ManageEngine
Log360

4 Pillars of cybersecurity monitoring

Index

Introduction

Many companies have grown comfortable with remote work after the pandemic caused a sudden disruption in business. Currently, adoption to cloud technology is at its highest. However, amid the chaos, security has taken a back seat. Hackers know this and are taking advantage, targeting their efforts towards remote employees and organizations with weaker security. This rise in cyberattacks has become a wake up call for enterprises to focus on cybersecurity.

The **four pillars of cybersecurity monitoring**

Hackers were quick to modify their strategies to suit remote work conditions. This e-book discusses the four pillars of cybersecurity monitoring you should keep in mind to ensure that attackers do not have the upper hand and ensure the safety of your organization.

Let's take a look at these pillars and how you can implement them using Log360, an SIEM solution recognized by Gartner in its 2020 Magic Quadrant for Security Information and Event Management for the fourth straight time.

Pillar 1

Having a bird's-eye view of your IT environment

Having a holistic view of your network security is essential. To get this view, you need to capture, analyze, and constantly monitor security data from all network devices, applications, and servers in your network. Continuous monitoring of this log data will give you better visibility on what went wrong, when an incident occurred, and how.

This process is a little simpler (but no less important) in a single cloud or on-premises only environment. However, many companies have adopted hybrid or multi-cloud environments. In cases like these, monitoring every aspect of all components of your environment can become cumbersome.

Security solutions such as Log360 solve this issue by offering a single console from which you can monitor all your environments. The auditing module of Log360 retrieves all the log data from an Active Directory domain controller and Azure AD environments, and displays it in easily readable formats such as graphs and charts.

Log360's cloud monitoring module can monitor your Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) environments, and provides all the information you need in a single dashboard. This puts all the vital information about your organization's environment, regardless of the type of network, right at your fingertips.

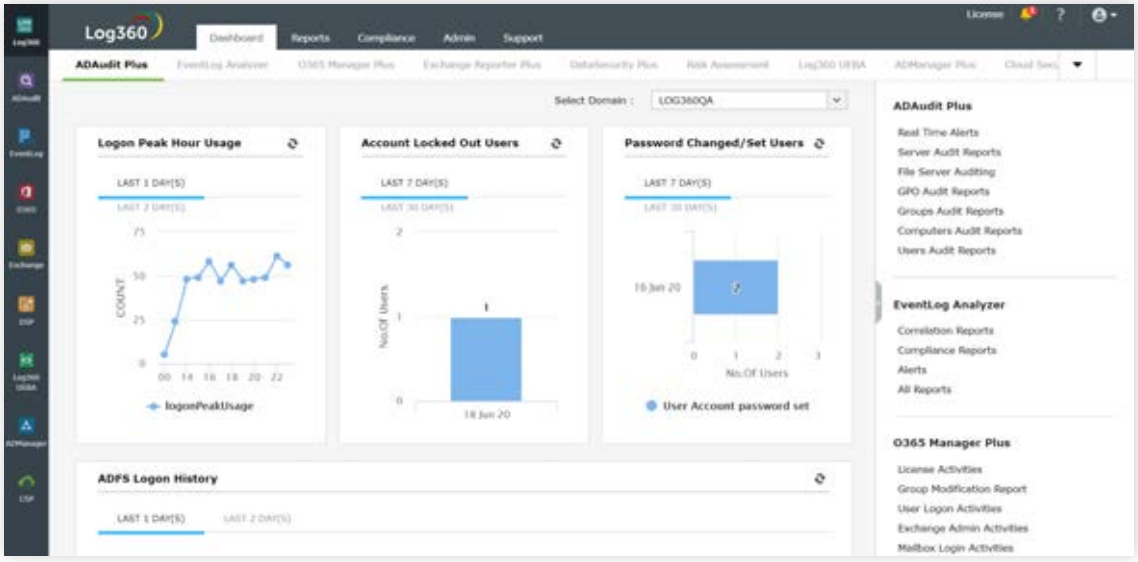

Figure 1: Log360 dashboard

Pillar 2

Keeping your defense systems in check

Firewalls and VPNs are two strong defense mechanisms you can use against attackers. These are also good places to check for any attack attempts, as catching them here helps you quash attacks in their earliest stages. Monitoring events such as firewall rule changes, which can detect the initial stages of an insider attack, or an unusual increase in data being sent (possible data leak) can help in tracking attack attempts and ensuring that your network is safe. VPNs are susceptible to brute-force attacks, but monitoring failed VPN logons by users and remote devices can provide information on any potential breach in security.

Log360 supports all major commercial network firewalls such as Cisco, Juniper, Fortinet, etc., and can provide exhaustive reports on firewall connections that have been denied, changes to firewall rules, allowed firewall traffic, top traffic based on source, and more. It also offers a comprehensive set of reports and tools to monitor various aspects of VPNs such as logon information, authorization errors, logon trends, and much more.

