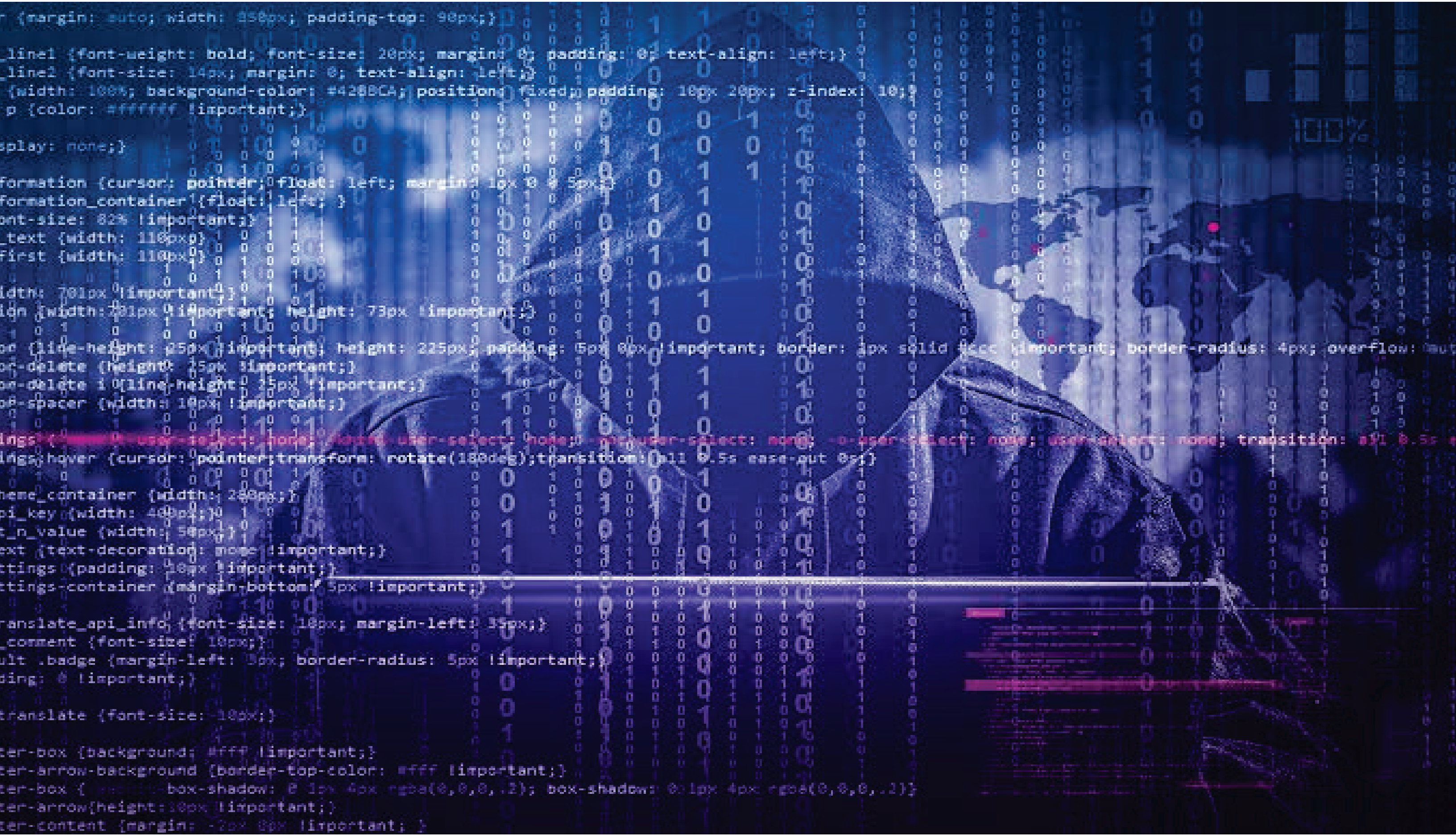
Fighting Fraud in Online Services with XTN Cognitive Security



XTN's goal is to fight fraud in online services through our Advanced Behavior-based Security solutions we develop since 2014. Through the award-winning and multi-layered Cognitive Security Platform®, we protect the services of several kinds of environments, such as Banks, Fintech, e-commerce, and Automotive.

