COVAX DATA

Product Bulletin

"WHAT IF" SOLARWINDS BREACH

THE SOLARWINDS BREACH MADE GLOBAL HEADLINES, POTENTIALLY COMPROMISING IT SYSTEMS AT OVER **18,000 ORGANIZATIONS AND GOVERNMENT AGENCIES.**

The persistent idea that perimeter cybersecurity is sufficient to protect the most sensitive data, or a nation's, is just mindboggling. It is analogous to leaving your money on the kitchen table just because you have locks on your doors. Perhaps SolarWinds is the wake-up call the world needed to truly understand this deficiency. Because when the trusted systems used to protect IT networks are weaponized to become threat vectors, we need much more than perimeter security.

Approximately 18,000 customers implemented the "trojanized" upgrade of SolarWinds cybersecurity software, and the backdoor code actually loaded before the legitimate code executed. Organizations were misled into believing that no malicious activity had occurred. This resulted in the attacker having a foothold in the network, used to gain elevated credentials. The credentials enabled the bad actors to impersonate any account or user on the network, including highly privileged accounts.

What does all this mean? It means organizations' cybersecurity solution actually became the problem, providing bad actors unfettered potential access to their deepest secrets. But **what if** there was a way to know something was not quite right? **What if** the impersonated user immediately set off alerts and alarms? And even if all of those warnings went unnoticed, **what if** the bad actors were still blocked from accessing actual data? To some, it seems too good to be true. To Covax Data customers, it is the Covax Polymer solution.

With Polymer, AI-driven user behavior analytics (UBA) would have blocked access to the data, and the blockchain based chain of custody would have alerted administrators to the attempts. Even if the bad actors could fool the UBA, they would have been unable to circumvent the chain of custody and alerts. And with Covax's patented blockchain lite, their presence would have been immutably logged, impossible to erase. Finally, any data that the hackers somehow could have accessed would have been in the form of Covax data molecules – making it useless unless viewed through an authorized Covax driver.

POLYMER PROTECTS THE DATA, REGARDLESS IF OTHER CYBER PROTECTIONS FALL DOWN.

BEYOND DATA SECURITY… DATA CONTROL