CASE STUDY

INDUSTRY
TECHNOLOGY

LOCATION
BURLINGTON, MA

CHALLENGES

- **Risk management**
- **Remove Identity Silo**
- **Multiple IDP sources**
- **Continuously remote business**

Technology companies often have a diverse attack surface when compared to other industries. End users have more power and technical capabilities than in other firms. This means the security organization needs to balance control and access without impacting productivity. Additionally, having a highly dispersed workforce requires connectivity with security technology that can scale alongside without creating friction. With a myriad of technology solutions deployed, having visibility across identity infrastructure has never been more important.

RESULTS

- **Enhanced visibility into Identity environment**
- **Gained additional visibility into weak multi-factor authentication usage**
- **Achieved proper hygiene for Identity access program**
- **Behavioral detection of account sharing**

SOLUTION

Using the Oort platform, Avid was able to realize broad value in multiple areas. Enhanced visibility in Identity profiles that previously required heavy manual activities. Being able to collate and consume static and dynamic events, Oort generates only alerts and findings to ultimately reduce the attack service while not adding noise or false positives.

"Oort is helping us with things we didn't previously do because we lacked technology and helping us with things we didn't know we needed to do," says CISO & CSO, Dimitriy Sokolovskiy. "Oort is focused on solving your goals and not selling cyber security software. Additionally they have a smart team in front of the problem, you know it is going to get solved."

> *"OORT WAS ABLE TO GIVE US PRIORITIZATION INTO DIFFERENT KINETIC ALERTS THAT DRAMATICALLY INCREASED EFFICIENCY.*
>
> *UNDERSTANDING WHERE WE HAVE WEAK MULTI-FACTOR AUTHENTICATION, SPECIFICALLY SMS, HAS BEEN A BENEFIT OF THE PLATFORM"*

Dimitriy Sokolovskiy
CISO & CSO, Avid