

## Cybowall™

A SINGLE PLATFORM FOR ORGANIZATION INTERNAL SECURITY NEEDS



Cybowall central monitoring interface for total network visibility and reporting

### 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, 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 active breaches
- Identify and minimize potential vulnerabilities
- 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
- **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
- **Detect Lateral Movement:** Trap attackers that have already breached perimeter defenses
- **Detect Active Breaches:** Discover network breaches quickly to reduce damaging effects
- **Meet Compliance Requirements:** Adhere to compliance standards; GDPR, ISO, PCI-DSS, HIPAA etc.

## SOLUTION FEATURES

 <p>Before Attack</p>	<ul style="list-style-type: none"> <li>• <b>Vulnerability Management:</b> Monitor business assets and identify vulnerable systems ,applications and services inside the network, including risk level ( Anti-virus, Windows updates , Firewall... ) for patch deployment prioritization.</li> <li>• <b>Default/Weak Passwords:</b> Pinpoint and change default/weak passwords to reduce risks</li> <li>• <b>Asset Mapping:</b> Dynamic asset map of all endpoints, including port profiles and activities</li> </ul>
 <p>During Attack</p>	<ul style="list-style-type: none"> <li>• <b>Breach Detection :</b> Uncover Unwanted Or Malicious Traffic (IDS) ,Identify lateral movement (Honeypots), brute force attacks, privilege escalation (HIDS), ransomware, command &amp; control exploits and network anomalies (UEBA)</li> <li>• <b>File Integrity Monitoring &amp; Malware Hunting :</b> Protect Your Sensitive Information from Unauthorized Access and Malware Infection agentless (Desktop &amp; Servers)</li> </ul>
 <p>After Attack</p>	<ul style="list-style-type: none"> <li>• <b>SIEM Capabilities:</b> Log management (Syslog to Cybowall), event correlation and reporting to help identify policy violations and forward to external SIEM (Syslog CEF).</li> <li>• <b>Reports:</b> Meet Compliance Requirements by Software &amp; Device Inventory, Vulnerability (CVE) , Risk and Executive Summary reports.</li> </ul>

## 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 continuous network visibility and effective breach detection.

