As an MSP, you know the MFA fight too well: Customers don't want to do it. (It's a whole extra step!) Then they get breached. Then you have to clean up the mess.

That's the cycle John Kistler, CEO of J&B Technologies, found himself in. He had tried for ages to convince one of his customers to integrate MFA.

Then one day John came into work … to 88 alerts from SaaS Alerts. That customer was under attack. *Facepalm*

John's team immediately dug in and discovered a bad actor from Russia was trying to hack multiple users at the organization.

"Thankfully, SaaS Alerts went absolutely apeshit," John said. "It would have been a bad day without SaaS Alerts."

Because nobody at the client's office had MFA turned on, the Russian hacker was able to infiltrate their Microsoft 365 accounts and live off the land, waiting for the perfect moment to attack.

Fortunately, even without MFA, John was able to save his client's SaaS thanks to the tip-off from SaaS Alerts. It was the perfect opportunity to prove in real time how important MFA is.

"It's something you have to do, even if you don't like it," John told the customer. "It's like paying taxes."

The organization now has enabled MFA — and John's team set up SaaS Alerts automations to let them know if employees try to turn it back off.

Because sometimes, customers never learn. That's what cybersecurity experts like John — and tools like SaaS Alerts — are for. Safeguards to save customers from themselves.

SaaS Alerts®
A **Kaseya** COMPANY

+1 (910) 887-3352   sales@saasalerts.com   www.saasalerts.com