innspark
NDR

REAL-TIME IN-DEPTH VISIBILITY

innspark.in/ndr

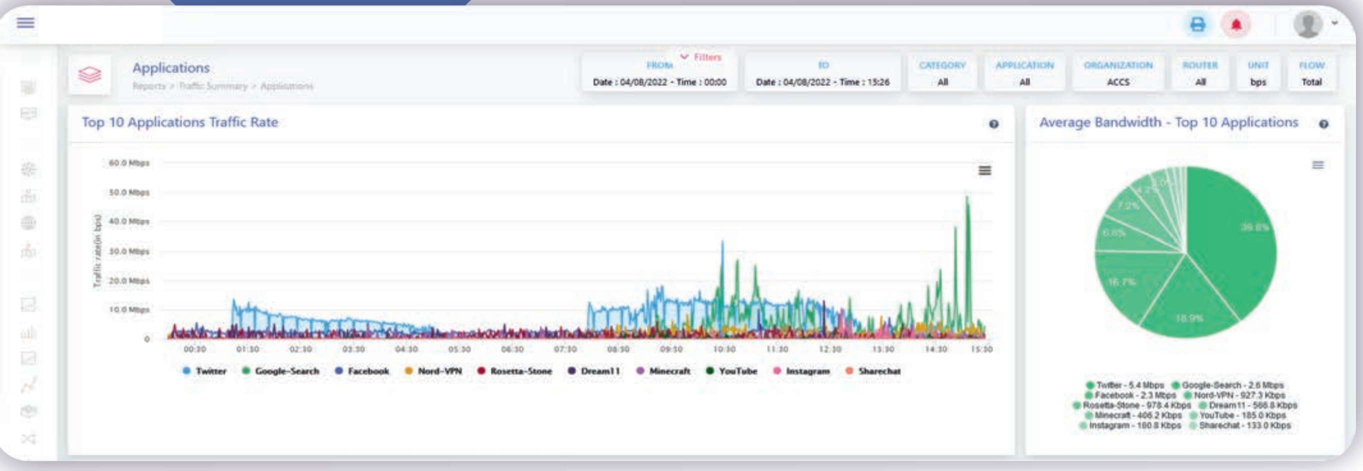
NETWORK DETECTION AND RESPONSE

Overview

Innspark NDR provides real-time in-depth visibility into each and every flow in and out of the organization network. The platform monitors North-South & East-West traffic and applies Machine Learning & Artificial Intelligence models to detect hidden threats and respond to them using automated response.

Deeper insights

Provides unparalleled visibility into the organization's traffic by Identification native application profiling. Innspark NDR platform profiles each flow to its respective application categories such as search engines, social media, media streaming, cloud storage and to applications such as Google, Facebook, Netflix etc.



Applications

Reports > Traffic Summary > Applications

Filters

FROM: Date : 04/08/2022 - Time : 00:00

TO: Date : 04/08/2022 - Time : 15:26

CATEGORY: All

APPLICATION: All

ORGANIZATION: ACCS

ROUTER: All

UNIT: bps

FLOW: Total

Top 10 Applications Traffic Rate

Average Bandwidth - Top 10 Applications

Anonymous traffic identification

Identifies the anonymous traffic through VPN, TOR, SOCKS Proxies, etc. HTTP Proxies and classifies them to provide increased visibility and context awareness.

Integrated enrichment

Native integration with curated Innspark Intelligence sources such as PDNS Intelligence, Geospatial Intelligence, WHOIS Intelligence, and Autonomous System Number (ASN) Intelligence.

Quicker response - SOAR

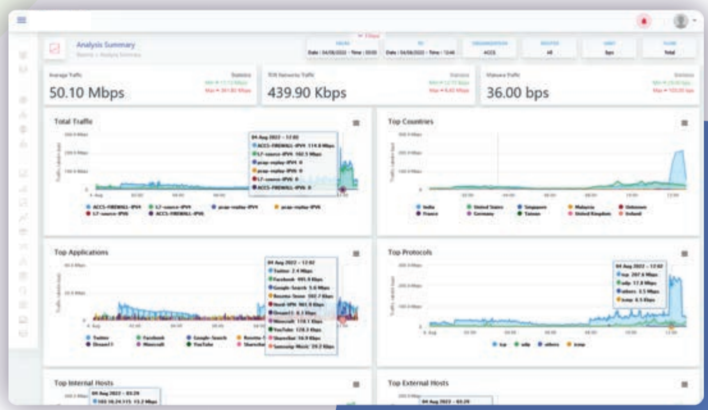
Automated responses to mitigate threats in real-time using predefined and customizable playbooks. It orchestrates the threat contamination workflow across the network by integrating with Firewalls, IPS, WAF, Routers, and other security products.

Faster forensics

Innspark NDR platform is built on Web-scale big data based architecture which retrieves network forensics data within sub-seconds. Granular level filters in the forensics search enables analysts to dig deeper.

