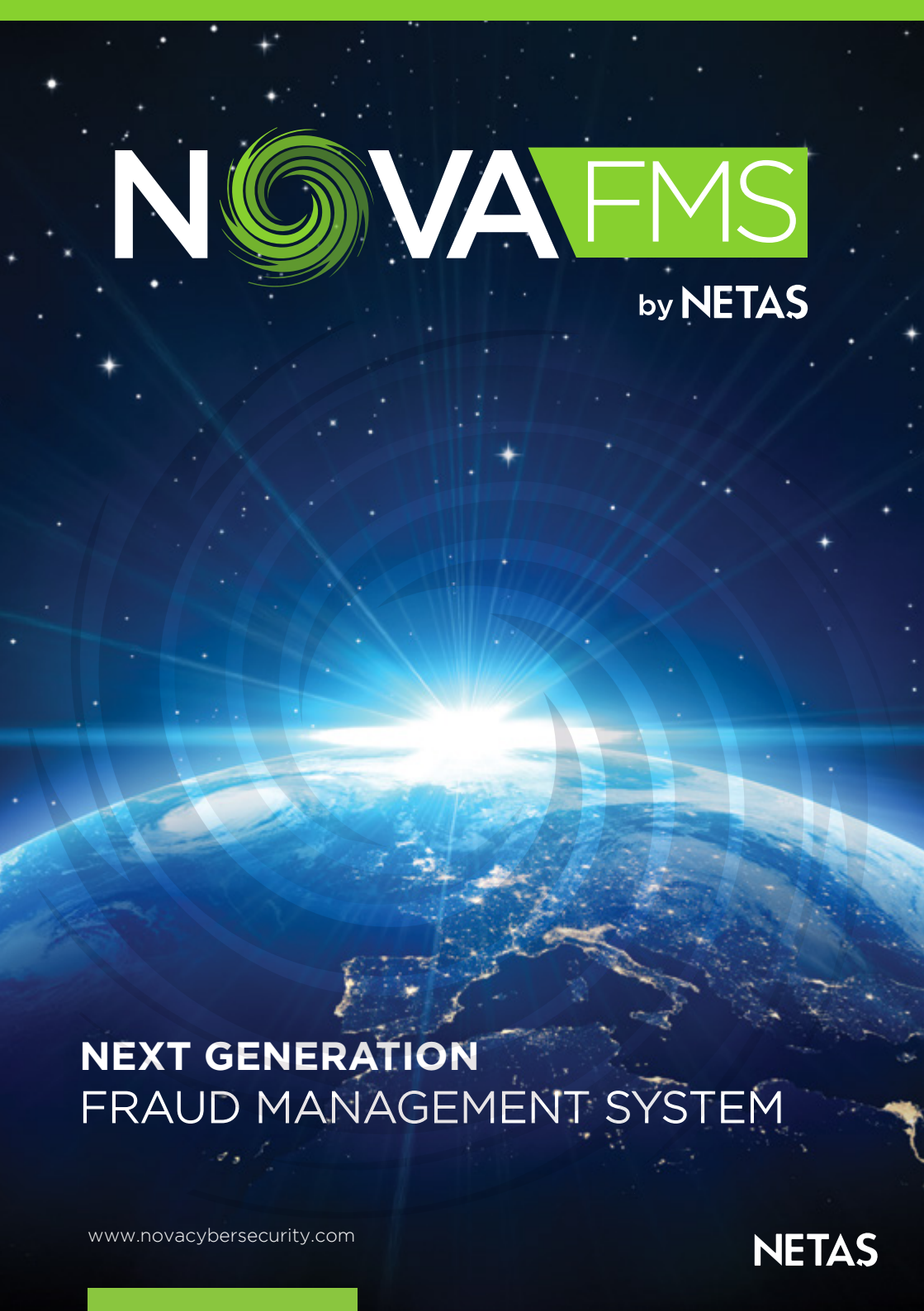

NOVA FMS
by NETAS
NEXT GENERATION
FRAUD MANAGEMENT SYSTEM
www.novacybersecurity.com
NETAS

