Customer Success Story

AC Transit Moves People & Information Securely with Behavioral AI-Based Cloud Email Security

AC Transit provides bus service to more than a dozen counties in the California East Bay, serving about 200,000 customers on an average weekday. As a major regional transit provider and a partner to federal agencies, AC Transit must operate efficiently while protecting its employees and partners from sophisticated email-borne attacks.

When Head of Cybersecurity Tas Jalali arrived, his first priority was to stop active account takeover attacks. "We didn't have time to deploy a secure email gateway," said Jalali. AC Transit needed a solution that was easy to implement, and could start detecting threats right away. "We implemented Abnormal within minutes, quickly identifying and remediating the email attacks in our inboxes."

"Advanced attacks like BEC, ATO, and spear phishing are more complex than the spam that typically comprises 60-70% of unwanted emails. With Abnormal, we have superior detection capability from all of these threats, helping us avoid disaster from malicious attacks," added Jalali. "Plus, with the Email Productivity add-on, we now save more than 120 hours of company time each month by filtering out graymail. These are non-malicious but time-consuming emails, critical to filter out particularly for our executives," Jalali said.

"Our executives and Board of Directors are commonly hit with significant amounts of phishing and BEC email attacks. Abnormal's behavioral-based modeling and pattern recognition have been great in detecting and stopping those attacks. We are confident we have the right solution in place."

Tas Jalali
Head of Cybersecurity

Industry
Transportation

Location
Oakland, California

Protected Mailboxes
1,100+

CHALLENGES

- Identify an API-based solution that could also provide superior detection services.
- Stop ongoing account takeover attacks in motion and quickly protect employees, executives and partners.
- Improve executive productivity by filtering away time-wasting graymail messages.

BUSINESS IMPACT

- Detected and auto-remediated compromised accounts to maintain partner trust, protect reputation, and enhance security.
- Prevented sophisticated attacks from reaching executives, board of directors, partners, and employees.
- Saved 120+ employee hours each month by reducing the amount of graymail in inboxes.

50+ compromised vendors detected by Abnormal VendorBase™

SECURITY ENVIRONMENT

Attacks Prevented by Abnormal, the Past 2 Years

Phishing	BEC & Impersonation	Malware	Account Takeover	Fraud
1,658	1152	61	26	178