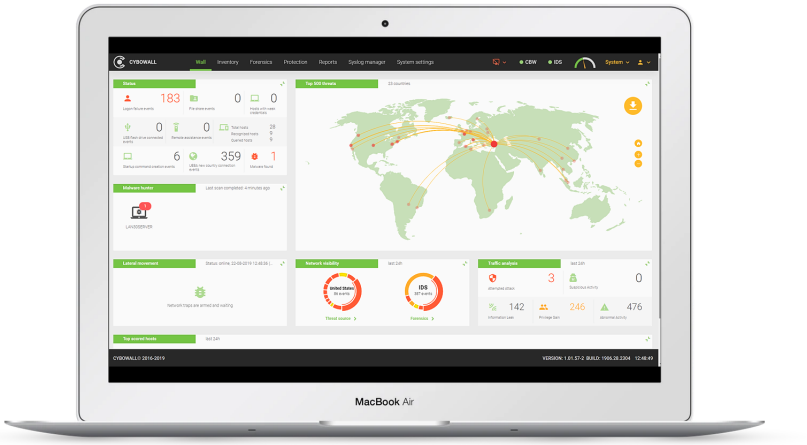
Cybowall™ Net-Breach

A SINGLE SOLUTION FOR ORGANIZATION BREACH DETECTION NEEDS



Cybowall Net-Breach provides central monitoring interface for network and host breach detection from C2C communication to lateral movement to host events.

SOLUTION OVERVIEW

Cybowall Net-Breach is a non-intrusive, agentless solution that provides advanced breach detection with continuous monitoring of your network across all protocols and extending to all endpoints. Cybowall Net-Breach protects the network , detecting and reacting to threats as they arise.

Cybowall enables organizations to:

- Quickly detect active breaches
- Identify and minimize response time
- Manage and report on compliance (GDPR, PCI-DSS, ISO etc.)
- Record and analyze all events and incidents within the network for further investigation

Cybowall Net-Breach combines multiple cybersecurity tools and capabilities in one solution - securing networks of all sizes and providing unified defense against a continuously evolving threat

SOLUTION BENEFITS

- **Stop Endpoint Tampering and Malware**: Leverage network and endpoint detection of Advanced Persistent Threats
- **Detect Lateral Movement**: Trap attackers that have already breached perimeter defenses
- **Detect Active Breaches**: Discover network breaches quickly to reduce damaging effects
- **Find Network Anomalies Faster** : Cybowall Net-Breach AI system has been proven successful at detecting anomalies which are the first sign of a network breach.
- **Monitors File and Folder Access:** Monitors files, folders, system configuration files, content files.
- **Meet Compliance Requirements**: Adhere to compliance standards; GDPR, ISO, PCI-DSS, HIPAA etc.
- **Visibility Into Connected Devices** : Control over network security posture, management of risk to the network and company data, and Internet of Things manageability.

SOLUTION FEATURES

Network	• **IDS** Uncover Unwanted Or Malicious Traffic • **UEBA** command & control exploits and network anomalies based on remote ip and service access , network utilization anomalies (packets and data). • **Honeypots** Identify lateral movement via network traps aim at detecting a network scan
Host	• **Host IDS** Detect brute force attacks on network devices , Data stick connection / Volume creation , start up command or logon / screen lock and unlock. • **Malware Hunter**: Identify malicious files and where they reside in the network server and hosts
User	• **Host IDS** Detect compromised users brute force attacks or logon failure and screen lock and unlock. • **File Integrity Monitoring** Monitors files, folders, system configuration files, content files

TECHNICAL OVERVIEW

Cybowall Net-Breach solution collects and analyzes information from both endpoint and network events. With an Intrusion Detection that sits out of line and takes a copy of all network and internal traffic via TAP/Port Mirroring, Cybowall functions as an IDS at the network level. Cybowall also utilizes an Agentless Scan that leverages, amongst other technologies, WMI capabilities to collect detailed forensic data and correlate it with known Indicators of Compromise (IOC). By centrally aggregating network-wide activity. Deploying Network Trap decoy technology, and connected directly to the network's core switch via SNMP, Cybowall enables continuous network visibility and effective breach detection.