

Overview

With the advent of new business technologies and evolving Internet threats, organizations are deploying an increasing number of solutions and devices to ensure security and business continuity. This includes firewalls, content filtering systems, unified threat management solutions, routers, servers, applications, operating systems and more which generate a vast amount of logs.

Cyberoam iView Open Source Logging and Reporting Solution

Cyberoam iView is an open source logging and reporting solution that provides organizations with visibility into their networks across multiple devices for high levels of security, data confidentiality while meeting the requirements of regulatory compliance.

Enabling centralized reporting from multiple devices across geographical locations, Cyberoam iView offers a single view of the entire organization's activity. This allows organizations not just to view information across hundreds of users, applications and protocols, it also helps them correlate the information, giving them a comprehensive view of network activity.

Security Reporting

With Cyberoam iView, organizations receive logs and reports related to intrusions, attacks, spam and blocked attempts, both internal and external, enabling them to take rapid action throughout their network anywhere in the world.

Identity-based Reports

Cyberoam iView offers reports based on the user identity allowing organizations to see "Who is doing What" anywhere in the network. Given the criticality of insider threats in network security and data confidentiality, these reports give an instant view of a user profile through indepth user identity-based reporting across applications, protocols and multiple devices and solutions, allowing organizations to take preventive measures.

Regulatory Compliance

Cyberoam iView's user identity-based drill down reports form a critical element in enabling organizations to meet the access control, audit and forensic requirements of regulatory compliances like HIPAA, GLBA, SOX, PCI-DSS, CIPA, BECTA and others.