Case Study:
Reducing Cybersecurity Risk with Azure Active Directory and F5 BIG-IP APM

Lyvon Garth, CISO, Durham County, Aaron Stone, Assistant Director and members of his team provide details about how they use Azure Active Directory (Azure AD) and F5 BIG-IP APM to apply consistent security policies across their hybrid environment. With half the county workforce working remotely, it was important to make it easy for users to access both on-premises and cloud apps while enforcing multi-factor authentication. Azure AD and BIG-IP APM enabled them to do just that.

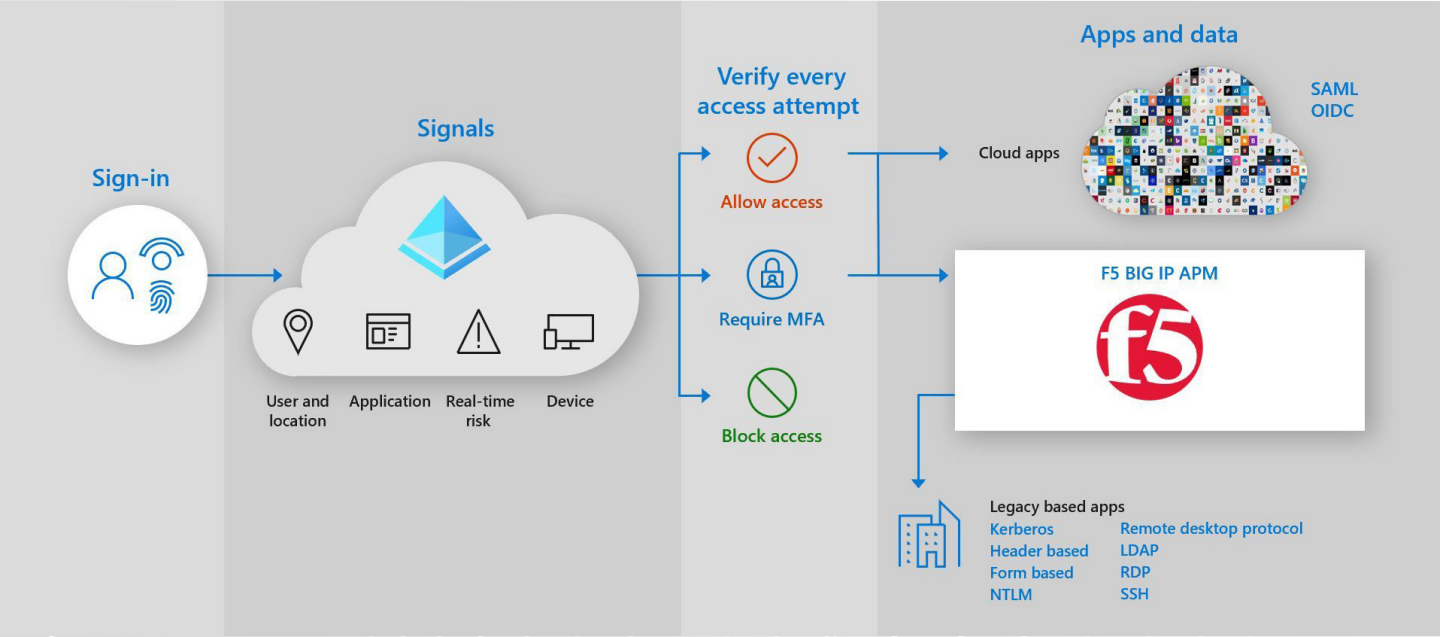
Durham County is located in North Carolina. This vibrant and creative region is home to the Research Triangle Park, an innovation center anchored by three major research universities, University of North Carolina Chapel Hill, Duke University, and North Carolina State University.

On March 6, 2020, Durham County was the victim of a ransomware attack. Fortunately for us, our threat response solution notified us quickly and we were able to shut down our systems before it spread. We did not pay a ransom, no data was stolen, and we were able to keep critical infrastructure up and running. But it was still extremely disruptive. Eighty servers and hundreds of computers needed to be rebuilt. Staff weren't able to access all our systems and applications. To reduce the risk of this happening again, we decided to implement multi-factor authentication (MFA), which makes it more difficult for a user's accounts to be compromised.

Improving security in a hybrid environment

As we made plans to implement MFA across the organization, it was important to use the same authentication solution across all our apps to simplify the process for employees. This was challenging because, although we have begun modernizing our technology, we still support about 400 legacy on-premises apps. Many of these are homegrown apps that service the specific needs of one of the 27 departments within our county.

F5 BIG-IP APM and Azure AD



carahsoft

By:
Lyvon Garth
CISO, Durham County;
Antonio Davis, Platform Manager, Durham County;

Aaron Stone
Assistant Director, IT Operations and Infrastructure, Durham County; Monte Cooley, Network Administrator, Durham County

To complicate matters, the malware attack occurred as COVID-19 began spreading in the United States. Within a few weeks, half of Durham County staff transitioned to remote work. We needed a solution that would allow these employees and others who work in the field to easily authenticate to on-premises apps using MFA.

We chose Azure AD as our identity and access management solution for several reasons. Improving the security of our identities is very important to us, and Azure AD security capabilities like MFA, Conditional Access, and Privileged Identity Management will help us do that. Azure AD also supports SCIM provisioning, which makes it easy to integrate software-as-a-service (SaaS) apps. The team was also already familiar with Azure AD because we use it for authentication to Office 365 apps.

Single sign-on across cloud and on-premises apps

Once we selected Azure AD, we needed to address authentication to our cloud apps and our legacy apps. Many of legacy apps do not support modern authentication standards, which made integration with Azure AD challenging. F5 BIG-IP APM provided the perfect solution. We use F5 BIG-IP APM as a VPN to our on-premises apps. It is interoperable with Azure AD, so employees can use their Azure AD credentials to single sign-on (SSO) to apps that are on-premises. We were able to get all our legacy apps onboarded to F5 in about three weeks.

Better protection with fine-grained security controls

The primary objective of our deployment was to improve security. Because we use Azure AD as the identity provider for all our apps, we can apply security controls to all of them without requiring users to sign in multiple times. The most important security control that we've put in place is MFA. By requiring two or more authentication factors, we significantly reduce the risk of an account compromise.

Saving money with self-service password reset

We also anticipate cost savings from our Azure AD deployment. The service desk currently receives 100 calls per month from users who need help with their passwords. Our Chief Information Officer has mandated that we get that number down to zero. We recently rolled out self-service password reset to a pilot group of users. When these users forget a password, they can now go to a web form to change their password rather than call the service desk. So far this has reduced our calls by 80% By the end of June, we will deploy a registration process to enroll the entire county in self-service password reset and MFA.

Building a security culture

The malware event was challenging for everyone who works for the county government. But the good news is that employees are interested in helping to improve security to reduce the risk of it happening again. The security controls provided by Azure AD combined with employee engagement make it much less likely that we will suffer another attack.

Learn more

If you operate a hybrid environment and want to make access to on-premises and cloud apps easier for your remote workforce, Azure AD and F5 BIG-IP APM may be the right solution.

Contact our team to learn how Azure AD and F5 can help you secure your apps.

- 877-95-F5GOV
- F5@carahsoft.com

carahsoft