Q:CYBER

Privilege Assurance for Microsoft Active Directory

Protect the heart of your Windows domain network.

Since its release in 2000, Microsoft's Active Directory (AD) has become critical infrastructure for most enterprises. Nearly 95% of all enterprises use Microsoft's Windows domain networks and the beating heart of these domains is Active Directory.[1]

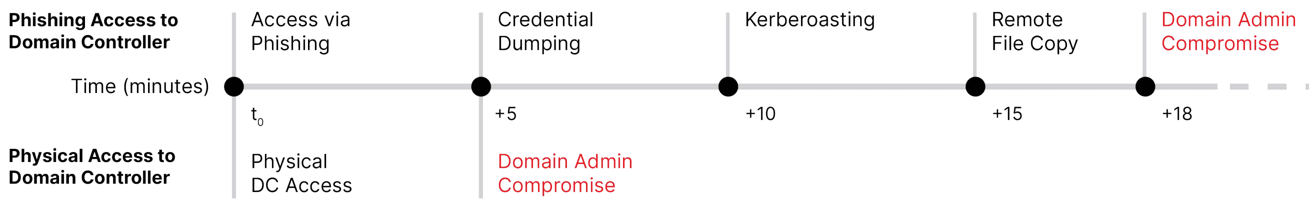
Active Directory is not just a directory. Of course, it is a white-pages directory that lists employees, groups, and managerial relationships. And it is an authentication provider for accounts logins. But it is also a lightweight configuration management database (CMDB) for Windows resources, keeping track of users, hardware, and applications. And finally, it is also a policy enforcement point that implements trust boundaries and enterprise security policies for endpoint devices and software. Because it does all of these things, in one place, it is a tempting target for attackers.

Which is why it comes as no surprise that **over 80% of recent headline-grabbing attacks have involved breaking into Active Directory**.[2] As Ed Amoroso, former CISO of AT&T and CEO of the global cybersecurity consultancy TAG Cyber, cautioned in 2019,

> *"When really good hackers break into your perimeter, when they get in the enterprise, they don't walk, but they run to your Active Directory, because it provides a map of your entire network."* [3]

The consequences of a catastrophic data breach are severe. But the damage from an Active Directory attack extends beyond the breach. It weakens the assurances CISOs provide to their regulators, customers and partners. That's because Active Directory provides authentication for employees—a crucial IT General Control. When authentication is compromised, the integrity of the entire security program is compromised as well.

Attack Path Scenario:



[1] Frost & Sullivan. "Active Directory Holds the Keys to your Kingdom, but is it Secure?" March 2020.
[2] Zonic Group. " Defending Active Directory." 2017.
[3] Ibid.

Avoid an AD Disaster

What Top CISOs Know About Protecting Active Directory

For many years, Active Directory flew beneath the radar of the CISOs attention. But in the past decade, Active Directory's central role in enterprises was instrumental in fueling a wave of devastating ransomware campaigns such as WannaCry and NotPetya:

Maersk: The NotPetya ransomware campaign hit the Netherlands-based global shipping company Maersk and destroyed every Windows asset connected to the network, costing Maersk over $300-million.[4]

Merck: A crippling attack on Active Directory at U.S. pharmaceutical giant Merck resulted in drug shortages and the loss of over $1-billion in sales.[5]

In a recent analysis[6] of over 250,000 endpoint devices from enterprises ranging from mid-sized firms to large enterprises:

- Every single corporate network showed evidence of a targeted intrusion,
- 34% of the threat activities identified involved lateral movement activity, and
- Nearly 10% of all targeted intrusions consisted of "Kerberoasting," an attack method that allows an attacker to crack the passwords of service accounts in Active Directory offline and without fear of detection.

Yet, even as the threat increases, **Active Directory remains too large and complex for Microsoft to secure on its own:**

For most enterprises, **Active Directory is aging, underfunded and complex.** Enterprises find it challenging to stop attackers from exploiting Active Directory, because it needs to be open in order to work, and the ways to configure (and mis-configure) it are endless.

