SERVER**

**Easy client
and server
deployment.**

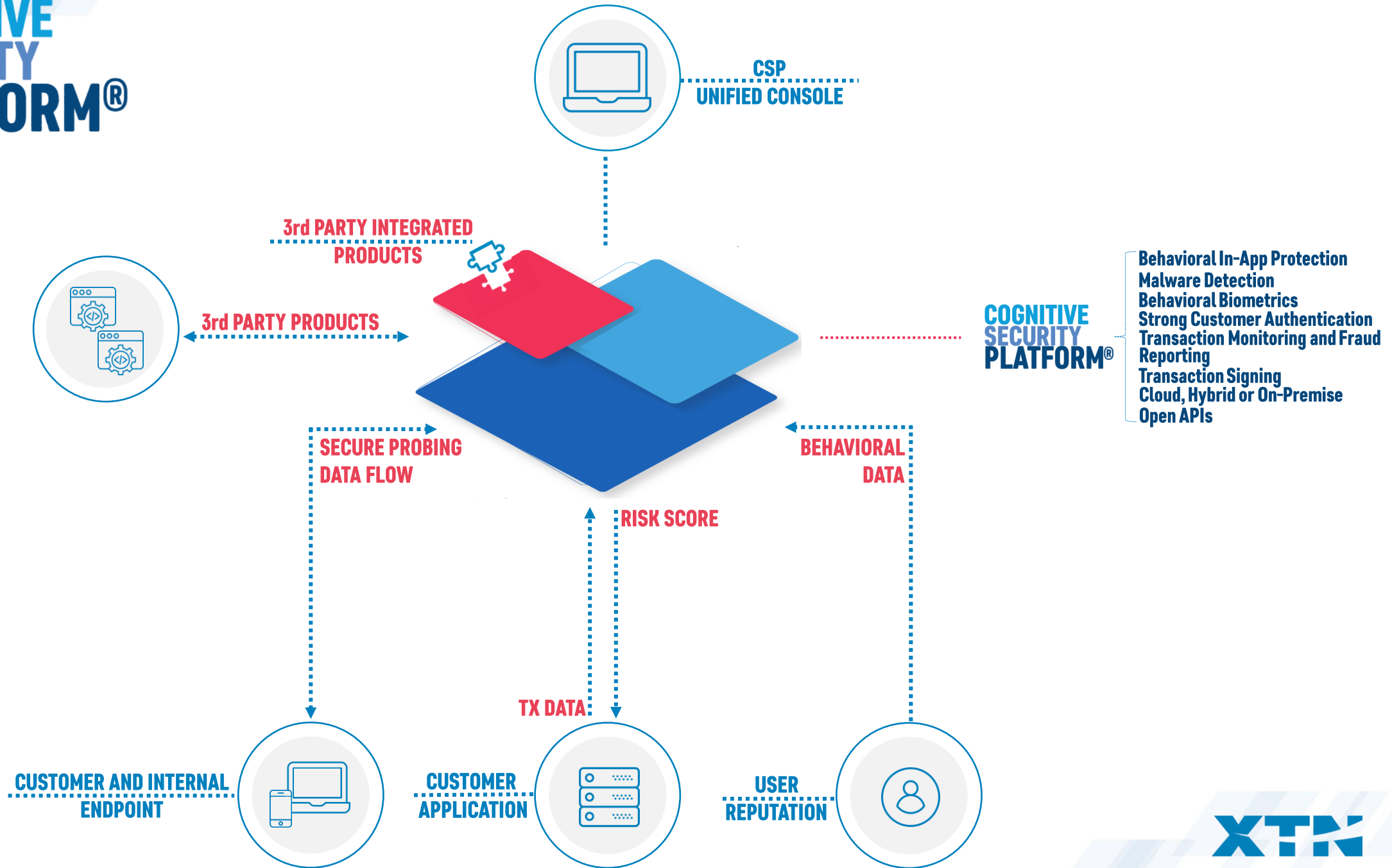
**API BASED
INTEGRATION**

**API based
integration.**

CLOUD

**Deploy in Cloud
(AWS & Azure),
Hybrid Cloud and
On-Premises.**

COGNITIVE SECURITY PLATFORM®



TRUSTED IDENTITY CORROBORATION MODEL (TICM)

AFFIRMATIVE SIGNALS

EVIDENCE that *increases* the confidence in the identity claim, elevating the associated level of trust.

