DATASHEET

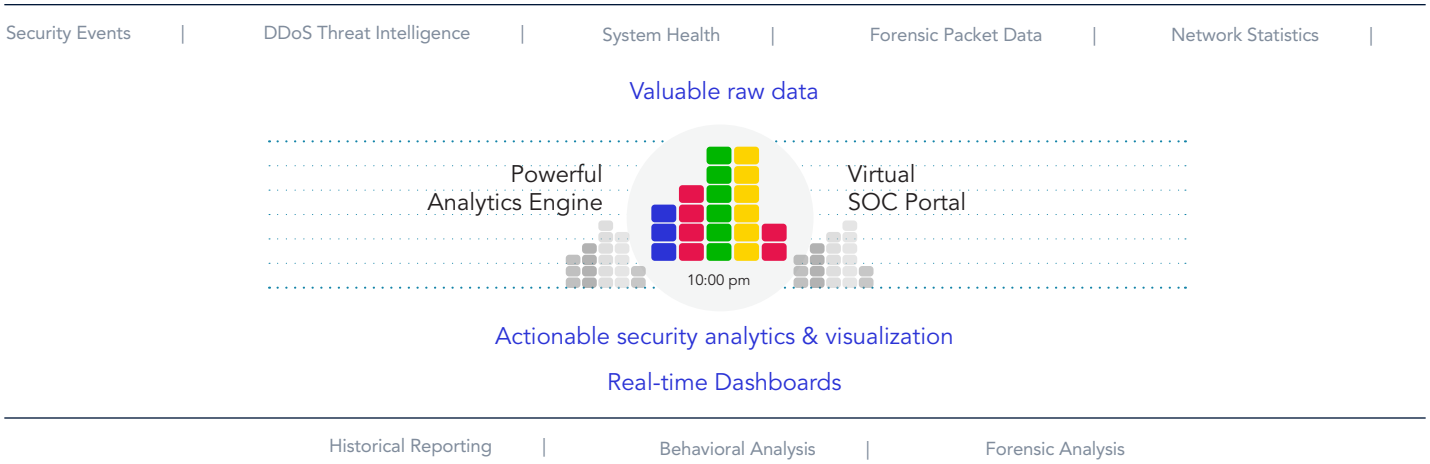
CORERO SECUREWATCH® ANALYTICS

COMPREHENSIVE DDOS ATTACK VISIBILITY

Corero SmartWall® SecureWatch® Analytics (SWA) solves a significant challenge facing many organizations; their inability to extract meaningful realtime information on DDoS attacks from volumes of security events.

Typically, only minimal visibility into these classes of security events is possible, and only to organizations with significant investments in detailed analytics tools and expert security staff. Security analysts are often left reacting to DDoS threats after the damage has already been done.

SecureWatch Analytics is a powerful security tool that delivers comprehensive visibility into DDoS attacks with easy-to-read security dashboards. Organizations benefit from the DDoS focused granular security intelligence which can enhance their broader security event monitoring practices.
The multi-user web UI of the SecureWatch Analytics application delivers unprecedented DDoS visibility and actionable intelligence, before, during, and after the attack, without requiring specialist security analysts to sift through reams of unintelligible log data. Traffic information is stored for as long as needed, drastically reducing the time it takes to identify an issue and saving hours of manual labor.



SecureWatch Analytics is included as a key component of Corero's SmartWall® real-time, automatic, DDoS defense solutions. It transforms DDoS tailored security feeds from SmartWall deployments into autonomic defense actions and dashboards of actionable security intelligence, exposing:

» Volumetric DDoS - reflection, amplification, & flooding attacks
» Targeted resource exhaustion attacks

» Under the radar non-saturating attacks » Victim servers, ports, and services » Malicious IP addresses and botnets

Empowered by this enhanced visibility, organizations can utilize SecureWatch Analytics as a single pane of glass to visualize DDoS attacks and help ensure uninterrupted business continuity for their Internet facing services.

Key Benefits

Comprehensive Visibility
Forensic-level visibility and analysis of DDoS; before, during and after attacks, via easy to use dashboards of actionable intelligence that minimize trouble-shooting time.