Fraud in online services

Online services suffer from a wide variety of frauds. One of the more common patterns is related to account or sensitive information takeover. Takeovers range from the control of the bank account of the victim up to stealing their credit card information. The result is most of the time an undesired transfer to a temporary account managed by the fraudster. There are more technologically advanced frauds where the attacker takes control of the application used to perform fraudulent transactions directly. With the rising of online onboarding procedures in next-generation payment services, there is also a rising trend related to rogue identities and BOT driven account creation. In the end, the fraudster goal is to monetize the attack as quickly as possible, finding an easy to scale and maintain fraud flow.

XTN vision is to correlate different layers of analysis to obtain a holistic approach to detect fraudulent events. The Platform considers the posture of the endpoint used to access a critical service, the digital identity of the user and the risk profiling related to business content of events. Our unique technology relies on cutting edge artificial intelligence to provide excellent accuracy and minimal false positives.
XTN technology conciliates different needs that are mandatory in the fraud analysis space: behavioral perspective, the intelligibility of the risk causes, flexibility and real-time response.
We solve the challenge of providing visibility about fraud attempts coming from consumer-facing or internal critical services. The banking sector is one of our reference markets and is pretty evident the urgency of limit payment related frauds. But also other markets need this kind of protection. That's why we are also working in the automotive environment to protect connected-vehicles services.

Mobile and web application security

We see, globally, very high pressure on mobile online services. Security awareness is increasing, and users demand secure services, both considering privacy and money. On the other side, service providers are struggling with growing security while keeping easy and enjoyable user experience in their apps. The result is that a new generation of service providers is starting pointing on great functionalities designed to include security and easiness of use by default. These new generations of services are finding spaces to compete in these fields. Our aim for the future is to face advanced threats while maintaining small or no impact on the user experience. At XTN, we are ready to embrace this challenge. Our goal is to provide the smoothest user experience possible while keeping the highest security level. To do that we consider the endpoint, and in particular mobile devices, as the central actor in identity proofing.

Smart Authentication

Authentication for us is much more of a password or second factor of authentication. In the XTN Cognitive Security Platform®, digital identity validation relies on different layers: behavioral biometrics features, endpoint trust and cryptographic quantities. These layers let us modulate the authentication factors considering the endpoint trust or risk and including continuous behavioral analysis to recognize anomalies.

In-App protection next level

At XTN, we believe that protecting the app goes beyond the app assets in the end-point. We think that modern protection requires implementing a probe-evaluate-react pattern, including the app's technological threats detection together with behavioral and identity-related features. Our technology is taking all relevant information from the app to our clients, without any user experience impact, building risk-driven reaction flows that originate at server-side, where the trust should be.

XTN goes global

Nowadays, we are approaching the global market, knowing that our technology offers unique features and differentiators. Moreover, having a stable presence in Italy could be a value for clients worldwide. You probably don't know that, but Italy is a virulent country from a fraud perspective, and this came out to be an excellent training ground for our technology.

XTN is based in London, Boston, Milan and Rovereto (TN).

ABOUT

XTN Cognitive Security® develops Advanced Behavior-based Security solutions since 2014.

Thanks to founders' experience in cybercrime, XTN designs a new generation of Anti-Fraud solutions which allows companies and institutions to protect their business and their customer's sensitive data.

XTN non-invasive and frictionless solutions are made unique by breakthrough Behavioral Biometrics technology. Through the award-winning and multi-layered Cognitive Security Platform®, XTN protects the services of several kinds of environments, such as Banks, Fintech, e-commerce, and Automotive.

Since its inception, the company has significantly invested in activities, thus improving and earning competencies in developing Artificial Intelligence and Machine Learning based solutions.

XTN is based in London, Boston, Milan and Rovereto (TN).

About the Author

Guido Ronchetti is the CTO of XTN Cognitive Security.

In his career, he has been involved in designing several security products.

In XTN one of its primary aims has been to apply machine learning models to behavioral related security problems.

Watch some interesting interviews with him at www.cyberdefensetv.com or visit him online at https://xtn-lab.com/