NOVA FMS
by NETAS

NEXT GENERATION FRAUD MANAGEMENT SYSTEM

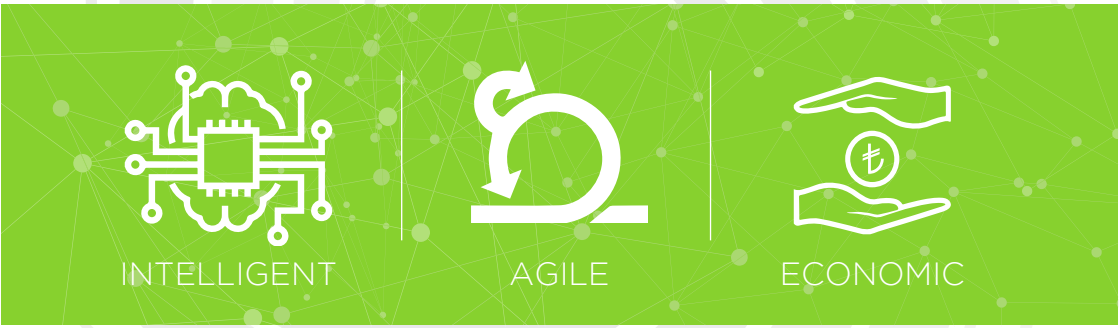
The ongoing digitalization of the business world is putting companies at risk of cyber-attacks more than ever before. Big data analytics has the potential to offer protection against these attacks. Big data security analytics involves data ingest, processing, and analysis to derive actionable intelligence. Various techniques and methods for security analytics, such as sophisticated machine learning algorithms, have become more effective and accurate in the recent years.

NOVA FMS is a big data security analytics platform that supports deep, holistic, correlative assessment using statistical and machine learning approaches. Key points include complex anomalies, cyber-attacks, cyber-threats, cyber-fraud, user behavioral analysis, analytical rule engine and advanced network monitoring (Web, VoIP, and Netflow data).

NOVA FMS
by NETAS

NEXT GENERATION FRAUD MANAGEMENT SYSTEM

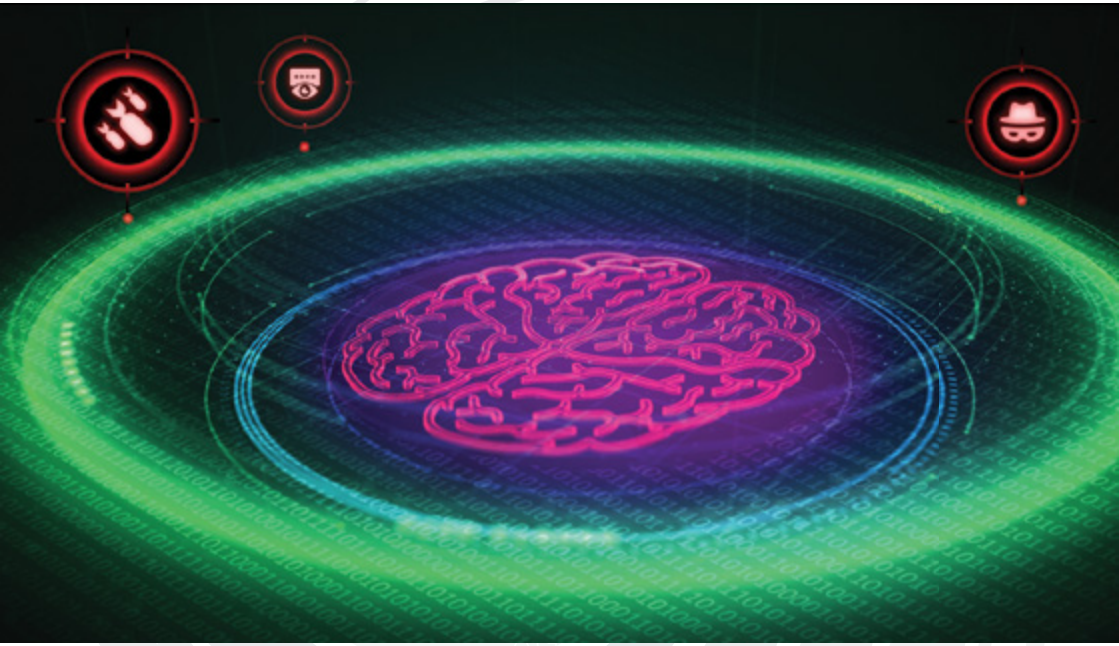
NOVA FMS platform combines two complementary approaches to analyze high volume of telecom data that either is streamed in near-real time or that has accumulated over time. It offers rule-based detection of known patterns, anomalies and attacks. On the other hand, it runs advanced machine learning to learn normal user and entity behavior and detect changes and anomalies in each user's account and call usage. It assigns scores to users based on their risks, and alerts fraud specialists of potential threats and anomalies. NOVA FMS, additionally, provides operational monitoring and data analysis framework with rich visualizations.



