opentext™ | Cybersecurity

Position Paper

# Top 7 Active Directory Challenges—and How to Solve Them

## Table of Contents

# Top 7 Active Directory Challenges—and How to Solve Them

If you're like more than 90 percent of companies today, you use Microsoft's Active Directory to manage your user accounts and access to your network resources. Created in 2000, Active Directory was designed to be a one-stop shop for authentication and authorization across the enterprise.

But it was never a perfect solution, and the IT world has expanded enormously since it was created. Active Directory has significant limitations for IT administrators, especially when it comes to security. Here are seven of the most serious Active Directory challenges and some suggestions for resolving them.

Managing privileged accounts—those with access to high-level administrative controls over identities, group policies, or domain resources—is essential for enterprise security.

## 1. External Threats

Managing privileged accounts—those with access to high-level administrative controls over identities, group policies, or domain resources—is essential for enterprise security. To maintain a tight ship, organizations should always follow the principle of least privilege, giving everyone precisely the access they need to do their jobs, no more and no less.

Cyberthieves are well aware of this problem and target Active Directory administrators through phishing emails. The best practice is to provide these admins a separate username and password for ordinary internet use, so if their credentials are compromised, the thief won't gain control of the organization. But not all busy IT departments do it. One study found that over 50 percent of organizations allow administrators to use the same credentials for everything, whether they're configuring Active Directory settings or checking their email.

Someone who gains control of a highly privileged account can control your entire IT infrastructure. They can shut down your operations, damage your systems, and steal the personal information of your customers, partners, and employees, as well as your business secrets.

Once you find out—which may take months—you can restore your system to a previous version, but the hacker may have installed secret back doors allowing them to gain access again.

**Solution: Unauthorized Access Prevention**
Ensure the right controls are in place to mitigate the damage that hackers who gain access to Active Directory credentials can do. NetIQ Directory and Resource Administrator (DRA) by OpenText™ enables granular delegation so AD admins guarantee that the fewest people have full administrative rights. Workflow automation can incorporate approval processes to help prevent unauthorized access in the case of hijacked credentials.

NetIQ Change Guardian by OpenText™ can also with real-time, exceptionally readable alerts enable you to identify and respond to potential threats quickly. Improved security information and event management capabilities provide the who, what, when, and where of a change, for when you need the enriched security event data.

## 2. Privilege Abuse

Active Directory does not contain automated privilege management tools natively. At many organizations, IT administrators—even help desk staffers, who need very limited access—are given blanket permission to the "keys of the kingdom"—the critical systems that keep the enterprise running.

Companies must have a strategy for mitigating risks around insider attacks, which constitute 34 percent of breaches, according to Verizon's 2019 Data Breach Investigations Report. A disgruntled employee can wreak havoc, as the Canadian Pacific Railway found out after a departing IT administrator deleted files, removed accounts, and changed passwords, wiping his laptop and destroying all the change logs before returning it to the company.

Companies must have a strategy for mitigating risks around insider attacks, which constitute 34 percent of breaches, according to Verizon's 2019 Data Breach Investigations Report.

Insiders can also steal trade secrets, as happened when an engineer left a company to start his own firm—with over $400,000 worth of his former employer's proprietary information in hand. Theft of intellectual property amounts to $600 billion a year, according to the Commission on the Theft of American Intellectual Property.

**Solution: Granular Controls**
You can manage privileged accounts with much more granular controls than Microsoft offers by using NetIQ Directory and Resource Administrator to manage your Active Directory accounts and permissions.

This tool allows you to delegate access so that all employees—including IT workers—can easily get to the applications and data they need, but can't see or make changes to critical systems they shouldn't be managing. Admins with access to sensitive systems or data are given a different username and password to use for other tasks, and account management is much simpler.

## 3. Scripting Errors

Managing PowerShell, Microsoft's tool for configuration and system administration of Active Directory, is a complex endeavor, and many IT administrators write scripts to handle some of the processes for them.

But writing scripts is time-consuming, and because it's done manually, it's error-prone. Scripting errors can bring down systems, interfere with other scripts, or inadvertently bypass important security protocols. Human error and system glitches cause 49 percent of data breaches, according to the Ponemon Institute.

Another problem is that while a script may be perfectly intelligible to its creator, it can read like hieroglyphics to other administrators, due to the complex and administrator-specific scripting tactics and preferences. Many organizations have no idea how many scripts they have or whether they contain conflicts or violate security procedures.

**Solution: Automation**
With DRA, you can build automated management controls into Active Directory, eliminating the need for scripting and ensuring that your security policy is enforced at all times. Whether you're provisioning new users, connecting new servers or virtual machines, or disabling a departing employee's access, the process can be fully automated, saving you hours that you can spend working on high-level projects instead.

