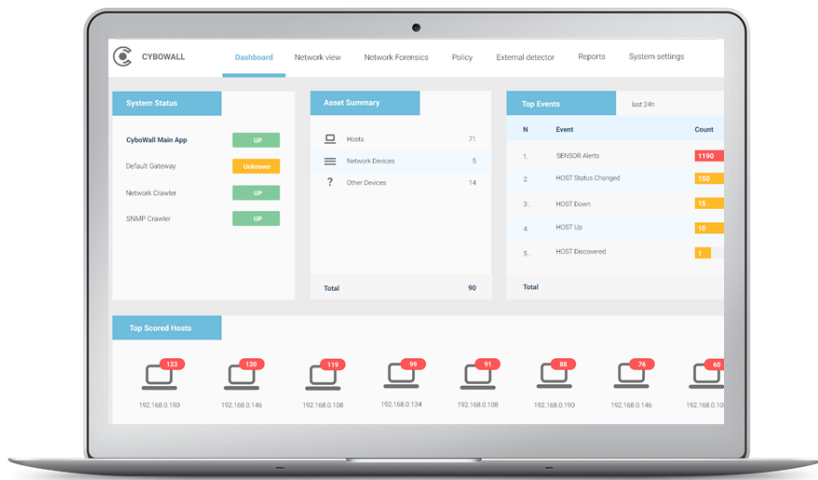


Cybowall™

AGENTLESS, MULTI-VECTOR THREAT DETECTION AND RESPONSE



Cybowall central monitoring interface for total network visibility and remediation

SOLUTION OVERVIEW

Cybowall is a non-intrusive, agentless solution that provides complete and continuous monitoring of your network across all protocols and extending to all endpoints. Cybowall protects your network in real time; detecting and reacting to threats as they arise. Reduce risks to your organization by gaining full visibility into your network. Cybowall enables organizations to:







- Quickly detect potential vulnerabilities and active breaches
- Automatically respond to threats as they are discovered
- Manage and report on compliance (GDPR, PCI-DSS, ISO etc.)
- Record and analyze all events and incidents within the network for further investigation

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

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
- **Map Network Assets:** Increase visibility with a map of all endpoints connected to your network to gain insight into your environment
- **Identify Vulnerabilities:** Stay informed of vulnerabilities for patch deployment prioritization
- **Meet Compliance Requirements:** Adhere to compliance standards; PCI-DSS, HIPAA, HITECH, GDPR, ISO etc.
- **Automate Responses:** Implement automated response policies without intervention by a System Administrator/CISO/SOC, including; endpoint quarantine, port shutdown, stopping a suspicious application/process on an individual endpoint

SOLUTION FEATURES

 Asset Mapping	Continuously updated list of all endpoints, including port profiles and activities
 Intrusion Detection	Full inbound and outbound network traffic visibility without causing interference
 SIEM	Log management, event management, event correlation and reporting to help identify policy violations and enable response procedures
 Network Traps	Enable insight into lateral movement between endpoints and detect threats originating within the network by serving as a trip wire for active attacks
 Vulnerability Assessment	Monitor business assets and identify vulnerable systems inside the network, including risk level, for patch deployment prioritization
 Automated Response	Policy-based responses initiated according to assigned activity/risk factor scores, enabling containment of real time attacks

TECHNICAL OVERVIEW

The Cybowall solution collects and analyzes information on both endpoint and network events. With a Sensor 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, Cybowall mines IOC data such as CVE, file hash, DNS, URL, hostnames, IP addresses, domains, URI and file paths. Deploying Network Trap decoy technology, and connected directly to the network's core switch via SNMP, Cybowall enables effective, policy-based automated responses.