Third-party
credentials

Curated
credentials

Familiarity
signals

IDENTITY
CORROBORATION

combines
affirmative and
negative signals
to yield a net
confidence, or
level of trust, in
the identity
claim.

Risk
signals

Attack
signals

Anomalies

EVIDENCE that *reduces* the confidence in the identity claim, decreasing the associated level of trust.

NEGATIVE SIGNALS

2017 Gartner, Inc.

OUR PRODUCTS

SEAP /[®]

ANTIFRAUD and **THREAT PROTECTION** controls at the endpoint level for both **WEB** browser and **MOBILE** devices, providing a unique, integrated and powerful solution to manage fraud and security risks of online digital services.

SA /[®]

Ultimate solution for customer **IDENTIFICATION (BIOMETRIC AUTHENTICATION and TRANSACTION SIGNING)**, based on behavioral and risk based continuous evaluation, designed for innovative e-payment services.

SMASH /[®]

ANTIFRAUD SOLUTION based on a widespread model of Transaction Monitoring primarily for financial markets. **SMASH**[®] learns to recognize users of online payment services and their **USUAL BEHAVIOR** and patterns.

CASE STUDIES

FRAUD IN FINANCIAL SERVICES



- ⊕ Mid-size European bank
- ⊕ ~300K users
- ⊕ Corporate and retail services



- ⊕ In 2017 about 1.1M euros of fraud attempts cross products



- ✓ 100% of the attempts prevented
- ✓ Zero euros lost in fraud
- ✓ False positives reduced up to 40%
- ✓ Fraud detection improved up to 30%

MALWARE IN FINANCIAL SERVICES



- + European multi-national next-generation bank
- + Online-only services (mostly mobile)
- + 30M transactions on their platform every month
- + Focused on retail banking (financial management and advisory services)



- + Experiencing an increase in malware attacks and account takeovers
- + Needing to improve the user experience without weakening security posture



- ✓ Perimeter endpoints have been secured
- ✓ Continuous risk evaluation
- ✓ No human interaction
- ✓ Higher security without any negative customer experience
- ✓ Targeted awareness campaigns

PROTECTING ONBOARDING FOR CHALLENGER BANKS



- + Next-Generation bank
- + App-based services
- + Onboarding process totally app-based



- + Need to spot out fraudulent new users that try to onboard



- ✓ Thanks to behavioral analysis and consistency checks, a fake account is recognized as soon as it starts the online procedure

AUTOMOTIVE ENTERPRISE SECURITY



- + World famous automotive vendor
- + +100 billion \$ in revenues
- + 9M users
- + Several contractor working inside the company perimeter



- + Protecting B2B and internal services to prevent reputational damage
- + Preserve end-customer privacy data
- + Block industrial spying



- ✓ Perimeter endpoints have been secured
- ✓ Continuous risk evaluation
- ✓ Monitoring Know Your Customer checks
- ✓ BYOD approach

AUTOMOTIVE CONSUMER FACING



- + World famous automotive vendor
- + +100 billion \$ in revenues
- + 9M users
- + Several contractor working inside the company perimeter



- + Protecting consumer-facing connected vehicle mobile and web services
- + Prevent reputational damage
- + Preserve end-customer privacy data and vehicle security



- ✓ Technological and behavioral checks
- ✓ Strong digital identity validation
- ✓ Continuous and real-time server-side risk evaluation
- ✓ SIEM and backend integration and reporting
- ✓ RASP functionalities
- ✓ App obfuscation



 xtn-lab.com

 sales@xtn-lab.com