Red Cup IT's Game-Changer:

Mastering Security with Beyond Identity

About Red Cup

Red Cup IT is a proactive and "secure by design" Managed Security Service Provider (MSSP) delivering security architecture, support, technical project delivery, and enterprise class cybersecurity solutions. Their clients call on them for their expertise in solutions that include SOC 2, HIPAA, PCI, and privacy-related compliance for complex environments.

REGION	INDUSTRY	SIZE
Worldwide	Managed Security Service Provider	20+ team members providing services to multiple clients

Solution: Secure Workforce

RESULTS

- Attack surface reduced for customers
- Over 2,000 Red Cup IT team hours saved each year with passwordless authentication
- Baseline controls are always effective, even in complex client environments

Challenge

Red Cup IT employees need to log into multiple environments a day. Each environment was protected by multi-factor authentication, and once into the environment, the user would then have to log into and manage individual resources, which also have multi-factor authentication from various providers. On average, each employee was going through this process 50 times a day.

In an effort to simplify the authentication process, Red Cup IT's leaders decided to look for a passwordless solution to remove the friction.

Solution

Beyond Identity added additional layers of security to the existing infrastructure, and according to Red Cup IT Founder and CEO Dan Le, "The continuous device posture checks and the conditional access policies were a huge part of why we picked Beyond Identity." Because they are an MSSP, the products Red Cup IT uses must benefit both Red Cup IT and their clients. Le stated ease of use and ease of deployment, both in house and for clients, was one of the primary benefits of Beyond Identity.

Results

Deploying Beyond Identity resulted in time savings, increased third-party device security, increased device trust, and a reduced attack surface.

"Too difficult" to hack

Red Cup IT wanted to build a secure compliant cloud environment to pair with a secure and compliant endpoint. Working toward a NIST and CIS compliant environment, they installed Beyond Identity, Okta, CrowdStrike, ThreatLocker, Talon Cyber Security, Huntress, Salesforce, NetSuite, Snowflake,and other tools. They deployed everything and took the laptop to DEFCON with a sign that said, "Hack Me" on it.

Their goal was to discover the methods hackers would use to circumvent their security postures and defenses. After seeing the defenses, and hearing about the security enclave and the public/private key, the hackers said it would be near impossible to break in, especially with Beyond Identity, as the software checks for credentials every 10 minutes. Every hacker walked away. Their reason for not attempting the hack? "It's too difficult, and we'd probably get locked out immediately."

Ease of use leads to massive time savings

Not only is Beyond Identity easy to use, the frictionless authentication process has led to significant time savings for both Red Cup IT and for the company's clients and their end users. For the internal team alone,

Le estimates they save approximately 8 hours each day logging in to the complex environments they manage. In the course of a year, that's over 2,000 working hours Red Cup employees have reclaimed

and now use to benefit the company's bottom line.

The reduction in help desk tickets related to lost passwords and account lockouts benefit both Red Cup IT and their clients. End users spend less time waiting for IT help and Red Cup IT's staff can spend more time on building IT automation workflows, quality of life enhancements, policy management, and other services.

Increased security for third-party devices

A major benefit for Red Cup IT's clients is the added level of security Beyond Identity provides for third-party devices used by contractors. New contractors who use their own device introduce new areas of risk. One gap Red Cup IT faced in the past was ensuring new devices met security policies. "Beyond Identity is great for helping to discover that, since it extends device trust to SaaS apps that don't typically support it," said Le. This added level of security and ease of use has become one of Red Cup IT's selling points when onboarding new clients.

Benefits to Red Cup IT

- Ease of use and ease of deployment
- Faster, frictionless login for end users
- Ensure policy compliance of BYOD devices for employees and third parties
- Significant reduction in internal and customer help desk requests
- Red Cup IT staff save over 8 hours a day with passwordless login

Device trust

Red Cup IT, as an MSSP, manages a large number of endpoints. They are responsible for numerous logins, tenants they manage for their customers, and an architecture built of an array of IT and security tools. They regularly push out policies to the MDM software, and there wasn't a proactive way to track that with Okta or other typical MSP RMM tools. Beyond Identity allows them to ensure the MDM is on the endpoint, active, and that the policy is active.

Device trust and ensuring endpoint devices are verified before allowing access is a priority for Red Cup IT and for their clients. Beyond Identity notifies administrators if device security has been tampered with, if someone removes or disables antivirus or encryption, or if there is a malware issue.

Reducing attack surface took attacks from non-stop to nonexistent

Many of Red Cup IT's clients are in the financial space, which are the most frequently attacked. According to Le, Beyond Identity has reduced the attack surface dramatically. He said their client's "Microsoft accounts were getting attacked 24/7. So we turned on conditional access—still getting attacked. So we put Okta in and Okta kept getting attacked. Then we put Beyond Identity in front of that, and now it's just non-existent. You can't attack Beyond Identity, because it's a credential on your computer."

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 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.