Microsoft cannot be trusted to provide a solution. As Roi Abutbul, co-founder and CEO of Javelin Networks explained in 2019:

> *"Microsoft, at the end of the day, is not a security company: most of their efforts are focused on operational management. Their security solutions are not available today in the market to prevent hackers from stealing domain credentials or from querying and learning about the environment using Active Directory manipulations."*[7]

[4] A.P. Møller - Mærsk A/S. "Interim Report Q2 2017"." August 2017.
[5] Bloomberg. "Merck Cyberattack's $1.3 Billion Question" Was It an Act of War?" December 2019.
[6] APNIC. "New Generation of Attacks Targeting Active Directory Can be Mitigated". 2019.
[7] Zonic Group. " Defending Active Directory." 2017.

Secure Your Success

Protect Active Directory with *QOMPLX Privilege Assurance*.

Implementing comprehensive, reliable, and real-time privilege assurance is the single most critical step you can take to protect your Active Directory environment: *QOMPLX Privilege Assurance* is the solution.

QOMPLX Privilege Assurance accurately identifies weaknesses in your Active Directory environment, spotlights accounts that pose a risk to your organization, and immediately alerts you to concentrated pockets of privileges that malicious actors could exploit.

Instant Implementation: *QOMPLX Privilege Assurance* includes an Active Directory analysis function (built into the Q:Cyber platform) that's delivered via an agent and is installed on a single domain controller in each of the domains inside of a forest.

That means it takes just minutes to install *QOMPLX Privilege Assurance*, map even the most complex, multi-forest AD environments, and illuminate the pathways that attackers may take to your organization's most sensitive and valuable assets.

World-Class Performance: With *QOMPLX Privilege Assurance*, its intuitive design and easy-to-use features makes managing your Active Directory security simple. Key features include:

Effortless Administration	Powerful Analytics
▪ Identify over-privileged accounts, such as non-administrator accounts, with rights to add computers to a domain and other excessive non-admin permissions. ▪ Review password-policy compliance on all accounts, flagging accounts out of policy based on the age of the account password, and identify admin. account passwords with no expiration date. ▪ Identify stale accounts and machines without successful log-ins during a custom time period. ▪ Find end-of-life assets, such as machines running an operating system that's no longer supported and can no longer be patched or updated.	▪ Create analytics for your specific cybersecurity risk management program. ▪ Capture critical forensic data on your Active Directory environment for investigations and audits. ▪ Provide board-level risk metrics that go beyond simple measures of activities. ▪ Visualize blast radius, lateral movement pathways, and attack vectors for hardening your Active Directory security and incident response operations. ▪ Identify and monitor accounts in close proximity to ("one hop away from") sensitive domain administrator accounts.

Q:CYBER

Don’t Accept Defeat. Or Delay.

Defend Your Active Directory with *QOMPLX Privilege Assurance*

With all the new techniques that exist for attacking Active Directory, it’s time to stop thinking about what you’ll do if someone attacks your Active Directory environment, and time to start building your defenses.

From the minute you install *QOMPLX Privilege Assurance*, the benefits are immediate:

Executive Insights	Instant visibility into critical cyber risks that your Board should know about, such as external hygiene exposures or outdated, unpatchable systems.
Management Made Easy	Better identify and manage over-privileged accounts and groups with high privilege concentration.
Better Cyber Hygiene	Rapid improvements to your security posture by identifying and removing unpatched and exposed systems.
Meaningful Metrics	Monitor for security problems with cyber-risk metrics that give you visibility into assets, threats, and risks to your business.

Ready to learn more about *QOMPLX Privilege Assurance*? Contact us today.

+1 (703) 995-4199 | info@QOMPLX.com | www.QOMPLX.com

Why QOMPLX®

QOMPLX makes it faster and easier for organizations to integrate all of the disparate data sources across the enterprise into a unified analytics infrastructure to make better decisions.

This broader analytics infrastructure is provided through QOMPLX:OS, an enterprise operating system that powers QOMPLX’s decision platforms in cybersecurity, insurance underwriting, and quantitative finance.

Headquartered in Reston, VA, QOMPLX, Inc. also has offices in New York and London.
More information about QOMPLX can be found at https://www.qomplx.com