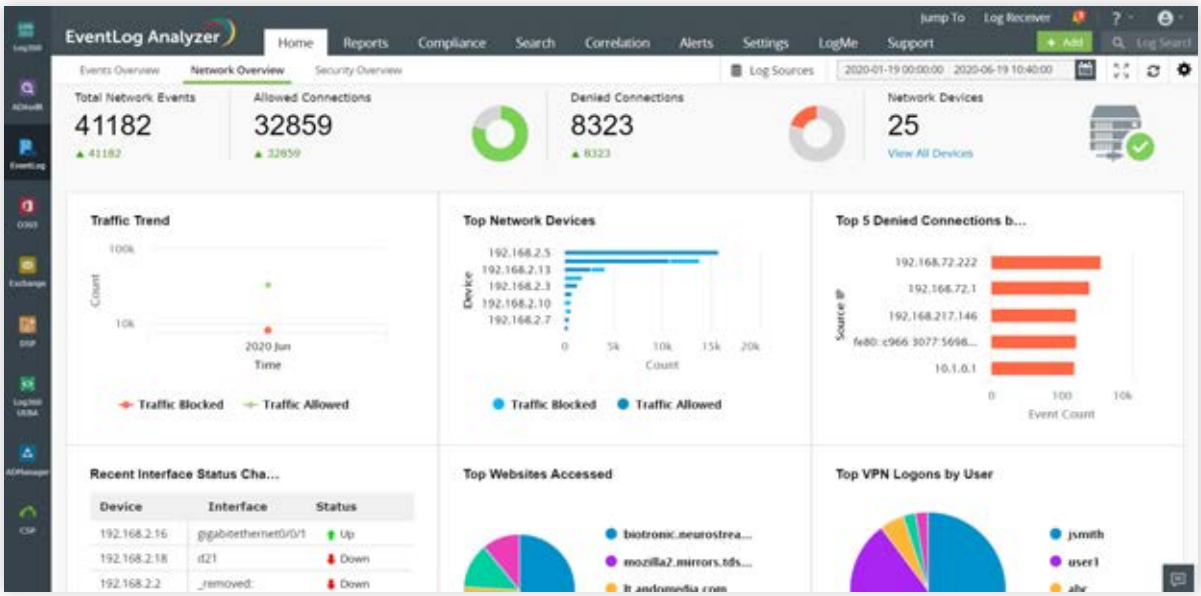

Figure 2: Network overview tab of Log360

Pillar 3

Safety mechanisms for outside threats

Monitoring your environment is only part of an effective cybersecurity strategy. When a breach does occur or is suspected, it's important to get information on the attack as soon as possible so that quick action can be taken to prevent or stop a breach. If any anomaly is detected in your environment, an alerting system can help notify you about it as soon as possible.

Log360 has an advanced alerting and threat intelligence system that can piece together bits of information such as user logon/logoff hours and user privilege changes to detect possible attacks.

For example, if a malicious actor is trying to connect to your network using brute-force technique or by compromising your VPN logins, Log360 can instantly identify and block it. The solution can identify traffic from or to a malicious source with its built-in threat intelligence platform, that is dynamically updated with the latest threat feeds. Further, you can remediate the condition by configuring automated workflows.

