CASE STUDY

Cornell Makes the Active Directory Security Honor Role

One Identity Active Roles helps Cornell University secure a distributed, diverse, and disjointed AD environment

Key Facts

- **Company**
  Cornell University
- **Industry**
  Higher Education
- **Country**
  United States
- **Faculty**
  1,679
- **Staff**
  8,392
- **Students**
  23,600
- **Website**
  www.cornell.edu/about/

Challenges

- Bringing consistency to a highly distributed and diverse AD environment
- Protecting University data from AD-based attacks
- Eliminate human error and misuse of AD Admin credentials

Results

- Implemented the desired complex delegation model for AD Admins
- Streamlined Unix/ Linux authentication and Authorization based on AD-based administrative tasks
- Removed the risk of unfettered Admin Access across all AD domains without obstructing IT activities

Solutions

- One Identity Active Roles

In higher education, risk is everywhere. With the wealth of personal information, financial data, and intellectual property universities are prime targets for bad actors. In addition, the fact that much of the IT workload at higher education institutions is managed by students, contractors, and transient staff across widely distributed and loosely controlled networks only makes matters worse. Fortunately, Cornell University has found a solution to these long-standing challenges.

"A compromise of our Active Directory domains is one of our greatest security concerns," reported Muhammad Arif, Identity Management, CIT at Cornell. "We cannot succumb to the theft of sensitive data and damage to the reputation of the University as a whole that a compromise would bring."

"We used to have a very distributed environment with more than one hundred completely independent Active Directory (AD) domains," said Arif. "There was no monitoring of these domains, how they were configured, how well the security settings were implemented, what type of authentication and access were being granted. These were all factors that put the University's data and reputation at risk. We had no knowledge of how secure these domains were and no visibility into what someone in IT was doing."

One of the main challenges with securing AD is the limitations of the native tools. The AD Admin account is typically shared among all IT staff that must use the entitlements; the permissions are generally all-or-nothing with no individual accountability for actions taken as Admin; and tasks such as delegation, temporary rights elevation, and policy duplication across domains are extremely difficult if not impossible.

"Active Roles provided several key features right off the bat including delegation and sub-delegation, naming convention enforcement, change history and enforcing policies for AD objects."

Muhammad Arif, Identity Management, CIT, Cornell University

"With such a highly distributed AD environment and so many administrators across multiple departments, we needed a way to delegate access to manage AD objects," said Arif. "Furthermore, we needed the ability to allow admins in other departments to 'sub-delegate' access. With this delegation model came the need to properly control the naming of objects in AD as well as auditing of the actions taken with Admin rights."

The University determined that the best way to address the security challenges presented by its AD environment would be to look for commercial off-the-shelf software that augmented the native capabilities of AD tools with the desired granularity and control that would reduce risk and increase security.

"We wanted a solution that would meet our requirements, was mature, and proven with customers whose environments had challenges and complexities that were similar to ours ," explained Arif. "We also wanted a vendor that offered excellent support, one we could rely on when we needed help."

One Identity Active Roles has been solving the AD administration and security needs of more than 3,500 organizations like Cornell University for nearly 20 years. It overcomes the limitations of native tools with automation, workflows, approval, and centralization of Active Directory account administration tasks such a provisioning and group management. In addition, Active Roles' role-based access paradigm enables organizations to implement security in a least-privileged model for administrators with many flexible security-enabling options such as Temporal Groups and template-based workflows.

"Active Roles provided several key features right off the bat including delegation and sub-delegation, naming convention enforcement, change history and enforcing policies for AD objects," added Arif. "It offered additional flexibility with easy customization of web interface and support of the programming interfaces we use including VBScript, PowerShell and SPML. Its customization capabilities allowed us to implement access in a way that Admins can only view and work on their OUs in AD."

With Active Roles, the University can operate its diverse AD environments with full confidence that nothing can happen unless it is within the established policy (and many actions can now happen with no IT intervention whatsoever). In addition, Admins are only given the permissions they need to do their jobs – nothing more and nothing less – and all actions are audited and tracked, and can even be rolled back if necessary.

"With Active Roles in place, we planned out a good model for managing delegation, naming standards, OU structure and access to AD for several hundred admins... that model has been working for close to ten years now."

Muhammad Arif, Identity Management, CIT, Cornell University

"Because of Active Roles, I believe that the trust in our central IT organization's ability to deliver reliable service has increased – not to mention the reduction in risk and corresponding increase in security."

Muhammad Arif, Identity Management, CIT, Cornell University

"With Active Roles in place, we planned out a good model for managing delegation, naming standards, OU structure and access to AD for several hundred admins," said Arif. "That model has been working for close to ten years now. We have also been able to implement new features using scripting, virtual attributes and web customization to meet new requirements."

One major advantage of Active Roles is its ability to expand beyond the confines of AD. The solution also supports Azure AD (and all that it entails), and can be extended to Unix/Linux systems through an Active Directory bridge such as One Identity Authentication Services, and to a high number of web applications via the SCIM standard.

"Since we're an education and research institution, many faculty, staff and students use Linux systems as their primary workhorse," said Arif. "After AD became the central provider for authentication and authorization, we needed a way to integrate the Linux systems with AD for those functions. We use Active Roles to automatically publish Unix attributes based on AD User and Group objects. This empowers departmental administrators to enable user accounts as 'Unix accounts' within Active Roles, which means that the departmental administrators can help themselves without having to send a request to the central IT organization for enabling individual Unix accounts on an as-needed basis."

"Because of Active Roles, I believe that the trust in our central IT organization's ability to deliver reliable service has increased – not to mention the reduction in risk and corresponding increase in security," Arif concluded.

About One Identity

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com