QOMPLX:CYBER

Identity Assurance

Protect critical data on-premise and in the cloud

Authentication is the most important technology control because identity is fundamental to your organization's activities. Attackers abuse your organization's critical control infrastructure to create fraudulent credentials and gain administrative privileges while hiding their tracks.

Data breaches cost companies an average of $3.86 million per instance, according to the IBM's 2020 Cost of a Data Breach report. And, the companies in the report said the timeline to identify and contain breaches was 280 days. QOMPLX can help protect your business and your reputation from damage.

Identity authentication is the key control

In a world where thousands of data breaches can cause trillions of dollars in damage, you need software that can quickly detect attacks against your own organization, both on your servers and in your cloud.

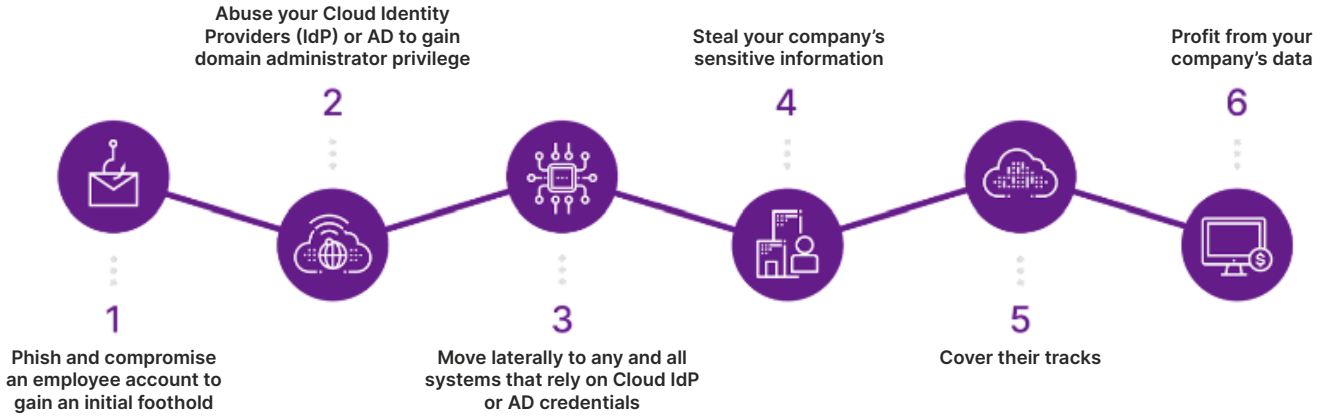
Identity authentication is the single most important technology control because all IT general controls — including authorization, entitlement management, change management, incident management, software lifecycle, and business continuity — depend on it.

Verify every identity transaction

Since its launch, QOMPLX Identity Assurance has offered unparalleled detections for Golden Tickets, Silver Tickets and other Kerberos attacks. Our Identity Assurance capabilities bring detection, safety, and security to companies' cloud applications and expand capabilities in the on-premise environment.

Enterprises authenticate their employees, customers, and partners before authorizing them to access systems, processes, and data. QOMPLX Identity Assurance provides solutions for both cloud and on-premises servers by utilizing external validation that each user who requests access is who they say they are in just minutes. Identity Assurance disrupts attacks by detecting the techniques common to nearly all large-scale breaches, including credential forgery and privilege escalation.

Cloud and third-party applications rely on Active Directory (AD) credentials to permit single-sign-on. Unfortunately, bad actors regularly attack both on-premises targets like AD and related critical control infrastructure. Similar to the $1.4 billion Equifax breach in 2017, most catastrophic data breaches of the past decade follow that playbook:



Minimize alert fatigue

Given resource constraints and the shortage of qualified cybersecurity professionals, many organizations are looking for software to intelligently ingest, parse, monitor and correlate events in order to reduce false positives and minimize alert fatigue for SOC analysts. With our Q:CYBER 6.0 update, we provide enhanced visibility into our collectors and ledger to further distinguish between mere insights and true alerts that require human intervention.

Key features

QOMPLX Identity Assurance solution ensures that identities issued by Active Directory (AD) domain controllers and cloud identity providers (IdPs)[1] are valid and that they implement authentication protocols correctly.

Unlike our competitors, QOMPLX Identity Assurance software validates the authentication protocol itself without resorting to time-delayed "rule of thumb" heuristics. It also automatically detects catastrophic cyber attacks in near real-time and filters the most relevant data to your security operations team.

Features include:

- **Attack Detection Templates:** Use QOMPLX pre-built templates, aligned with the MITRE ATT&CK® framework, to detect and alert on common Kerberos and SAML attack techniques including pass the hash, pass the ticket, overpass the hash, skeleton key, and kerberoasting.
- **Advanced Detections:** On top of the industries' most accurate detections and stateful Kerberos protocol validation tools, we offer 100+ built-in rules and detections all aligned to critical MITRE ATT&CK tactics.
- **Administrator Console:** Verify that your firm's most important control is working as designed, with real-time updates. Take action with built-in incident management tools.

[1] For supported cloud Identity Providers (IDPs).

- **Asset Discovery:** Identify all Active Directory (AD) domain controllers on your network, not just those in your official inventory system. Ensure that your asset inventory is complete and up-to-date.
- **Integrations:** Using QOMPLX 50+ integrations, ingest, parse and normalize additional contextual data from popular sources including Windows Event Logs. Send resultant alerts to external log management or SIEM products.

Benefits

When attackers compromise authentication, the organization is compromised catastrophically. All other IT general controls are also compromised. To stop attacks before they damage your organization, QOMPLX Identity Assurance helps you:

- **Secure Active Directory and cloud Identity Providers (IdPs):** Address a top CISO and CIO priority— strengthening your Active Directory and cloud Identity providers (IdPs) against attack.
- **Detect Attacks:** Detect stealthy attacks on Active Directory and Kerberos including Golden and Silver Ticket and Kerberoasting, password spraying, pass-the-ticket, pass-the-hash, ntds.dit extraction, domain enumeration, LDAP reconnaissance, DCSync, DCShadow, skeleton key.
- **Shorten Dwell Time:** Shorten attacker's dwell time with timely detection in minutes or hours rather than weeks or months.
- **Enhance the Value of Existing Security Tools:** Reduce the load on your existing security tools including log management, security and incident management, and endpoint detection.
- **Maintain Control:** Ensure that your most important IT general control — authentication — operates with integrity.

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**.