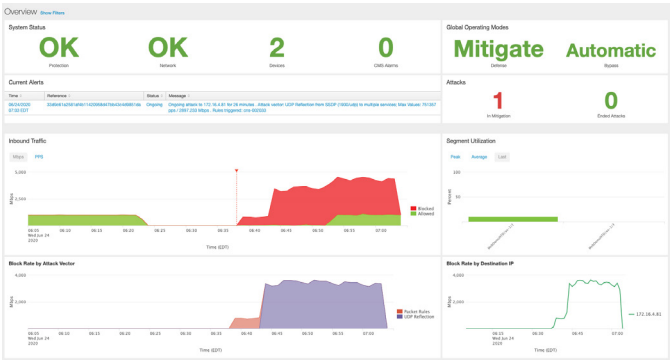
Automatic & Accurate
Accurate automatic mitigation delivers lowest TCO and enables your IT and security teams to spend more time defending.

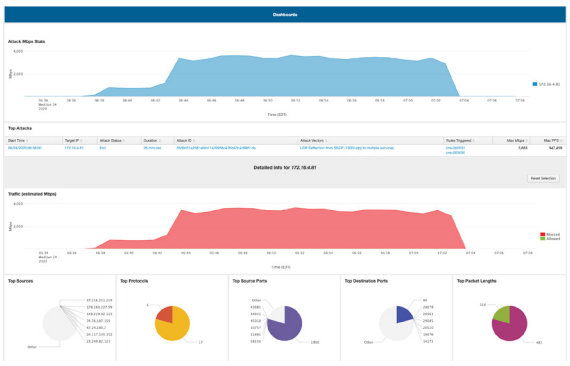
Service Enablement
Comprehensive visibility with reporting and alerting for clear, actionable, intelligence on the DDoS attack activity across the network.

Multi-User NOC/SOC Dashboards

SecureWatch Analytics (SWA) is easily accessible via any browser and delivers real-time and historical dashboard views that summarize network and DDoS activity across the organization. Analysts can view thesedash-boards at a site by site level or in an aggregate view that provides a consolidated security picture.

SWA enables analysts to quickly understand the size and profile of each attack, in realtime, including the specific vectors used at any point in time. It also delivers, in a single pane of glass view, real-time monitoring and reporting on the overall SmartWall system health and protection status.



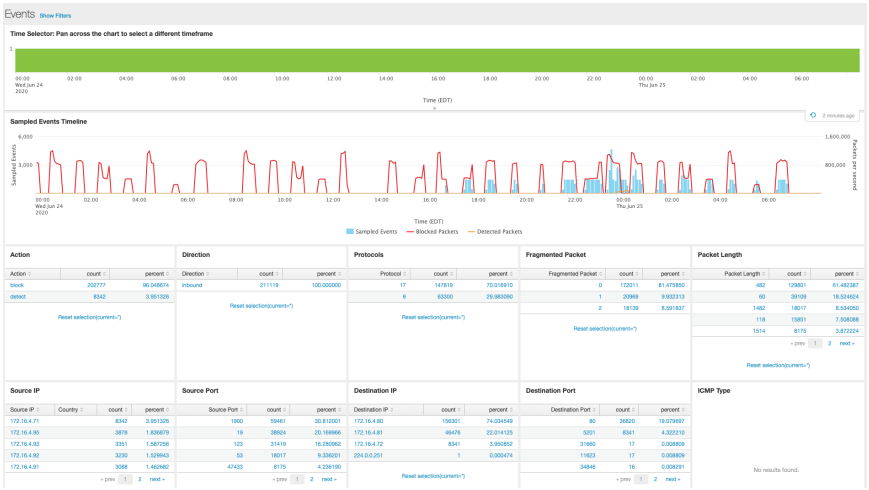


Drill-Down on Attacks

SecureWatch Analytics displays a statistical view of the inbound traffic activity using IP sFlow samples collected from the Corero SmartWall Threat Defense System. These top charts contain reports about; source and destination IPs and Ports, Protocols, TTL (time-to-live), Packet lengths and Fragments. These top reports can provide additional data to analyze and determine if security policy changes or tuning is required.

