All FireHydrant Employee Devices Secured with Beyond Identity

Company Overview

Founded in 2018, FireHydrant is a fast-growing company providing software that automates incident responses for developers.

REGION	INDUSTRY	INTEGRATIONS
North America/US	Incident management software	Okta, Kandji, and CrowdStrike

Solution: Secure Workforce

RESULTS

- 100% of employees enrolled after one month
- Numerous logins from insecure devices blocked

Challenge: personal devices putting company data at risk

Like many tech startups, FireHydrant has a fully-remote team, meaning employees and contractors often work from personal devices. But the company couldn't tell if those devices had been secured, or whether they were accessing sensitive company data through enterprise networks like Okta.

FireHydrant's IT Manager, Ylan Muller, recognized the security risks that insecure personal devices posed. "It became more and more evident that we needed to validate that someone is not only who they say they are… but also that the device that they are using is trusted, managed, and is not going to float around unencrypted with company data."

If cybercriminals accessed sensitive data from an employee's compromised mobile or laptop, the consequences could be disastrous. So to prevent this, Muller and FireHydrant's security team wanted to implement better security measures, tie together their entire security stack, and secure their identity access plane.

Muller was spending valuable time dealing with issues like resetting passwords and reviewing device reports to ensure that company devices were being used for their intended purpose—time she wanted to devote to more strategically important work.

Solution: authenticating the device, not just the user

To combat the risk of a data breach stemming from employees using their own endpoints, and to ensure device trust, Muller turned to Beyond Identity.

Beyond Identity captures over 25 user and device security signals from the device requesting access. Beyond Identity then utilizes those signals to enforce risk policies before access to the company's resources is granted, implementing these policies every 10 minutes while the session is active. This allows FireHydrant to detect when devices don't meet their minimum security standards and block them from accessing company systems and data.

Despite the company's needs being complex, Muller said, "Beyond Identity hit all of the marks on our requirements list." The testing process went well, confirming that Beyond Identity would work for the company. "When I tested it with the initial group of beta testers, everything went smoothly. There were no breaking outages and it didn't block people from doing work, and a few even praised the magic of not having to memorize a password."

Unlike other solutions, Beyond Identity smoothly integrates with FireHydrant's tech stack, gathering device indicators from Kandji and CrowdStrike to inform access to Okta. This reduces implementation difficulty and allows for a strong security architecture.

Results: 100% of employee devices secured, risky logins blocked

Thanks to a smooth onboarding process, 100% of employees have now been enrolled in Beyond Identity. The workforce at FireHydrant responded positively, appreciating the convenience of not having to use passwords. This achieved their key device trust goal of knowing that any device accessing their data is either trusted or meets the security policies they set.

Muller has seen in a very real way how Beyond Identity protects FireHydrant, catching misconfigurations and preventing logins from insecure devices that previously would have put the company's data at risk. Muller stated,

> *I can see how many devices get blocked by certain policies… being able to see it in action has been valuable for us.*

Beyond Identity has also eliminated time-consuming tasks like going through security reports frequently and dealing with login issues, freeing up time for Muller to focus on other initiatives that are important to FireHydrant. And while Muller found Beyond Identity's customer support helpful, it isn't often needed. ***"I like to say, if we can set it and forget it, that's perfect. That's largely what we've been able to do."***

BEYOND IDENTITY

Beyond Identity is revolutionizing digital access for organizations looking to improve protection against cyber attacks and deliver the highest levels of security for their workforces, customers and developers. Its suite of passwordless, phishing-resistant, and zero trust authentication solutions improves security and user experience. The platform delivers continuous risk-based authentication incorporating signals from the zero trust ecosystem to ensure only valid users and secure devices gain or maintain access to critical resources. Orangizations like Snowflake, Cornell University and Unqork rely on Beyond Identity's highly available cloud-native platform to thwart attacks and advance their zero trust strategies. To learn more about Beyond Identity's FIDO-2 certified multi-factor authentication (MFA) solutions, visit beyondidentity.com and stay connected with us on Twitter, LinkedIn, and YouTube.