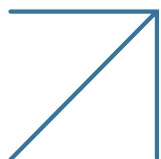# Management, Configuration & Attack Lifecycle – Unified

The Radware Cyber Controller is a unified solution for management, configuration and attack lifecycle. Radware Cyber Controller provides frictionless security, increased visibility and an improved user experience via multiple security operation dashboards for a unified view into attack lifecycle and mitigation analysis for both inline and out-of-path DDoS deployments. Cyber Controller provides network analytics with comprehensive visibility of traffic statistics during peacetime and attack, simplified management and configuration with unified visibility and control.

Rich User Experience and Visibility with Simple Management and Configuration

Robust Analytics
Provides insight into network behavior and assistance in identifying anomalies as they occur, during peacetime or under attack.

Advanced SecOps
Enabling faster and more intuitive loop-closure between attacks, active mitigations and mitigation refinement.

Advanced Protection Coverage
Innovative policy editor supporting new and enhanced protections, including connection PPS limit, HTTPS protection, SYN protection, signature protection, traffic filters, BDoS and more.

High Availability
Ensuring high availability of management and control systems with faster mitigation actions using side-by-side mitigation pane and monitoring dashboards.

Advanced SecOps

Security operations dashboards (SecOps), showing side by side, both attack information and mitigation actions within the same window, allowing the administrator to:

↗ Easily and instantly navigate between a variety of traffic dashboards

↗ View detailed detection events, policies applied and participating DefensePro devices

↗ Change and refine configurations for better attack mitigation

All while always staying on the same SecOps screen. Ultimately, those dashboards lead to faster and more intuitive loop-closure between attacks, active mitigations, and mitigation refinements.

Figure 1

Cyber Controller
SecOps
Dashboard
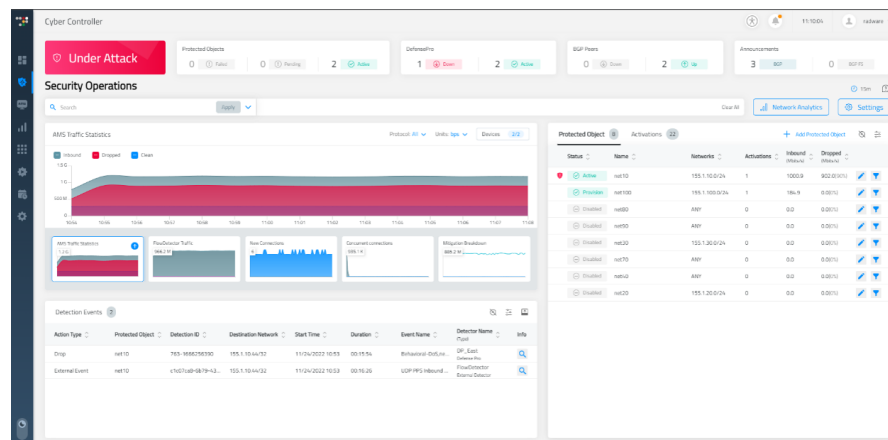
Cyber Controller Network Analytics

Network Analytics provide peacetime information, coupled with detailed attack-time analytics to provide Top-N parameters (top source or destination IPs, top source or destination ports, top protocols and locations from where your applications and services are being accessed. The dashboards provides a weekly trend of traffic to enable characterization of the network's DNA over time, identify anomalies as they show up and relate those to on-going attacks.

Figure 2

Cyber
Controller
Network
Analytics