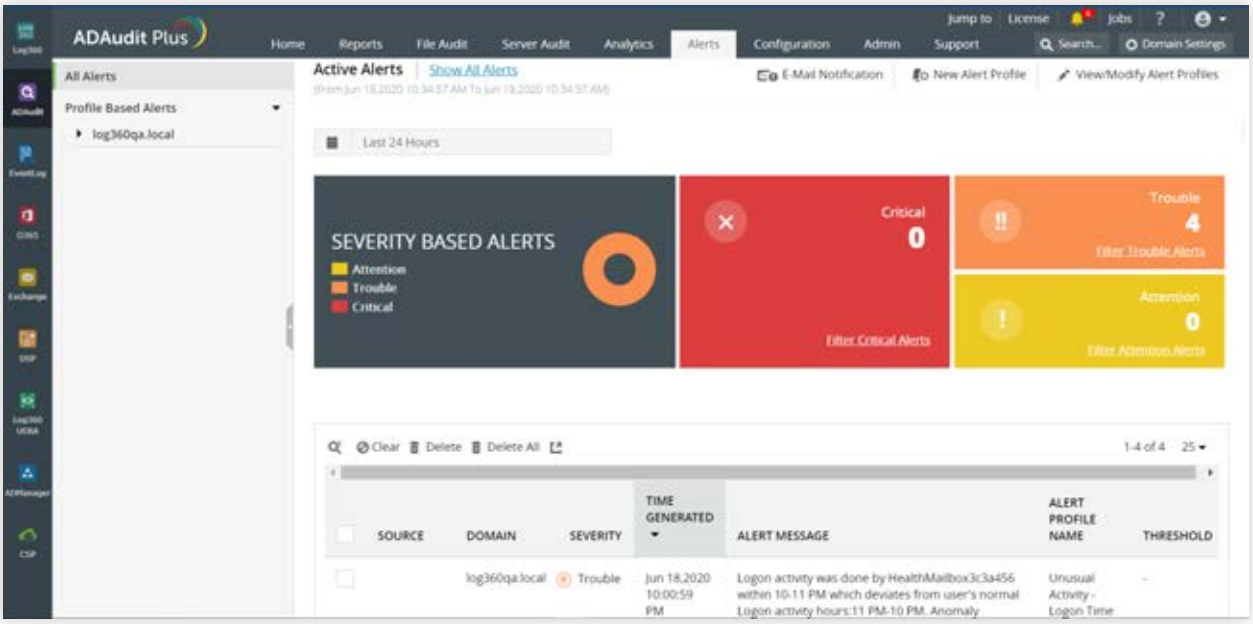

Figure 3: Alerts tab in the auditing module of Log360

Pillar 4

Safety mechanisms for inside threats

Now that we know how to handle external attacks, it's time to tackle the insider threat. No matter the organization, there's always the possibility an insider will go rogue and try to get access to sensitive information or compromise your network.

Monitoring your employees is essential to detect these kinds of threats. Various parameters can be tracked such as employee logon/logoff time, logon duration, and whether they've been granted unusual permissions. All these parameters can indicate whether there are potential bad actors within the organization.

Log360 is capable of monitoring and analyzing all these aspects automatically. With the advanced machine-learning (ML)-driven user and entity behavior analytics (UEBA) add-on, Log360 can monitor employees and create a pattern of what's considered normal behavior. If any user defers from their regular patterns, the solution can be set to alert you so that you can deal with the situation instantly.

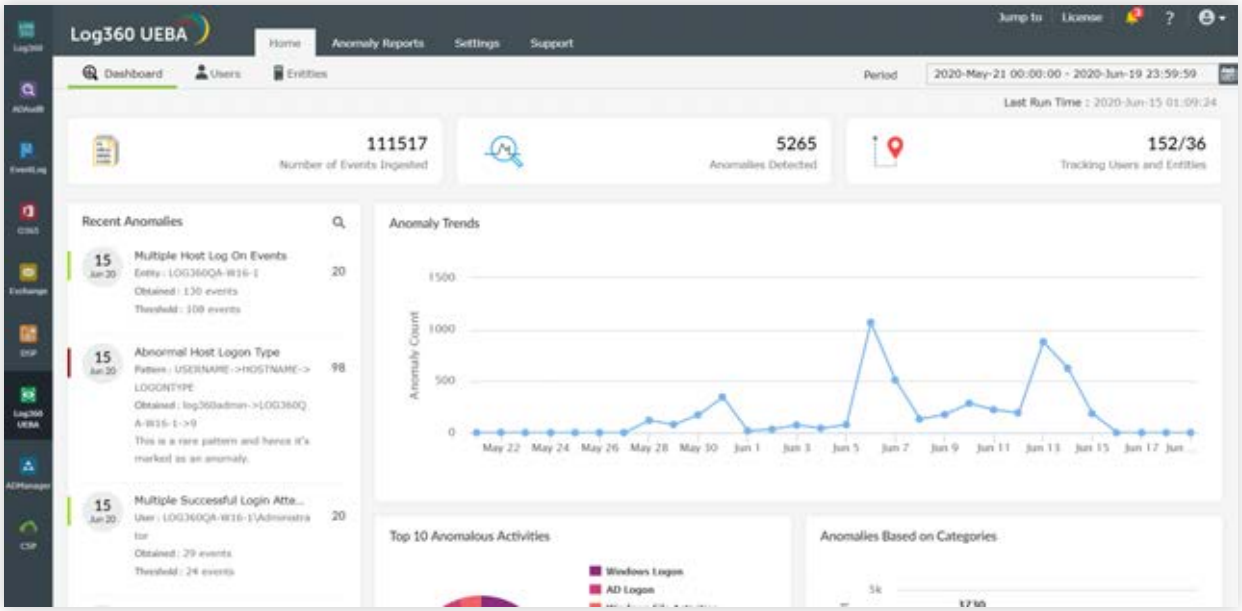

Figure 4: UEBA module of Log360

Conclusion

We are going through a paradigm shift in work culture, which has left some loopholes in security that need to be plugged. The mass adoption of remote work has provided new, vulnerable targets for attackers, and it's up to IT admins to ensure that their organizations are secure.

As attackers evolve, organizations have to boost their security measures, too. Solutions such as Log360, an integrated log management and Active Directory auditing and alerting solution, helps fortify the security of organizations and keeps attackers at bay. In these times, it's never been more important to have better preventive measures and strong security solutions.