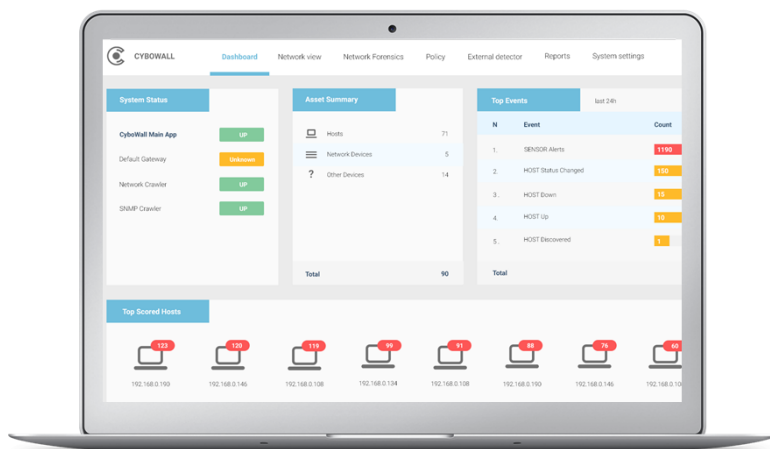


Cybowall™

ERKENNUNG VON SICHERHEITSVERSTÖßEN, VERWALTUNG VON NETZWERK-SICHTBARKEIT UND SICHERHEITSLÜCKEN



Zentrales Cybowall-Überwachungsinterface für vollständige Netzwerksichtbarkeit und Berichterstattung

LÖSUNGSÜBERSICHT

Cybowall ist eine eingriffsfreie, agentenlose Lösung, die eine vollständige, kontinuierliche Überwachung Ihres Netzwerks über alle Protokolle hinweg ermöglicht und bis an alle Endpunkte reicht. Cybowall schützt Ihr Netzwerk in Echtzeit, indem es alle akuten Sicherheitsbedrohungen direkt erkennt und darauf reagiert. **Reduzieren Sie die Risiken Ihres Unternehmens, indem Sie vollständigen Einblick in Ihr gesamtes Netzwerk erhalten.** Mit Cybowall können Unternehmen:

- Aktive Sicherheitsverstöße schnell entdecken
- Potentielle Schwachstellen erkennen und minimieren
- Vorschriften einhalten und entsprechend Bericht erstatten (DSGVO, PCI-DSS, ISO etc.)
- Alle Ereignisse und Zwischenfälle im Netzwerk für weitere Untersuchungen aufzeichnen und analysieren

Cybowall kombiniert mehrere Cybersecurity-Tools und Funktionen in einer Lösung und ist damit in der Lage, Netzwerke jeglicher Größe zu sichern und eine einheitliche Verteidigung gegen die sich ständig weiterentwickelnde Bedrohungswelt zu bieten.

VORTEILE UNSERER LÖSUNG

- **Manipulationen an Endpunkten und Probleme mit Malware stoppen:** Nutzen Sie die Netzwerk- und Endpunkt-Erkennung des „Advanced Persistent Threats“-Systems
- **Netzwerkressourcen aufzeichnen:** Steigern Sie die Sichtbarkeit mit einer Karte aller mit Ihrem Netzwerk verbundener Endpunkte, um mehr über Ihre Umgebung zu erfahren
- **Schwachstellen erkennen:** Bleiben Sie über Schwachstellen auf dem Laufenden, um zu wissen, welchen Patches Priorität eingeräumt werden soll
- **Erkennung lateraler Bewegungen:** Sperren Sie Angreifer aus, die Ihre Sicherheitssysteme bereits durchbrochen haben
- **Erkennung von aktiven Sicherheitsverstößen:** Decken Sie Netzwerkangriffe schnellstmöglich auf und reduzieren Sie damit schädigende Auswirkungen
- **Einhaltung regulatorischer Bestimmungen:** Entsprechen Sie regulatorischen Standards wie DSGVO, ISO, PCI-DSS, HIPAA etc.

LÖSUNGSFUNKTIONEN



Erkennung von Eindringlingen

- **Erkennung von Eindringlingen:** Erkennung von Sicherheitsverstößen ohne Netzwerkinterferenz
- **Netzwerk-Fallen:** Einblicke in laterale Bewegungen zwischen Endpunkten und Erkennung von Bedrohungen durch „Fallstrick“-System für akute Angriffe
- **Network Forensics:** Entdecken und analysieren Sie die Quelle von Security Attacks und Vorfällen



Netzwerk-Sichtbarkeit

- **Asset Mapping:** Dynamische Asset Map aller Endpunkte, einschließlich Port-Profile und Aktivitäten
- **WMI:** Nutzung von WMI und kontinuierlichen Endpunkt-Scans für vollständige Netzwerksichtbarkeit
- **SIEM:** Log-Management, Ereignis-Management, Ereignis-Korrelationsabgleich und Berichterstattung, um Verstöße gegen Richtlinien zu melden und entsprechende Reaktionen zu aktivieren



Verwaltung von Schwachstellen

- **Schwachstellen-Prüfung:** Überwachung von Geschäftsanlagen und Erkennung anfälliger Systeme innerhalb des Netzwerkes, einschließlich Risikolevel, zur Einsatz-Priorisierung von Patches
- **Standard-Passworte:** Feststellung und Änderung von Standard-Passworten zur Verringerung von Sicherheitsrisiken
- **Malware-Jäger:** Erkennung bösartiger Dateien und deren Lokalisierung im Netzwerk

TECHNISCHE ÜBERSICHT

Die Cybowall-Lösung sammelt und analysiert Informationen zu Endpunkt- sowie Netzwerkereignissen. Mit einem externen Sensor, der eine Kopie des gesamten Netzwerktraffics sowie internen Traffics per TAP/Port Mirroring anfertigt, agiert Cybowall auf Netzwerkebene als IDS. Außerdem nutzt Cybowall einen „Agentless Scan“, welcher neben anderen Technologien WMI-Funktionen nutzt, um detaillierte forensische Daten zu sammeln und mit bekannten Hinweisen auf Sicherheitslücken (Indicators of Compromise - IOC) abzugleichen. Durch die zentrale Erfassung aller Netzwerktätigkeiten ermittelt Cybowall IOC-Daten wie CVE, File Hash, DNS, URL, Hostnamen, IP-Adressen, URI und Dateipfade. Mit der „Network Trap“ - Locktechnologie sowie einem direkten Anschluss an den Network Core Switch per SNMP, ermöglicht Ihnen Cybowall eine kontinuierliche Netzwerksichtbarkeit und effektive Angriffserkennung.