Our tools allow you to manage Active Directory and Azure AD together in one place, simplifying the process and ensuring consistency for authentication and authorization.

## 4. Azure Management Blues

As Microsoft pushes deeper into the cloud, more companies are using Azure Active Directory. Azure is a wonderful resource, but if you use Active Directory in the Azure cloud, you will need to create new users, new groups, and new policies, then manage them separately from those in the Active Directory system you already have. That's a pretty big administrative burden. Additionally, with Azure AD comes another management console, as well as understanding the complex and encumbering administrative controls for the Help Desk and Line of Business administrators, who need to perform day to day operations for these objects. Furthermore, administrators need to ensure that business policies and naming conventions remain consistent both on premise and within Azure AD.

**Solution: Unified Azure Management**
Our tools allow you to manage on premise Active Directory and Azure Active Directory within a single pane of glass, alleviating the swivel chair management of having multiple administrative consoles, as well as providing the ability to delegate the right level of access to the right admins across the expanding Hybrid Microsoft enterprise.

## 5. Microsoft Application Overload

If you're a Windows shop, you probably use Office 365, Skype for Business, and maybe Microsoft Exchange. To manage these applications, you need to use separate, unconnected consoles or web portals—unless you write scripts (see Scripting Errors above). Because these applications store and share critical information across your IT systems, they require constant maintenance.

**Solution: Application Consolidation**
With DRA, you can manage Office 365, Skype, and Exchange on a single web console, without having to log into application-specific management consoles, as well as removing the need for comprehensive and elevated scripting.

NetIQ AD Bridge lets you manage and secure all your Linux and UNIX resources in Active Directory.

## 6. Managing Outside Systems

As you know if you run Linux/UNIX servers, servers, Active Directory doesn't work with them. That means all the security policies you so carefully set up don't apply to some of your most important services, such as point-of-sale machines and customer-facing applications. These are places where maintaining security is of the utmost importance.

As the use of Linux/UNIX servers expands, the problem will only grow. You will need to log on to different operating systems all day to manage multiple identities—often for the same people. Given that organizations use Linux/UNIX machines in order to achieve efficiency and scalability, it's the ultimate irony.

**Solution: A Bridge for Non-Microsoft Resources**
NetIQ AD Bridge by OpenText™ lets you manage and secure all of your Linux and UNIX resources in Active Directory. All the privilege, delegation, and policy management tools you use in AD now apply to all users and data in other operating systems. You manage everything from a single location.

That means your authorization and access policies are automatically and consistently enforced in the cloud, in the hybrid environment, and at home. NetIQ AD Bridge allows you to maximize your existing Active Directory investment and seamlessly expand as you extend your cloud infrastructure. It's truly a bridge to the future.

## 7. Auditing Headaches

Compliance regulations have multiplied in recent years, with no end in sight as lawmakers respond to concerns about data misuse.

It's not enough to have compliant policies. You need to prove to auditors that they're working. The only way to do that is to have a thorough and responsive audit trail.

Microsoft systems are certainly thorough—they create a log for every micro-event behind an address change or a new permission. But sorting through the massive sets of information to find what auditors are looking for is quite a chore.

**Solution: Better Visibility and Awareness**
With DRA, all audit data, to include who, what, where, and when an object was modified and are stored in a secure location and the data cannot be tampered with. Additionally, DRA reporting allows for the audit details to be exported into easy to understand reports, to give the contextual data needed for the audit and compliance teams.

NetIQ Directory and Resource Administrator and NetIQ AD Bridge greatly simplify management by automating and enforcing your policies across all your operating systems, saving you time and money and bringing you the kind of security you need in the age of the cloud.

## Learn More

Active Directory is a vital enterprise resource, but it is difficult to manage and it's not inherently secure. Unless you use a strong complementary service to manage it, it's all too easy to you expose your organization to serious security risks, compliance violations, and errors that lead to system breakdowns. NetIQ Directory and Resource Administrator (DRA) and NetIQ AD Bridge greatly simplify management by automating and enforcing your policies across all your operating systems, saving you time and money and bringing you the kind of security you need in the age of the cloud. To learn more click here.

**About NetIQ by OpenText**
OpenText has completed the purchase of Micro Focus, including CyberRes. Our combined expertise expands our security offerings to help customers protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. NetIQ Identity and Access Management is part of OpenText Cybersecurity, which provides comprehensive security solutions for companies and partners of all sizes.

**Connect with Us**

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.