User Access Auditing

THE PROBLEM OVERVIEW

- Organizations are unable to properly monitor the login and logout activity of their employees
- Lack of login and logout activity makes regulatory and policy compliance challenging
- Some user access technologies lack the ability to set policies by group or notify an administrator when a policy is violated
- Manual coordination of user access information can consume significant time and manpower

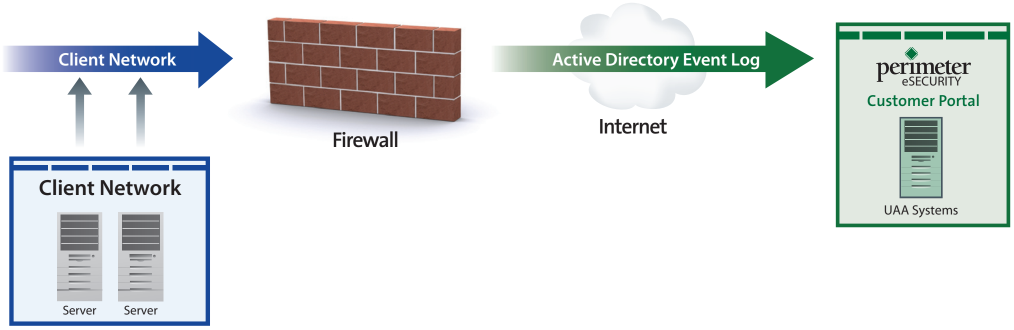
perimeter eSecurity™

Complete. On Demand. Affordable.

Many organizations do not adequately monitor the security events associated with Microsoft® Active Directory login and logout activity. Unauthorized users could be attempting to access critical applications and resources on the company's network without any warning or timely alerts that could lead to preventative action or remediation. Also, the resulting lack of information available for auditing purposes can make regulatory compliance challenging.

Perimeter eSecurity's User Access Auditing (UAA) for Microsoft® Active Directory captures the appropriate information from the system event log of each AD server in an organization and structures and analyzes the data so that technical administrators can be effectively alerted and can provide useful reports to auditors and management. Our UAA service provides an additional level of monitoring, offering alerting and detailed reporting of Valid User Login Failures, Invalid User Login Failures, Login Attempts Made During Off Hours and Account Lockouts.

USER ACCESS AUDITING PROCESS

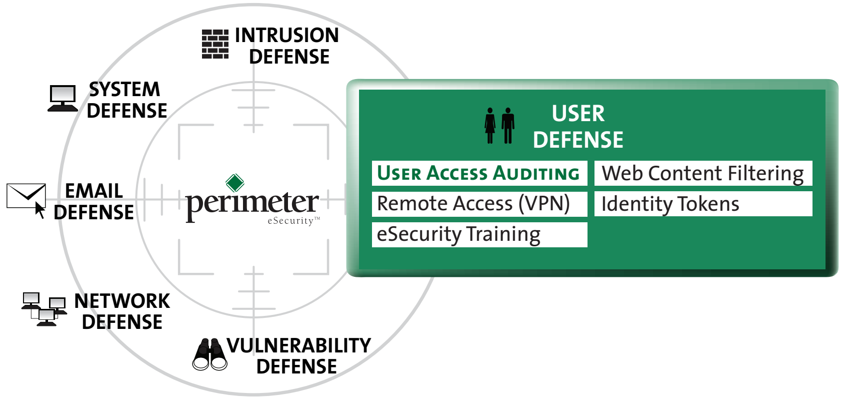


MICROSOFT® ACTIVE DIRECTORY

Microsoft® Active Directory (AD) is the leading user management facility implemented by all types of companies to control access to an organization's network applications and resources. Its main purpose is to provide central authentication and authorization services for Windows-based computers. Since AD controls all of an organization's user login and logout activity, it keeps track of several security-related system events that can be continuously captured and monitored for alerting and reporting purposes.

THE BENEFITS OF PERIMETER'S SOLUTION

Key Features	Benefits
Critical Event Capturing	Critical login/logout events are captured, such as Valid/Invalid User Login Failure, Login Off Hours, Event Log Empty, and Account Lockouts
Automatic Notification	Violations of policies generate notifications, including Login Off Hours
Account Synchronization	Synchronizes user changes in customer's Active Directory
Single Customized Online Portal	Easy-to-use online portal with access to a number of different detailed reports, enabling administrators to quickly view a snapshot of their UAA systems
24x7x365 Technical Support	Security Engineers are available for you day and night, 365 days a year to ensure that you receive the support you need, when you need it


INTRUSION DEFENSE
SYSTEM DEFENSE
EMAIL DEFENSE
perimeter eSecurity™
NETWORK DEFENSE
VULNERABILITY DEFENSE
USER DEFENSE
User Access Auditing
Web Content Filtering
Remote Access (VPN)
Identity Tokens
eSecurity Training