QOMPLX:CYBER

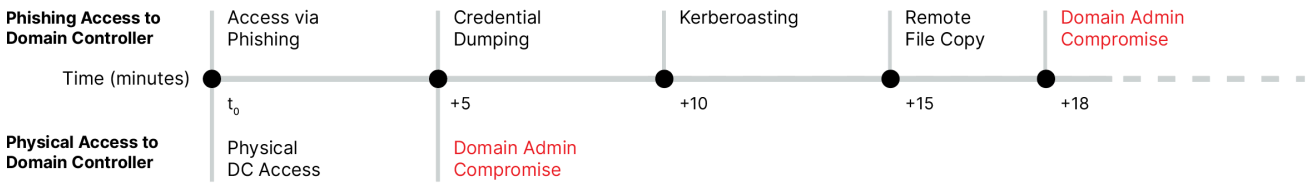
Privilege Assurance

Protect Active Directory (AD) the key controller of your Windows domain network

Active Directory is the beating heart of the enterprise's critical infrastructure. AD fulfills critical functions including identity provider, relationship storehouse, configuration management database, and policy enforcer. As such it is the single point of failure on which most security programs rise or fall.

So it comes as no surprise that most headline-grabbing attacks involve breaking into AD. As Ed Amoroso, former CISO of AT&T and CEO of the global 2 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."[1]

Since AD provides authentication for employees, when authentication is compromised, the integrity of the entire security program is compromised.



Avoid an Active Directory (AD) disaster

In the past decade, the central role of AD 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.[2]

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.[3]

In an analysis of over 250,000 endpoint devices from medium to large enterprises:[4]

---

[1] Zonic Group. "Defending Active Directory". 2017.

[2] A.P. Møller – Mærsk A/S. "Interim Report Q2 2017". August 2017.

[3] Bloomberg. "Merck Cyberattack's $1.3 Billion Question. Was It an Act of War?" December 2019.

[4] APNIC. "New Generation of Attacks Targeting Active Directory Can be Mitigated". 2019.

- 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 AD offline and without fear of detection.

Enterprises find it challenging to stop attackers from exploiting AD, because it needs to be open in order to work, and the ways to configure (and mis-configure) it are endless.

Quickly visualize, monitor, and protect your AD

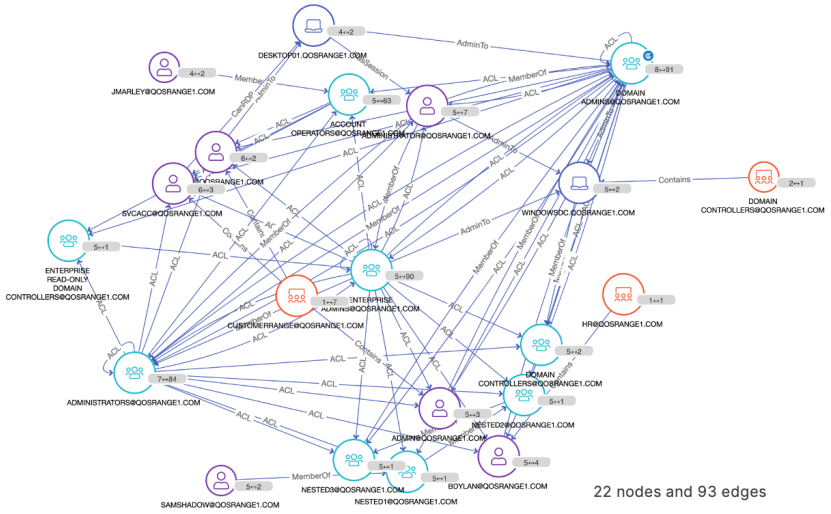
Implementing reliable privilege monitoring is the most critical step to protect your AD environment: QOMPLX Privilege Assurance is the solution.

It accurately identifies weaknesses in your AD environment, spotlights high risk accounts, and immediately alerts you to pockets of privileges malicious actors could exploit.

The Privilege Assurance graph view allows customers to explore attack paths and analyze “blast radius” of compromised assets.

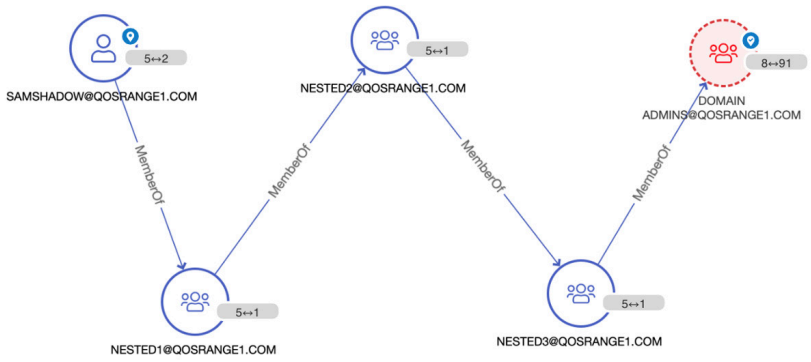
Blast radius

shows all nodes that an attacker can reachafter compromising a given start node.



Attack path

displays the pathways an adversary can use to reach a target from a start point, using a configurable number of “hops.”



QOMPLX:CYBER

High value visualizations

Our best-in-class Privilege Assurance with graph view visualization tool, enables you to see the attack paths to your high value targets, predict damage by seeing the “blast radius” of a potentially compromised asset, and see highlighted misconfigurations that can cause harm.

Fast implementation

QOMPLX Privilege Assurance includes an AD analysis function delivered via easy to install collector - one per forest. It takes just minutes to install, map 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 monitoring your Active Directory [AD] 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.	■ Provide board-level risk metrics that go beyond simple measures of activities.
■ 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.	■ Visualize blast radius, lateral movement pathways, and attack vectors for hardening your Active Directory security and incident response operations.
■ Identify stale accounts and machines without successful log-ins during a custom time period.	■ Identify and monitor accounts in close proximity to sensitive domain administrator accounts.
■ 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.	■ Identify “Kerberoastable” accounts that are likely at risk of compromise.

QOMPLX:CYBER

Defend Your Active Directory with QOMPLX Privilege Assurance

It's time to stop thinking about what you'll do if someone attacks your AD environment, and time to start building your defenses.

With QOMPLX Privilege Assurance, the benefits are immediate:

- **Executive Insights** for critical cyber risks that your Board should know about.
- **Monitoring Made Easy** to identify over-privileged accounts and groups .
- **Better Cyber Hygiene** by identifying and removing unpatched and exposed systems.
- **Meaningful Metrics** with visibility into assets, threats, and risks to your business.

Ready to learn more about QOMPLX:CYBER?

Contact us today.

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

Why QOMPLX®

QOMPLX harnesses data to provide unified visibility into cyber risks and trust in identity. QOMPLX solutions reduce cyber risk and attack surfaces by mapping exposures and performing real-time detection of attacks. This approach increases network observability by closing the largest remaining gaps in cybersecurity: identity verification, cross-tool data fusion, and data interoperability. QOMPLX defends some of the world's most renowned brands by re-establishing trust for client organizations, assuring authentication, and enabling confident security decisions.

For more information, visit **qomplx.com** and follow us **@QOMPLX**.