Datasheet

Blockbit NDR

NETWORK DETECTION & RESPONSE

Intelligence | **Visibility** | **Network Threat Response**

Blockbit NDR (Network Detection and Response) is an advanced solution that combines continuous network monitoring, behavioral analysis, and automated incident response. Built on the Blockbit Platform, it provides complete visibility into network traffic, enabling the detection of both known and unknown threats before they cause harm.

Its native integration with Blockbit CTI (Cyber Threat Intelligence) elevates detection and response capabilities, ensuring that Blockbit NDR is always up to date with the latest emerging threats, vulnerabilities, and attack tactics. This significantly enhances threat identification accuracy, reduces false positives, and accelerates incident response—keeping your company one step ahead of cybercriminals.

Blockbit NDR is the key to an efficient SOC, delivering total network visibility, intelligent threat detection, and real-time automated response. With integrated intelligence and advanced traffic analysis, your security team gains the power to anticipate, neutralize, and mitigate attacks before they have any impact.

Discover the key features of Blockbit NDR:

Continuous Network Traffic Analysis
Real-time monitoring of packets and metadata.

Behavior-Based Detection
Threat identification without relying on traditional signatures.

Native Integration with Blockbit CTI
Real-time threat intelligence for more accurate detection.

Machine Learning and Threat Intelligence
Advanced data correlation to minimize false positives.

Automated Incident Response
Rapid threat containment and mitigation.

Integration with SIEM, XDR, and SOAR
Event correlation for coordinated response.

Deployment Flexibility
Available as a hardware appliance, virtual appliance, and cloud-based solution.

About Blockbit

Blockbit is a leading cybersecurity provider, protecting thousands of companies and millions of users from digital threats and cyberattacks.

+5M corporate clients

+2MM protected users

Key Features

Traffic Monitoring and Analysis

- **Deep Packet Inspection (DPI):**
  Detailed inspection of network traffic, including encrypted packets.
- **Encrypted Traffic Analysis without Decryption**
  (Encrypted Traffic Analysis - ETA)
- **Intrusion Detection and Prevention (IPS):**
  Detailed network traffic inspection that detects and responds to attacks.
- **Threat Protection (ATP):**
  Advanced protection against malware and sophisticated attacks.
- **Cloud Sandbox:**
  Execution of suspicious files in an isolated environment.
- **NetFlow and Metadata Analysis:**
  Collection and correlation of traffic flows to detect anomalies.
- **Lateral Movement Detection:**
  Identification of suspicious communications within the network.
- **North-South and East-West Traffic Analysis:**
  Full visibility to detect internal and external threats.
- **Botnet Detection:**
  Monitoring to identify malicious communications.

Integration with SIEM, XDR and SOAR

Advanced Event Correlation	Indicators of Compromise (IoCs)	Incident Response Orchestration
Analysis of multiple sources to detect attack patterns.	Identification and rapid response to known threats.	Automation of security workflows.

Blockbit CTI

Cyber Threat Intelligence

Real-Time Correlation

Access to information on emerging threats and vulnerabilities.

Enhanced Detection

Reduction of false positives and greater accuracy in threat analysis.

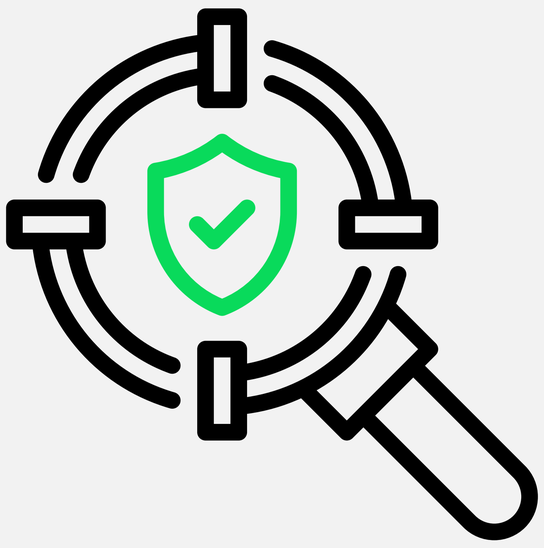
Proactive Prevention

Neutralization of attacks before they materialize.

Cyber Resilience

Continuous adaptation to new tactics and strategies of cybercriminals.

Forensics and Data Retention



Packet Capture (PCAP):
Traffic collection for forensic analysis.

Log Retention and Storage:
Detailed recording for auditing and compliance.

Customizable Reports:
Insights into threats and suspicious activities.

Flexible Deployment

Hardware Appliance

Models for different traffic volumes.

Virtual Appliance

Compatible with VMware, Hyper-V, Proxmox, and KVM.

Cloud Instance

Support for AWS, Azure, Google Cloud, Oracle Cloud and IBM.

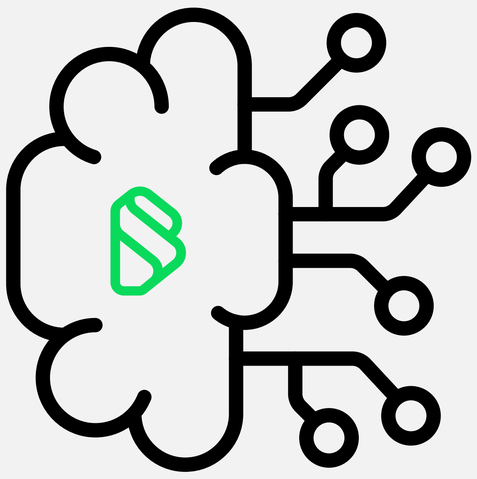
Performance and Technical Specifications

Model	Analysis Throughput (IMIX)	Analysis SSL/TLS	Simultaneous Events
BBX40	200 Mbps	150 Mbps	4M connections
BBX80	850 Mbps	700 Mbps	6M connections
BBX140	1.5 Gbps	1.2 Gbps	7.5M connections
BBX200	2.5 Gbps	1.3 Gbps	8.2M connections
BBX700	3.6 Gbps	2.2 Gbps	20M connections
BBX1500	6.5 Gbps	4.5 Gbps	22M connections
BBX3000	13 Gbps	10 Gbps	30M connections
BBX3600	20 Gbps	12 Gbps	45M connections
BBX4200	26 Gbps	14 Gbps	55M connections
BBX5000	40 Gbps	20 Gbps	70M connections

Anticipate threats and automate your defense with advanced intelligence

Blockbit NDR goes beyond threat monitoring and response—its native integration with Blockbit Cyber Threat Intelligence (CTI) provides continuous access to a global network of cyber threat intelligence. Through the analysis of millions of security events, machine learning, and advanced data correlation, it identifies emerging attack patterns and anticipates risks before they compromise your infrastructure.

With continuous network traffic monitoring, automated threat detection, and native integration with SIEM, XDR, and SOAR, Blockbit NDR strengthens your organization's security posture, ensuring full visibility, predictive analysis, and automated response against sophisticated cyberattacks.



- **Full Visibility and Behavioral Analysis**
- **Intelligent Threat Detection with Machine Learning**
- **Automated Response for Rapid Mitigation**
- **Event Correlation and Integration with XDR/SIEM**
- **Enhanced Protection with Global Intelligence from Blockbit CTI**

About Blockbit

With cutting-edge technologies and an advanced intelligence lab, **Blockbit** develops proprietary solutions to provide maximum protection for its clients, combining high quality and performance, always aligned with the latest global cybersecurity trends.

With Blockbit, it's easy to be **secure**