The goal of NOVA FMS platform is to provide an Intelligent, Agile and Economic solution that can perform security analysis on massive data volume with machine-learning techniques in real-time to detect frauds and threats. NOVA FMS platform is intelligent because it uses machine learning, user profiling, behavior analysis, threat modeling and combines them to obtain better results. NOVA FMS platform is agile because it can be deployed quickly with out-of-the-box collectors and connectors and machine learning-based threat models. NOVA FMS platform is affordable because it is established with an acceptable cost for both licensing and maintenance with open source big data platforms.

NOVA FMS
by NETAS

KEY CAPABILITIES



Fraud Detection with Streaming Data

The traditional CIA (Confidentiality, Integrity, and Availability) model of cyber security is insufficient to prevent fraud as a threat. In the fast detection of credit card fraud in the financial sector or toll fraud in the telecom sector, streaming data is an important part of the solution. NOVA FMS has a distributed, scalable and stream-based architecture. The process of reaching more meaningful knowledge through the enrichment of streaming raw data continues with understanding, searching and interrogation. Then, actionable intelligence is obtained with a scored and labeled alert through profiling, machine learning algorithms, threat models and analytic rule engine.

NOVA FMS by NETAS

KEY CAPABILITIES

Analytic Rule Engine (ARE)

ARE enables to create and manage rules in NOVA FMS. There is a Rule Build Wizard which is designed to specify the rules in detail field by field. Several types of rules are supported and each type has its own properties. Rules can be created, modified or deleted via this editor.

After the rules are created, they are executed by enrichment and transformation processes with a special scripting language. We can adapt to new threats more quickly with this approach beyond the static rules. Also, there are 2 modes of the rule engine: streaming mode and batch mode.

Anomaly Detection with Machine Learning, User Profiling and Behavior Analysis

Anomaly detection is to detect unusual patterns that do not fit the expected behavior. NOVA FMS correlates and applies security analytics and machine learning algorithms on the pre-processed data in order to detect complex anomalies, attacks and threats in near-real time with minimal false-positives.

Security analytics includes:

- Correlating events and data from heterogeneous sources with the goals of constructing event context and higher-level events, finding patterns.
- Feature set dimension reduction.
- Statistical and machine learning based user, entity, application behavior analysis, defining normal and abnormal behavior, detecting change or anomaly in behavior,
- Group behavior analysis, clustering users into groups,
- Detecting application-specific anomaly,
- Correlating traffic data and alarms across different layers and applications,
- Online and offline security analytics.

NOVA FMS by NETAS

KEY CAPABILITIES

Visualization and Reporting

One of the essential functions of big data security analytics is reporting, presenting information and support for analysis readily and rapidly.

NOVA FMS provides pre-defined and customizable dashboards and historical reports, efficient access to historical data, and investigation tools such as drill downs, ad-hoc search and query of all data for forensic analysis.

Alert Management

NOVA FMS offers scored and labeled alerts to decrease false positives and to speed up the investigation.

