opentext™ | Cybersecurity

Position Paper

Privileged Accounts: Securing Your Active Directory Environment

To protect your company from security breaches, you must carefully control internal access to sensitive information, and Windows won't do it for you. Here's what you need to do.

If your company is like 95 percent of Fortune 1,000 organizations, you have Microsoft Windows and use Active Directory to manage your company's user authentication and access. You also have a security operations center that actively monitors for threats. These controls make you feel pretty safe.

But are you? Probably not as much as you think.

When a Microsoft Active Directory expert asked security penetration testers how successful they were when attempting to hack their own companies' systems, the testers said that 99 percent of the time, they were able to gain access to administrative privileges and hack their companies' "crown jewels"—the most sensitive and important information they needed to protect.

Here's what you need to know about Active Directory and how to use it to keep your company safe, instead of opening the door to deadly attacks.

Yet when the same expert questioned companies' Active Directory administrators, they said it would be impossible to breach the system.

Clearly, that's not the case.

The truth is, when Active Directory is managed properly, it greatly reduces the chances of a breach and helps your security operations center by providing an early warning if there's trouble. But too many organizations ignore security in Active Directory. They may not realize it, but they are providing both the means and the opportunity for unauthorized users to steal information and wreak havoc.

Here's what you need to know about Active Directory and how to use it to keep your company safe, instead of opening the door to deadly attacks.

Why Is Active Directory Important?

Active Directory is Windows' system for connecting users to resources. It's what enables people to get to the applications, databases, and equipment they need to do their jobs. Everyone in your company has an account in Active Directory and is assigned rights that let them work with resources.

Within Active Directory are privileged accounts, which have far more rights than others. These accounts usually belong to system administrators, network engineers, database managers, and other administrators who have access to critical systems.

Not surprisingly, they are a frequent target of hackers. Sometimes privileged accounts are compromised by outside phishing schemes. Other times, they are misused by malicious insiders.

If you want to keep your information and resources safe, it’s critical to control your privileged accounts in Active Directory. Once an unauthorized person takes control of a privileged account, they can add new accounts or escalate the privileges of existing ones. They can lurk undetected in your system, tapping into applications and databases while they decide what to steal or manipulate.

Someone with access to a privileged account could create a new user, add them to the finance group, log in under the user’s account, and access the enterprise financial system. From there, they could set themselves up as a supplier, submit phony invoices, and get paid. This has actually happened.

Fortunately, OpenText has a comprehensive system that does the best job possible of keeping privileged accounts under control and alerting your security team if anything starts to go wrong.

To avoid such calamities, you need to manage your privileged users very carefully. And Windows won’t do it for you.

That’s right—Windows does not protect you from Active Directory misuse. You have to do it yourself.

Fortunately, OpenText has a comprehensive system that does the best job possible of keeping privileged accounts under control and alerting your security team if anything starts to go wrong.

Here are the four pillars of the NetIQ privileged accounts solutions by OpenText™:

- **Reducing the number of privileged accounts.** Large and mid-sized companies give privileged access to many people—often, too many. Some organizations have hundreds or even of thousands of privileged accounts, which let administrators, offices, and groups manage their own technology.

  Do they all need access to your critical systems? No. But ferreting out all the users with too many privileges is an enormous undertaking that exceeds the time and resources of many IT departments.

  It’s not just people who are the problem. Windows also grants privileges to service accounts, which are run by operating systems or applications to allow various parts of the network to communicate with each other. Service accounts should be shut down after they accomplish their tasks, but often, they aren’t. These privileged “orphan” accounts provide an ideal opening for hackers or unauthorized users because their activity appears normal and doesn’t raise any red flags.

  So how can you reduce the number of account holders—human or otherwise—with too many privileges?

  OpenText has a tool to locate all your privileged accounts, shut down the ones that are no longer needed, and manage the rest. It’s fast, efficient, and effective. But it’s just the beginning of what you need to do to make Active Directory safer.

