INDUSTRY
TECHNOLOGY

LOCATION
BURLINGTON, MA

CASE STUDY

ACCOUNT TAKEOVER

CHALLENGES

Technology has introduced innovative ways for organizations to facilitate access to applications for its employees. Frequently users are accessing applications remotely from a variety of different devices and locations. This dynamic relationship between applications and end users makes identifying potentially malicious activity more and more challenging. With credentials often being the end target for an adversary, being able to monitor acceptable use has become a last line of defense against compromise.

SOLUTION

The Oort Platform is constantly tracking and gathering static and dynamic attributes of every Identity. As a customer of Oort, Avid Technologies was able to identify inappropriate use by one of its employees through the platform in seconds. Often referred to as the “impossible traveler” scenario, Oort identified multiple sessions being used internationally by a user who did not operate in either of those regions. This capability is especially successful at identifying compromised credentials and unauthorized access via stolen credentials.

CISO & CSO at Avid, Dimitriy Sokolovskiy, says “we had a situation where an employee was exhibiting odd behavior on top of authenticating from different IP addresses and using an IP anonymizer. Oort was able to identify concurrent connections from different IP addresses in different countries... This gave us enough information to validate and partner with human resources to rectify the situation.”

> “Identity of the future is not going to be based on anything we use now. Identity in the future will primarily be based on behavior. This gives Oort the advantage. They're helping us a lot, augmenting the data we have and providing insight and context to events. They are very good at providing proactive alerts so incidents don’t happen. The tool helps you work less when in the middle of an emergency.”

Dimitriy Sokolovskiy
CISO & CSO, Avid