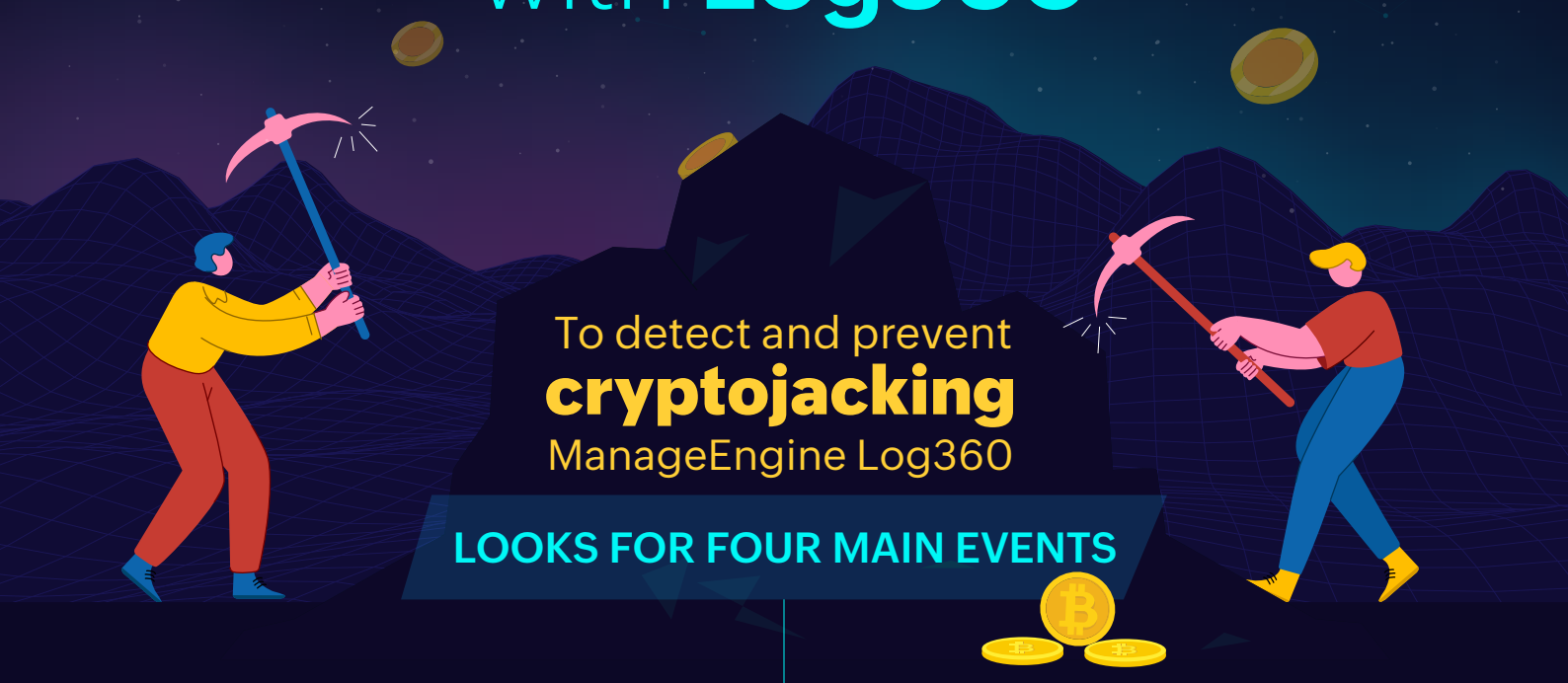
ManageEngine
Log360

COMBATING CRYPTOJACKING with Log360

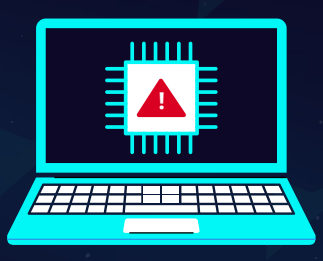


To detect and prevent **cryptojacking** ManageEngine Log360

LOOKS FOR FOUR MAIN EVENTS

1 High CPU usage alert

Mining cryptocurrency is a resource-intensive process. Looking out for and being alerted to high CPU usage is a good way of identifying and preventing cryptojacking.

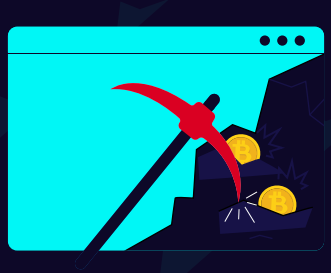


2 High machine temperature alert

The utilization of your device's resources is directly related to your device's temperature. When your CPU usage increases, your device temperature also increases. Temperature-based alerts can help you identify cryptojacking.

3 Cryptocurrency mining software started

You can monitor if there's an executable file downloaded and run a process containing names such as bitcoin-qt, cgminer, tbalance, and coin-miner. These are just a few examples of mining software that Log360 can detect.



4 Cryptocurrency wallet software started

Irrespective of whether an attacker uses your device's resources for mining cryptocurrency, or they steal the cryptocurrency stored in your wallet and transfer it to theirs, the wallet software would be running. So, monitoring the wallet software can help you combat cryptojacking.

To fully evaluate how ManageEngine Log360 can help your organization defend against cryptojacking,

Sign up for a personalized demo