- **Restricting what privileged accounts can do.** Eliminating privileged accounts that shouldn’t exist narrows the attack surface. But it still leaves you with a lot of users with privileged credentials and deep access to sensitive information—often more access than they need.

We solved that problem with NetIQ Directory & Resource Administration (DRA) by OpenText, which allows you to restrict on a very granular level what an administrator can do.

Smart security rests on the principle of “least privilege,” or giving people just enough resources to do their jobs, but no more. Many people with administrative access need it only for repetitive functions, such as resetting user passwords. They have no reason to tap into enterprise resource programs or add or delete information in corporate databases, yet at many companies, they have the ability to do that. If one of these employees develops a grudge, or if their account is hacked, enormous damage could result.

NetIQ DRA removes that threat by setting privileges according to job function. It eliminates “privilege creep,” in which someone who once needed access to sensitive information has moved on to a different role, but privileges were never revoked.

You can get even more granular with NetIQ DRA, restricting users at certain times or in certain locations. For example, an administrator setting up a network in Houston during business hours should not be able to access the server in New York at night.

- **Monitoring Privileged Accounts.** Restricting privileges goes a long way toward making Active Directory safer. But there’s still the possibility that people with legitimate access to sensitive information might misuse it, pass it along to others, or get hacked.

  That’s why NetIQ Change Guardian by OpenText monitors everything that happens in Active Directory. It spots any unusual behavior and sends alerts to your security operations center in near-real time. The center can immediately shut off access and begin an investigation before any damage is done.

  NetIQ Change Guardian gives you a detailed log of all activity in Active Directory, helping you meet compliance regulations. Because this log is tedious to read—there may be 20 events associated with a single action—NetIQ Change Guardian simplifies your view so that important changes don’t get lost in a forest of extraneous data.

- **Moving beyond passwords.** Most privileged accounts are controlled by usernames and passwords, just like other accounts. But we’re long past the point where “strong” passwords are safe. To protect these important accounts, you need multi-factor authentication. With OpenText, you can select which security layers you want to add. Our software accommodates text messages, fingerprint recognition, voice recognition, facial recognition, or any combination you choose. Strong authentication won’t keep hackers from trying to break in, but it will make their job a lot harder.

Like the rest of us, bad actors—whether they’re outside attackers or malicious insiders—tend to follow the path of least resistance. Don’t make life easy for them. If you don’t take steps to make Active Directory safer, you’re clearing a path for them to get to your most sensitive information and damage your company.

With OpenText, you allow only the right people to have the right access at the right time. That makes your Windows environment as secure as possible, giving you the best chance of keeping hackers at bay and avoiding a costly breach.

With OpenText, you allow only the right people to have the right access at the right time. That makes your Windows environment as secure as possible, giving you the best chance of keeping hackers at bay and avoiding a costly breach.

Improving the Security Operations Center

The privilege management solution also has a broader benefit: it enables your security operations center (SOC) and security and event management system (SIEM) to be far more efficient and productive.

Traditional SIEM solutions rely on analyzing logs of events from operating systems like Windows. These logs are chock full of discrete events that provide little useful information on an individual basis. For example, there may be as many as eight separate events to indicate the simple renaming of a file.

Reviewing a multitude of events is not only tedious and time-consuming, it diminishes the SOC's effectiveness in spotting suspicious activities and responding to them in a timely manner.

We have a different approach. Each event in our system is given context—it answers the all-important questions of WHO did WHAT, and WHEN and WHERE they did it. These easy-to-read events reduce the time it takes for SOC investigators to see what's going on. As a result, the SOC improves its reaction time and formulates more effective solutions for stopping malfeasance in its tracks.

We have a different approach. Each event in our system is given context—it answers the all-important questions of WHO did WHAT, and WHEN and WHERE they did it. These easy-to-read events reduce the time it takes for SOC investigators to see what's going on.

About 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.

Learn more at
www.microfocus.com/en-us/cyberres/identity-access-management/privilege-account-management

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.