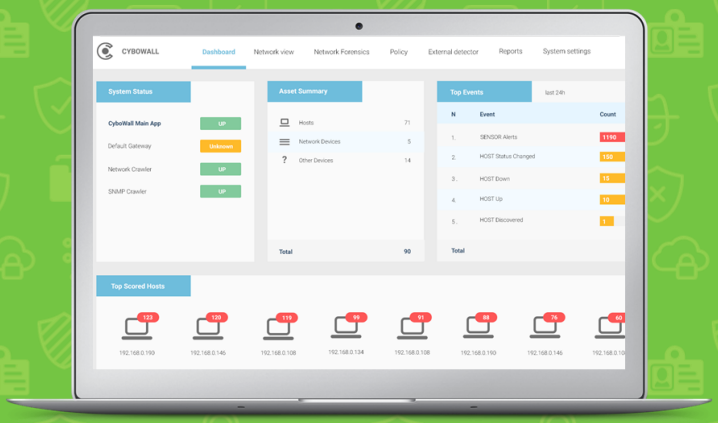
CYBONET

GDPR COMPLIANCE AND CYBONET'S CYBOWALL



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 active breaches and identify and minimize potential vulnerabilities. It aids compliance management and reporting, and records and analyzes 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.

GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is an EU wide regulation which will be enforced from May 2018 to strengthen data security and privacy protection for individuals. The scope of the GDPR is wide ranging and will require affected organizations to make far -reaching operational changes. This document will focus on some of the key principles of the GDPR and how they impact security and compliance teams. As this is a huge body of legislation, we will concentrate on a few specific areas to enable your organization as a whole, and your security, communications and compliance specialists in particular, to prepare for the upcoming May 2018 deadline.

SOLUTION FEATURES

Network Visibility

- **Asset Mapping**: Dynamic asset map of all endpoints, including port profiles and activities
- **WMI**: Leverage WMI and continuous endpoint scanning for full network visibility
- **SIEM Capabilities**: Log management, event management, event correlation and reporting to help identify policy violations and enable response procedures

Vulnerability Management

- **Vulnerability Assessment**: Monitor business assets and identify vulnerable systems inside the network, including risk level, for patch deployment prioritization
- **Default/Weak Passwords**: Pinpoint and change default/weak passwords to reduce risks
- **Malware Hunter**: Identify malicious files and where they reside in the network

Breach Detection

- **Intrusion Detection**: Breach detection capabilities without network interference
- **Network Traps**: Insight into lateral movement between endpoints and detects threats by serving as a trip wire for active attacks
- **Network Forensics**: Discover and analyze the source of security attacks and incidents

TECHNICAL SOLUTION 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.

GDPR TERRITORIAL SCOPE AND APPLICATION

The GDPR introduces a uniform data protection law across Europe, replacing the outgoing EU Data Protection Directive 95/46/EC and local laws such as the UK's Data Protection Act, 1998, and the German Bundesdatenschutzgesetz (BDSG). The GDPR aims to update and align existing data protection legislation, making EU privacy and data laws more relevant to the digital age by addressing gaps and encouraging transparency to support the rights of individuals.

The GDPR will be automatically apply in all EU member states as a single law, with no need to implement legislation in individual countries, and will be directly enforceable from 25 May 2018. In addition to all EU member states, the GDPR affects any organization that does business with an EU organization or individual. Non-EU organizations that collect and process European citizens' personal data will also need to comply with the new law and certify that their processes meet EU data privacy standards.

KEY CONSIDERATIONS OF GDPR

Financial Penalties

The new regulatory environment includes severe penalties for serious violations, with fines of up to €20M or 4% of an organization's global annual revenue, whichever is higher.

Expanded Definition of Personal Data

The GDPR has gone to great lengths in expanding the definition of personal data to any information related to an identified or identifiable person; the 'data subject'. Direct or indirect identification is possible by reference to an identifier such as a name, identification number, location data, online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

This could include data not previously viewed as personal, for example: IP addresses, application user IDs, GPS data, cookies, unique mobile device identifiers (UDID) etc.

Broad Territorial Scope

Beyond applying to EU member countries, organizations based outside of the EU that offer goods or services to EU data subjects are also covered by the regulation.

Requirement for Best Practice Frameworks

Information security controls: "technical and organizational measures" is a phrase used multiple times in the GDPR, and may necessitate controllers employing established industry or security best practice frameworks, such as ISO and PCI-DSS, which enable professionals to create consistent, repeatable processes and to implement controls that are generally accepted by the information security community.

TWO KEY ROLES DEFINED BY GDPR

The GDPR refers to two specific roles within an organization called Data Controllers and Data Processors, and places on them specific legal obligations.

Data Controller refers to the individual, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data within an organization.

Data Processor refers to the individual, public authority, agency or other body which processes personal data on behalf of the Data Controller.

GDPR REQUIREMENTS	CYBOWALL FEATURES	CYBOWALL BENEFITS
Article 30 - Records of Processing **Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility** Tips: ♦ Obtaining oversight and understanding how data flows through the organization is key to being able to secure, analyze and report on data ♦ Monitor all system and network activity, and include all data stored and processed, including on the cloud	▪ SIEM	• Cybowall's Security Information and Event Management (SIEM) and log management capabilities allow for monitoring of user and network activity and the identification of suspicious and malicious behavior • Multi-vector solution enables event correlation and analysis, alerts, incident response and reporting, with full coverage of endpoints; desktops, laptops, servers, routers, smartphones, tablets, wired/wireless LANs, printers, IoT devices - cameras, healthcare, manufacturing, POS etc
Article 32 - Security of Processing **The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk** Tips: ♦ Ensure ongoing confidentiality, integrity, and availability of data processing systems and services by reducing vulnerabilities and securing assets to help decrease risk ♦ Identify weaknesses that could be exploited and apply more stringent controls based on a complete inventory of assets that store or process sensitive data	▪ Asset Mapping ▪ Vulnerability Assessment	• Asset mapping increases network visibility by providing a continuously updated inventory of all endpoints, including port profiles and activities. It allows for a holistic view of an organization's system configuration and security posture • Integrated vulnerability assessment allows for a comprehensive analysis and prioritization of risks by collecting detailed forensic data and correlating it with known Indicators of Compromise (IOC). It identifies vulnerabilities in the network via endpoint scanning, and can pinpoint the severity of the vulnerability; facilitates auditor reviews and assessments and patch management prioritization
Articles 33 & 34 - Notification of Personal Data Breach (to Supervisory Authority and Personal Data Subject) **In the case of a personal data breach, the controller shall without undue delay… notify the personal data breach to the supervisory authority** Tips: ♦ Implement threat detection controls to identify immediately if a breach occurs; the regulation requires the relevant data protection authority to be notified "without undue delay" and within 72 hours of detection ♦ Continuous monitoring of network traffic for rapid incident investigation and response; organizations must demonstrate how they propose to address the breach, including "measures to mitigate its possible adverse effects"	▪ Intrusion Detection (IDS) ▪ Network Traps ▪ SIEM	• Intrusion detection continuous monitoring of network and endpoints ensure full inbound and outbound network traffic visibility to quickly identify breaches, without causing interference to network traffic • Network traps enable insight into lateral movement between endpoints and detect threats and data breaches within the network by serving as a trip wire for active attacks, enabling timely discovery • Optimized monitoring and breach detection via an intuitive user interface allows maximum visibility of a data breach, including discrepancies and anomalous behavior. Integrated reporting facilitates audit reviews