



COLLECT, ANALYZE, **ACT.**

NDR CYBERSECURITY PLATFORM



NDR



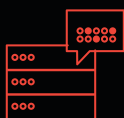
NTA



Vulnerabilities



Endpoint



XDR



Monitoring



BI & AI



Malware Analysis

redborder.com



RedBorder is an active network detection and response security management platform. It combines comprehensive network infrastructure information with intelligent intrusion probes to actively defend against intrusions. By compiling network analysis, intrusions, telemetry, vulnerabilities, assets, and email data, Redborder generates automatic policies to safeguard both users and the infrastructure.

Features	
Cybersecurity	• Incident automatic detection and response. • Detections: superpositions, ai anomalies, pattern base, behaviors. • Entangled correlations. • Reactive and proactive vulnerability & asset management. • Incident visualization, categorization, investigation. • Attack Investigation & Recovery. • Response with automations(playbooks) & integrations. • Multi threat intelligence source.
Network management/ performance	• Wired/less network infrastructure monitoring. • Telemetry, Observability performance management. • IT/OT network and hardware performance analysis. • Real time report and dashboard management. • Security Event Classification and Prioritization. • Dashboard, reports & personalization automation.
Deployment	• Quantum Security. • On premises, virtual, cloud. • In-line/off band. • Real time blocking capability. • High availability compatible. • Cluster configuration. • Multi-tenant. • Scalable.

Redborder follows a centralized processing layer (Manager) and a sensor layer (Probes). The Manager can be deployed fully on-premises or in the cloud, utilizing a clustered architecture that adapts and scales to your needs.

The sensor layer provides the data sent to the Manager. It consists of various network flow collectors, supports in-line or off-band deep packet inspection (DPI), and includes an API-based layer for seamless integration.