Ylopo Ensures Device Security Across Extended Workforce

Company Overview

Ylopo is a leading provider of digital marketing services for real estate companies and agencies. The company is based in the United States and has over 200 employees.

REGION	INDUSTRY	INTEGRATIONS
North America/US	Digital marketing services	Okta, Kandji, CrowdStrike, and Microsoft Intune

Solution: Secure Workforce

RESULTS

100% of employees enrolled within a month

Many insecure devices blocked from logging in

Challenge: securing remote work devices

Most of Ylopo's workforce is remote, allowing the company to hire the best talent from anywhere in the world. However, remote work also brought about a critical challenge for the company—making sure that all devices being used by their extended workforce to access company systems remotely are secure and trusted.

The fact that Ylopo works with around 200 remote contractors—who all use their own devices—further increased the risk of unsecured logins to their IT systems. When Miguel Espinosa was hired as Ylopo's Director of Information Security in 2021, finding the right device trust solution was a priority.

"We needed to have more visibility and control of our data on people's personal devices," Espinosa said, At the time Ylopo had "no real understanding of what devices they're using and whether they comply with our requirements or not." A failure to fix this security gap could enable cybercriminals to access Ylopo's IT systems through a compromised device and steal sensitive data, a serious risk that Espinosa and Ylopo were determined to mitigate.

Solution: strong assurance of device security posture

Espinosa's research into device trust vendors led him to Beyond Identity, which captures over 25 risk attributes from the device trying to access the network. Beyond Identity uses those signals to determine if the user and the device meet the security standards set by Ylopo's IT team. If the device doesn't meet the requirements, they are denied access to Ylopo's critical resources and data.

Espinosa said,

> ***"Beyond Identity provided everything that we required in order to comply with our SOC 2 requirements.***

while also being more cost-effective and customizable to their specific needs compared to alternative solutions.

What's more, Beyond Identity ensures all devices accessing company data are secure without using invasive MDM software. This was very important for Espinosa when it came to dealing with Ylopo's contractors. "Beyond Identity allows us to say, hey, we're just monitoring, we're not looking at your personal stuff. We're just making sure you hit these rules."

Ylopo was able to make sure that Beyond Identity worked for them in practice with great ease. "It was a smooth process testing out [Beyond Identity]," Espinosa said. Having established this, they felt confident enough to press ahead with the purchase and roll out the solution company-wide.

Results: 100% of employee and contractor devices secured

Getting Ylopo's workforce onboard with Beyond Identity was as smooth as the testing process, and within just a month the solution was rolled out to 100% of the workforce. Such high compliance represented a big success for Ylopo.

The fact that insecure devices are simply blocked during authentication has streamlined the security compliance process, saving Espinosa time. He no longer needs "to go and pull a report to make sure everybody's adhering" to the security guidelines. Beyond Identity is so easy and time-efficient to manage that Espinosa even feels he can, "Set it and forget it."

He has also seen first-hand how effective Beyond Identity is at flagging insecure devices, discovering "a lot of little use cases that we were able to address that would potentially cause harm to the organization."

According to Espinosa, Beyond Identity has ultimately achieved a key goal of Ylopo's.

> ***Beyond Identity helps us guarantee that our US employees are accessing our data through company-issued devices and contractors are accessing our system through devices that are fully compliant with our requirements.***

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.