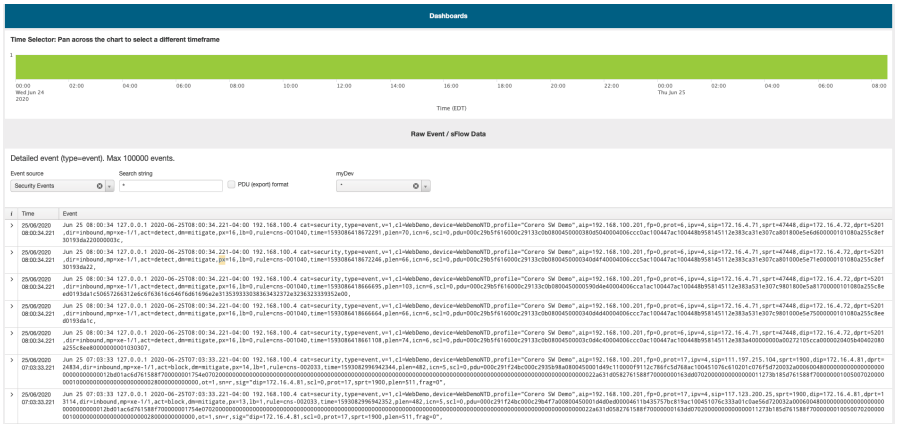
Detailed Traffic Statistics

It is critical to know the details when you are under attack. SecureWatch Analytics gives you the ability to immediately drill down to see the offending addresses, ports, protocols and other key insight into the attackers targeting your infrastructure. These can then easily be reported on, or incorporated into ACLs and blacklists to permanently or temporarily block access for devices with no legitimate reason to be accessing your network.



Packet-Level Forensics

SecureWatch Analytics archives security event data down to the power distribution unit (PDU) level, enabling forensic analysis of ongoing and past threats for greater intelligence and compliance reporting on security activity. Authorized Users can analyze event data based on preset timescales (e.g. last day, week, or month) or select a very specific timeframe when investigating past events, for example.



Events include all the metadata extracted by the SmartWall system as well as the first 128 bytes of the packet which the attack comprised of. In addition, PDU data from security and sFlow events can be extracted to a file for import to third-party applications, such as Wireshark for further forensic analysis.

Open Integration

SecureWatch Analytics (SWA) leverages the APIs and JSON formatted syslog event feeds of SmartWall's open architecture to deliver forensic-level attack analysis and closed-loop autonomic protection. It is built on top of a self-contained Splunk instance, which is included with every SmartWall soliution, to deliver its powerful, flexible and easily customisable attack. analysis and reporting.

Users with their own Splunk Enteprise instance can leverage that directly by running the SWA application on it and consuming the SmartWall feeds directly. Users with alternate an SIEM or other security platforms can directly consume the SmartWall JSON formatted syslog feed which delivers all the same detailed information which is available from SWA.

Technical Specifications

Management		
Web-Based GUI	**Programmatic API**	**Secure Authentication**
HTTPS Access through Portal Login Page	JSON-Based REST	Role-Based Access via LDAP

Physical Environment	
Hypervisors	**Minimum Requirements**
KVM running on Redhat Enterprise 7+, CentOS 7+ or Ubuntu 16.04+ VMware ESXi 6.5+	12 Cores, 12GB Memory, 400GB Disk

Learn more About SecureWatch Analytics

SecureWatch Analytics was developed with the deep security experience and knowledge of Corero's security analysts that deliver our market leading SecureWatch service. SecureWatch Managed is a comprehensive suite of DDoS configuration optimization, monitoring and response services. As a trusted advisor, Corero extends this security expertise to our customers and partners to better defend against cyber-crime.

To learn more, please visit https://www.corero.com/product/managed-ddosprotection-services/ or contact us at info@corero.com.

About Corero Network Security

Corero is the leader in real-time, high-performance, automatic DDoS defense solutions. Enterprises, Service Providers, Hosting & Co-Location Providers, Edge Providers and the MSSP/MSP's across the globe increasingly rely on Corero's award winning DDoS solutions. Our SmartWall solutions are the highest performing and most accurate in the industry, delivering the most automatic coverage, at scale, with the lowest total cost of ownership.

This, industry leading technology delivers scalable protection capabilities against DDoS attacks in the most complex environments, without the downtime associated with other solutions, while enabling a more cost-effective economic model than previously available. For more information, visit www.corero.com

US HEADQUARTERS info@corero.com **EMEA HEADQUARTERS** info_uk@corero.com

corero.com