ManageEngine
Log360

USE CASE

Auditing change control with Log360

Auditing change control with Log360

Are you aware of all the critical changes happening to your IT environment? As a security admin, your first line of defense is the security controls that you set to protect your network resources from unauthorized access.

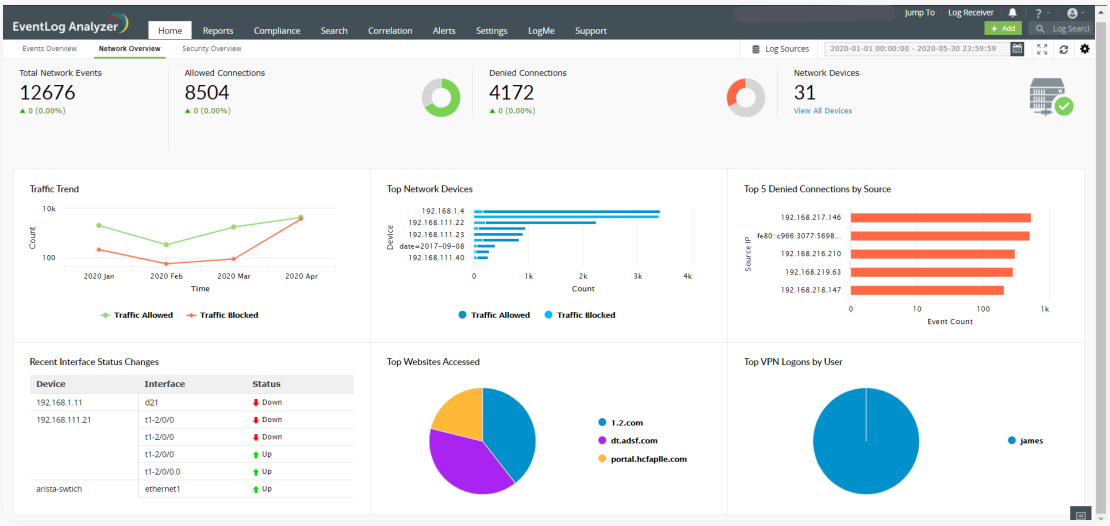
For an attacker, weakening these controls will be the first step to evading detection. For instance, consider that malicious actors have disabled the account lockout policy for invalid password attempts. This gives them just the room they need to brute force their way into any account without rising the slightest suspicion. The only way to stop this from happening is to granularly audit all the changes to security controls in your network infrastructure.

How Log360 can help

Audit multiple environments under a single console

Log360 has an exhaustive range of reports to audit critical changes to your Active Directory, Microsoft 365, AWS, and Azure Active Directory in real time. The moment any policy change or modification to users, groups, OUs, computers, Group Policy Objects (GPOs), sites, or FSMO roles is detected, an alert will be raised immediately. Log360 can also audit your applications, servers, databases, and network devices for critical changes in security policies.

Analytical dashboards to track critical changes



With a built-in analytical dashboard, you can granularly track critical changes in each of these devices. For instance, you can track changes to firewall access control lists (ACLs) and rules for incoming traffic. In applications like SQL, it is safer to restrict write access to a few privileged users to prevent unauthorized changes to the database. If a user suddenly gains write access through underhanded means, this has serious implications for data security. Such changes in user privileges also can be monitored with reports and dedicated dashboards.

With these in your arsenal, you can rest assured that your security controls stay intact, freeing up your time for other critical operations.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a Customers' Choice for SIEM

Check out why

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in Gartner's Magic Quadrant for Security Information and Event Management, 2020.

Get the report

https://www.linkedin.com/showcase/manageenginesiem

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

ManageEngine Log360

$ Get Quote

Download