FORENOVA

NovaCommand NDR

Detect & Respond to Threats with Speed and Precision

Product Overview

A widening attack surface due to increasing IT infrastructure complexity and fast-evolving cyber threats have left businesses in a precarious situation. Enterprises urgently need threat detection and response capabilities that go beyond traditional security technologies.

NovaCommand NDR provides a crucial yet often lacking element to network security – Visibility. With permanent surveillance of all network activity, NovaCommand detects even the most sophisticated and evasive cyber threats that are missed by firewalls and endpoint security. AI-powered analytics, self-learning ML algorithms, and up-to-the-minute threat intelligence feeds combine to deliver rapid and precise threat detection. NovaCommand gives customers peace of mind with round-the-clock protection without a dedicated 24/7 cybersecurity team.

NovaCommand lets customers create granular playbooks for incident response automation. Customers can define specific actions in response to an attack. For example, to isolate a client with irregular traffic flows and cut off the connection.

Core Capabilities

World-class Network Detection & Response powered by AI, Machine Learning, and Threat Intelligence.

Cloud (completely hosted in the EU) or on-premise deployment.

Customizable playbooks to respond automatically to positive threat detections.
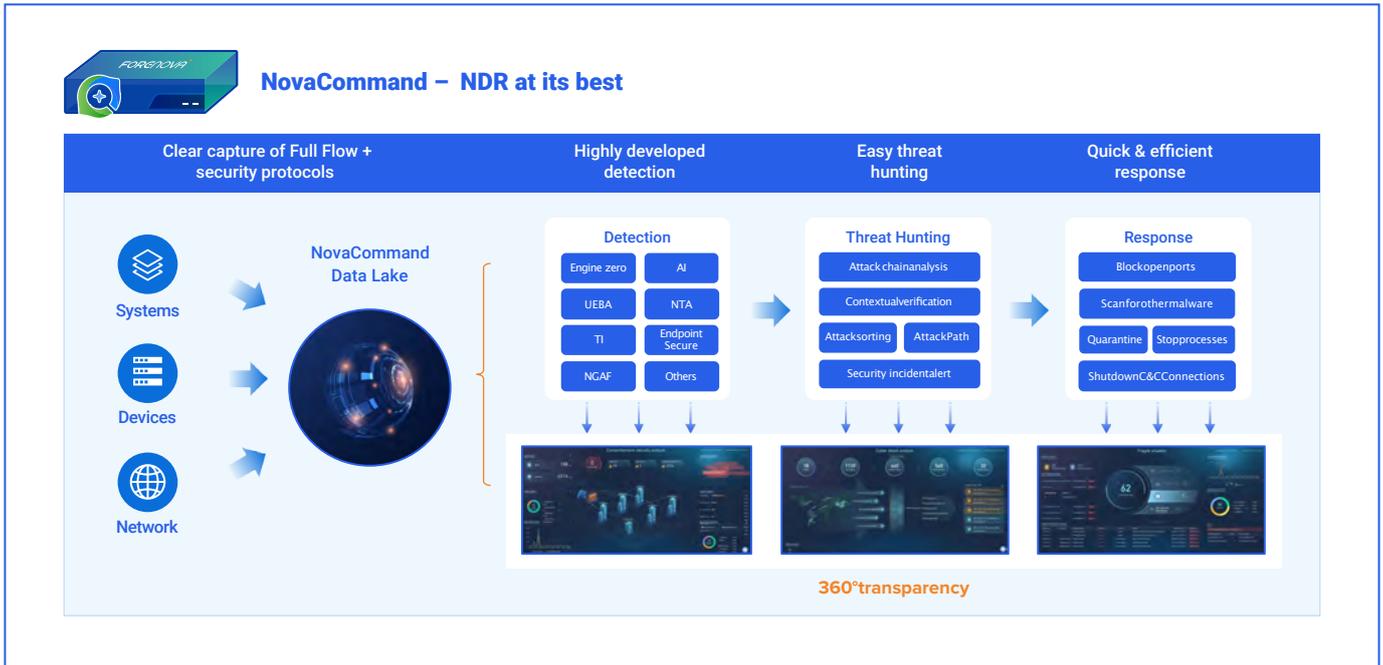
Customer Values

01
Detect cyber-attacks and respond to them without hiring an expensive specialist team.

02
Minimize cybercrime damage while ensuring the highest level of cyber resilience and compliance.

NovaCommand – NDR at its best

Clear capture of Full Flow + security protocols	Highly developed detection	Easy threat hunting	Quick & efficient response

Systems

Devices

Network

NovaCommand Data Lake

Detection
- Engine zero
- AI
- UEBA
- NTA
- TI
- Endpoint Secure
- NGAF
- Others

Threat Hunting
- Attack chain analysis
- Contextual verification
- Attack sorting
- Attack Path
- Security incident alert

Response
- Block open ports
- Scan for other malware
- Quarantine
- Stop processes
- Shutdown C&C Connections

360°transparency

Seamless 3rd-Party Integration

In a complex IT environment, every player in the IT infrastructure has to collaborate with the whole team. NovaCommand offers a RESTful API to integrate seamlessly into existing infrastructures.

Moreover, we are already integrated in major SIEM, firewall, and endpoint solutions as well as zero trust clients. NovaCommand can use the whole security toolset available at site, interacting with them by delivering and collecting data to enable global responses based on customer-defined playbook rules.

Other ForeNova Solutions

NovaMDR

- A professional managed detection & response solution for your network with 24/7 surveillance by dedicated cybersecurity specialists for fast alerting & response to cyberattacks.

NovaTA

- Let experts inspect your network and investigate threats with this service. Find any compromised devices with a full report and clear instructions.

SIEM	Firewall	Endpoint	Other
QRadar, ArcSight, splunk>, LEEF, CEF	paloalto, SOPHOS, FORTINET, Check Point, CISCO	McAfee, Bitdefender, SOPHOS, Symantec, kaspersky, TREND MICRO, F-Secure	macmon, vmware