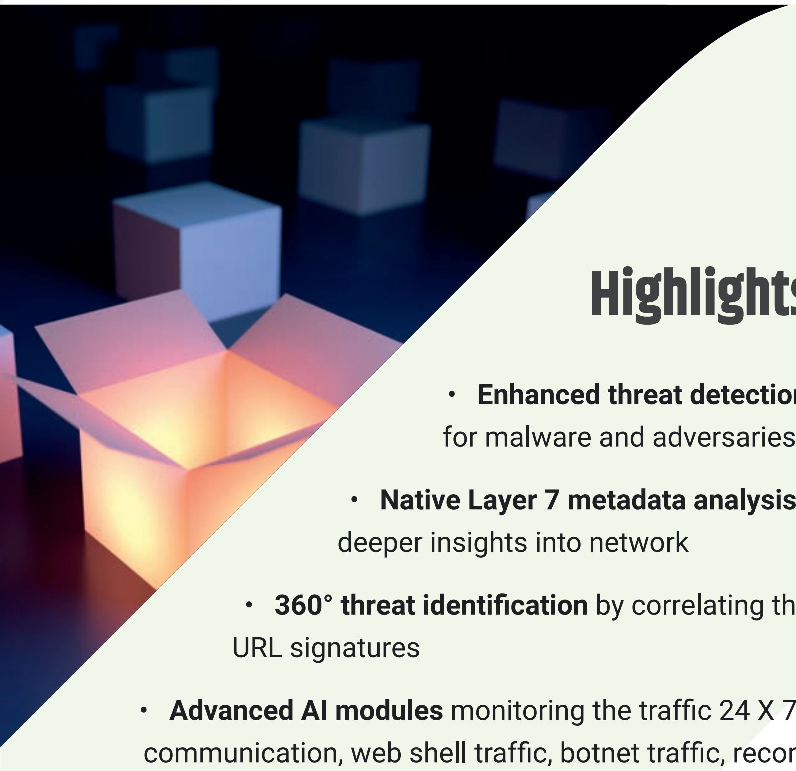
DDOS detection & response

Deep Learning based modules detect potential DDOS attacks on the networks. Innspark NDR detects SYN flood attack, DNS amplification attack, NTP amplification attack, Memcached amplification, and many more. Integrated SOAR playbooks respond to DDOS alerts in a flash.



Threat intelligence integration

Integration with external threat sources using standard formats like STIX, CSV, JSON, & TAXI. Native integration with Innspark Threat Intelligence (TI) feeds containing regularly updated TI signatures for a variety of malwares including botnets, ransomware, trojans, spyware and APT backdoors.



Highlights

- **Enhanced threat detection engines** powered by refined global TI leaves no gap for malware and adversaries
- **Native Layer 7 metadata analysis,** providing application wise traffic categorization and deeper insights into network
- **360° threat identification** by correlating the traffic with JA3/JA3S, FQDN, User-Agent, IP, Port, URL signatures
- **Advanced AI modules** monitoring the traffic 24 X 7 for detecting anomalous behavior such as C2C communication, web shell traffic, botnet traffic, reconnaissance port scanning and DDOS attacks
- **Automated response using SOAR** ensures that threats are mitigated in sub seconds
- **Provides contextual information** for all the flows by auto-enrichment and PDNS integration

Key features

- Managed entity profiling for monitoring specific entities
- Real-time traffic monitoring and statistics dashboards and visualizations for ease of operations
- Live services detection detects running service inside the organization
- Port scan detection powered by ML models identifies even the stealthiest reconnaissance scans from adversaries
- Supports offline network traffic analysis by uploading packet capture file
- Multi-tenant and role-based access control ensures data segregation among the analysts
- AI powered anomaly detection engines which identify sophisticated attacks and exploitation attempts
- Supports all formats of flows including Netflow V5, Netflow V9, IPFIX, sFlow, and Jflow
- Dedicated application bandwidth dashboards for each profiled application
- Supports blacklist monitoring and alerting
- Predefined & customizable report generation engines
- Supports integration with other security tools such as SIEM, UEBA, and EDR

About innspark

Innspark is a fast-growing deep tech solutions company. We provide next-generation products and services in Cybersecurity and Telematics. The Cybersecurity segment provides out-of-the-box solutions to detect and respond to sophisticated cyber incidents, threats, and attacks. The solutions are powered by advanced threat intelligence, Machine Learning, and Artificial Intelligence that provide deep visibility of the enterprise's security. The Telematics segment provides advanced location tracking devices, technologies, and software for any industry. The innovative telematics solutions help businesses with complete fleet visibility and better insight into every aspect of vehicles and personnel.

Our key capabilities include Cyber Security, Telematics, Large Scale Architecture, Deep Analysis, Reverse Engineering, Web-Scale Platforms, Threat Hunting, High-Performance Systems, Network Protocols & Communications, Graph Theory, and several others.

Please visit www.innspark.in for more information.

Talk to our security experts for demos

EMAIL US:

info@innspark.in

CALL US:

+91 476 2912 111 & 1800 2584 431 (Toll Free)

innspark.in