Migrating 1000s of applications to the cloud with confidence

Case Study: Migrating the one of the largest consumer healthcare business in the world to the cloud.

Problem

With so many applications moving to the cloud in a short period of time, the enterprise needed to ensure that cloud infrastructure resource owners could take immediate action if they violated a cloud security architect defined policy. The challenge was that current tools centralized security and funneled alerts to the SOC, where **only high risk security alerts made it back to developers**, allowing **misconfiguration debt to rapidly grow** into a shadow threat.

Solution

Secberus' Federated Risk Management feature integrates with identity providers to enable Attribute Based Access Control which enables the product to assign any scope of ownership to any user based on attributes in the IdP. Each cloud security architect can **adjust global policies to fit the needs of their applications**, and each developer is **immediately notified when their configurations violate a security policy**. All **in real-time**.

Outcome

With Federated Risk Management, the enterprise's developers **no longer have to wait for the SOC** to have investigated alerts and prioritized them highly enough, before they find out they've made a security misconfiguration. The enterprise was able to migrate rapidly, securely and at a **lower TCO** than with a security tool trying to do governance tasks.

"Secberus has lifted a big weight off our shoulders in giving me and my security team the ability to know how to do what's best for the business and what's right by security quickly and confidently."

Deputy CISO
Enterprise Healthcare

Contact Sales: sales@secberus.com