datanetworks

FOUNDATIONAL SECURITY WITH AZURE AD
Enabling Secure Identity & Access Management for Private Mid-Atlantic Liberal Arts College

What Data Networks Did for the University

- Planned a modern authentication solution leveraging existing investments and Microsoft's Authenticator application

- Integrated existing user, device, and group management solutions into the new, modern identity and access management solution

- Reduced the volume of password reset requests by enabling a self-service password reset portal

- Increased security by blocking legacy authentication solutions through Azure AD Conditional Access to prevent unsecured authentication protocols (POP, SMTP, IMAP, MAPI) that cannot enforce MFA

- Implemented Microsoft's Azure Directory Premium P2 and Identity & Access Management solution

THE UNIVERSITY had to keep IT infrastructure and security current with the demands of today's students, staff, and faculty. IT administration was already taxed with the planning and implementation efforts to improve their internal systems, including:

- A new finance application to protect and manage financial aid

- A new student information system (SIS) to deliver better learning and development tracking for students

As the application footprint grew (both on-premises and in the cloud), so did the university's attack surface. These growing security concerns caused the university to seek the support of Data Networks.

The challenge

With their student body becoming increasingly mobile and with more educational content moving online, the university faced an uphill climb. The university's IT leaders and staff were tasked with providing access to as many applications as possible while protecting the university and its students from unauthorized users, in addition to other key challenges:

- Deploying critical applications, such CampusNexus' campus management system and student management system

- Maintaining an effective access management and identity solution

- Replacing multiple siloed solutions that were burdensome to manage and secure

- Deploying a comprehensive "single source of truth" identity management system to resolve conflicts with data sources and personnel

- Eliminating significant security vulnerabilities and replacing outdated security practices

- Handling a high volume in password reset requests

The solution

Data Networks created a multi-phased plan to deliver increased security and modern applications to the university's students, faculty, and staff. The solution introduced new technologies while leveraging the university's existing technology investments, delivering a security overhaul that improved the university's service offerings while making the entire environment more secure.

Key components of the solution:

Implementation of Microsoft Azure Directory Premium P2

This comprehensive security suite already owned by the univesity allowed for the creation of a single sign-on across all applications, whether on-premises or in the cloud. As a robust and refined cloud-based Identity and Access Management platform, Azure AD Premium P2 provided the university with advanced security features, including:

- Conditional Access
- Multi-Factor Authentication (MFA)
- Single Sign-On (SSO)
- Self-Service Password Reset (SSPR)
- Privileged Identity Management (PIM)

With the support of Data Networks' Microsoft Engineers, the school was able to deploy the Microsoft Azure AD P2 application to its fullest.

Multi-Factor Authentication (MFA)

By asking more of the user, multi-factor authentication (MFA) adds a crucial extra layer of security. As a result, the univesity encountered fewer help-desk costs, while enjoying the benefits of MFA's enhanced protection.

Risk-based MFA

To maximize the experience for trusted users and stop infiltrators in their tracks, risk-based MFA intelligently analyzes users and decides when to request additional verification. With this capability in place, IT Admin can detect suspicious activity and challenge intruders before they can do any damage, while allowing frictionless access to legitimate users.

Microsoft Azure AD Conditional Access

Today's security administrators are faced with two competing priorities: protect the organization and its electronic assets, and enable users to be productive no matter their location. Organizations can no longer settle for passwords alone to block or allow access to their networks and applications. With Conditional Access, a component of Microsoft Azure Active Directory, the system analyzes various user signals like the user identity and location, the device they're using, the application they're accessing, and other risk factors. Based on these factors, the system can decide whather to allow access, require MFA, or deny access.

Knowledge Transfer

Data Networks' final deliverable was to setup knowledge transfer sessions with their Senior Microsoft Engineers and the university's IT staff. These sessions reviewed the setup and functionality of the new platforms, the Recent Activity page, remediation procedures, guest user access plans, Azure AD's activity and risk reports, their Microsoft 365 Security Score, and Conditional Access policies.

Mission accomplished

By leveraging the advanced features of Azure Active Directory Premium P2 (part of the Microsoft 365 A5 suite), the university was able to both modernize and simplify their identity and access management solution. Users benefit from a more simple authentication process that works everywhere (single sign-on), and administrators benefit from easier security reporting, management, and automation. Dashboard reporting of authentication allows for IT Admins to quickly identify and remediate threats and determine that the university's network is secure.

Want to Implement Foundational Security with Identity and Access Management for Your Organization? Turn to Data Networks and Microsoft.

In partnership with Microsoft, the experts at Data Networks can assess your environment and recommend the ideal identity and access management solution. With it, you can establish a global, risk-based multi-factor authentication system that will secure your environment and empower your users.

To learn more about integrated security solutions like secure remote access, endpoint security, network access control, data security, and cloud security, contact the team at Data Networks.

About Data Networks

Data Networks provides effective technology-based solutions to meet your unique needs. Our solutions are specifically developed to help you drive productivity and manage change.

INNOVATIVE TECHNOLOGY

By partnering at the highest levels with the industry's most respected manufacturers, Data Networks can deliver the right products for your environment with the most aggressive pricing possible. Our strong vendor relationships also bring technical training opportunities, expedited help desk resources, and professional service liaisons for consulting and project engagements.

INSPIRED ENGINEERING

Our goal is to be your trusted technology advisor. So we staff highly-qualified engineers who bring years of experience and the most advanced technical certifications to every engagement. We assign them a single area of technical focus, a unique approach that allows them to continually update their skills and expand their specialized technical knowledge. And we arm them with documented best practices developed over more than 35 years of public-sector service.

We invite you to learn more at datanetworks.com or by calling 800-283-6387.