nevisDetect – Risk Detection System

Digital access should be simple and secure, regardless of the channel customers choose. At the same time malicious attacks have increased in sophistication – 2nd factor authentication is not sufficient anymore to protect against malware-based "man in the browser" or identity theft attacks. In addition, multi-factor authentication creates friction in the user experience and leads to weaker customer engagement. The requirement to increase the protection of critical services without compromising user experience requires new, holistic security concepts. nevisDetect was built with these requirements in mind. It enables the integration of leading-edge detection technologies in one single platform. With nevisDetect, digital services are protected by continuous, risk-evaluating mechanisms, which guarantee a very high level of protection without compromising user experience.

Benefits

- Detect and prevent identity theft and account takeover.
- Detect and prevent session hijacking.
- Determine the true identity of individuals by the way they behave and interact.
- Improve session security without compromising customer experience.
- Reduce false positives by leveraging multiple leading-edge anomaly detection technologies.
- Forensic officers can quickly analyze suspicious activities and see identity data in historical contexts. This enables organizations to improve regulatory reporting and efficiently comply with new provisions set out by the authorities.
- Security teams can proactively identify suspicious identities before critical transactions are performed in the back end.
- The scoring mechanisms of other anomaly detection systems (e.g., payment anomaly detection systems) can be enriched with the scores observed by nevisDetect. This enables a dramatic reduction of the manual workload in fraud departments while minimizing losses and costs.
- Support desk teams can efficiently handle customer requests through retrieval of selected user information. After proper customer identification, support agents may be enabled to selectively override system actions.

Main Technical Features

- Modular and customizable setup
- Designed for high load and asynchronous detection
- Designed for multi-line deployments
- Correlation of TCP, TLS and HTTP features
- Plug-in architecture enables easy integration of new detection modules
- Data retention from nevisDetect and BehavioSec are fully customizable to comply with local regulation.
- Simulation- and training model for all detection modules
- Central Management Cockpit for all detection modules
- Seamless integration into existing NEVIS environments
- TLS-Secured communication between components
- Access control provides separation of duty between the roles of the Forensic Expert, Security Expert, Operator and Support Desk

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 Munich ▪ Germany ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de

What is it about?

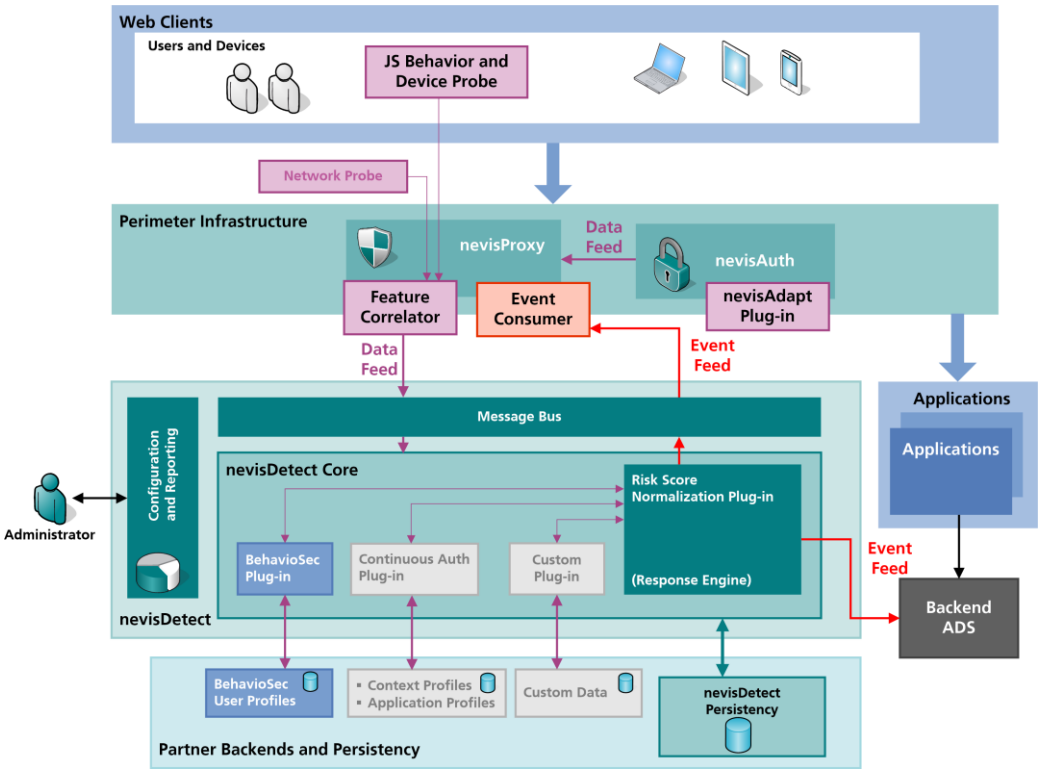

Figure 1: nevisDetect architecture

nevisDetect implements continuous, risk-based user authentication by correlating the output of multiple anomaly detection modules. It is based on the fact that the correlation of multiple attributes like behavioral biometrics, geo-location or device information creates very unique, digital user footprints. Even if an account has been completely taken over by an attacker, the system is able to detect this condition and react accordingly. If, e.g., a valid access request occurred in the early morning in Geneva and that same user tries to log in an hour later from Jakarta, it obviously cannot be the same person. To decide whether a certain user interaction is trustworthy, nevisDetect combines the results of multiple anomaly detection modules into a customizable risk scoring. Based on the risk scoring, the system can initiate mitigation actions: ask the user to re-authenticate, immediately kill the session or open a ticket for further investigation.

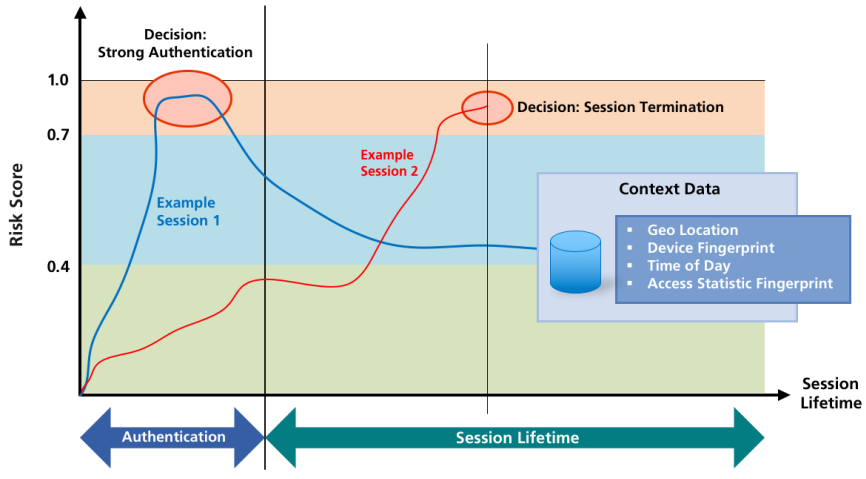

Figure 2: Continuous authentication

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 Munich ▪ Germany ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de