Out-of-the-box Collectors and Connectors

NOVA FMS presents out-of-the-box collectors and connectors and also allows collaborations with other Nova products as a solution. While Nova V-Gate, VoIP Application Firewall, is used as both collector and prevention tool for VoIP environments, Nova W-Gate, Web Application Firewall, is used as both collector and prevention tool for Web environments.

NOVA FMS by NETAS

SAMPLE BUSINESS CASSES

TELECOM FRAUD ANALYTICS

Due to various frauds, there is a loss of 38.1 billion dollars in the telecommunication sector. It is a challenge task to be alerted in a timely manner by processing huge volume of call records. Especially, Nova FMS focuses on to detect international revenue share fraud (IRFS, $10.8 billion), premium rate service fraud ($3.8 billion) and traffic fraud (interconnect bypass - $6.0 billion) in real time.

VOIP AND WEB APPLICATIONS ANALYTICS

NOVA FMS is also an instrumental in helping teams increase their productivity, providing the detailed statistical analysis of VoIP and Web applications, presenting real-time and historic key performance metrics and making these stats easily visible.

NOVA

Cyber Security Solutions by NETAS

Are you aware that you are vulnerable to all threats on the Internet?

With increasing voice and video transmission over IP and emerging new technologies such as 4G LTE and 5G, data vulnerabilities and insecurity of standard protocols are the main concerns due to the nature of IP infrastructure systems. Reports show that most of the attacks occur in the application layer. Therefore focusing on the application layer security is the most important aim of a secure IP communication. Discover vulnerabilities, detect and prevent attacks, enable secure media communication with our solution.

Be aware of your vulnerabilities and protect your network with the radiance of NOVA!

Create and operate a secure VoIP infrastructure beginning with VoIP Vulnerability Scanning and Analysis Tool, NOVA V-SPY. V-SPY is an automated, enriched VoIP penetration test suite including rich variety of VoIP attack modules, detailed reports of security measures via expert system.

Detect and prevent VoIP threats using VoIP Application Firewall, NOVA V-GATE.
V-GATE is ready to accomplish your security by performing deep packet inspection, statistical and behavioral analysis, detecting anomalies and preventing VoIP attacks, VoIP monitoring and operational management.

Make a secure multimedia communication via Media Security Platform, NOVA MSP.
MSP can achieve secure media transfer enriched with various security methods and flexible crypto algorithm usage, enabling secure voice and video communication, file transfer, message transfer and whiteboard usage.

Maintain a secure operation in Unified Communications network, VoIP and Web applications with Security Services and Consultancy, NOVA PENTEST.
Pentest Services test the applications, infrastructure and devices themselves to ensure they are protected from VoIP, WEB and Unified Communications-related attacks.

NOVA has cyber security projects such as VoIP, WEB and IoT security, big data security analytics, mobile malware analysis and security operation center.

NETAS

Netas provides innovative end-to-end value added systems integration and technology services in the fields of information and communications technologies. Its customers range from telco providers to public and private enterprises in domestic and international markets.

Netas is one of the top ten global VoIP multimedia labs in the world and holds a track-record of 43 years in R&D. The company continues its foray on VoIP and Unified Communications via delivering ultimate cyber security solutions under the Nova brand. Netas charters its vision to become Turkey's and Region's #1 systems integrator working as per global standards.

The company provides a wide array of services to enterprises functioning in various vertical segments, particularly telco providers, finance, general industry and defense. Netas also nurtures strategic partnerships with global technology giants to provide its customers an insight helps them keep pace with the latest developments in the field of Information and Communications Technology and adopt them more efficiently, and continues to develop software solutions for more than 200 global operators.

http://www.netas.com.tr

Detailed Info

/NetasTR
/NetasTR
/NetasTR
/company/netas
blog.netas.com.tr

E: info@novacybersecurity.com
T: +90 216 522 20 00
F: +90 216 522 23 62

NETAS TELEKOMUNIKASYON A.S.
Yenisehir Mahallesi Osmanli Bulvari No:11 34912
Kurtkoy-Pendik / Istanbul
www.netas.com.tr