Worried about identity security?

Protect your critical data on site 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, 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.

Challenge

In a world where thousands of data breaches can cause trillions of dollars in damage, you need software that can detect and prevent a catastrophic data breach against your own organization, both on your servers and in your Cloud. We can protect you.

Authentication is the single most important technology control because identity is fundamental to your organization's operations and security program. That's because all IT general controls — including authorization, entitlement management, change management, incident management, software lifecycle, and business continuity — depend on it.

Risk is a consequence of dependence — everything depends on authentication.

Solution

QOMPLX's Identity Assurance has historically been the foremost line of defense against Golden Ticket and Kerberos attacks. Identity Assurance's new capabilities bring detection, safety, and security to companies' cloud applications.

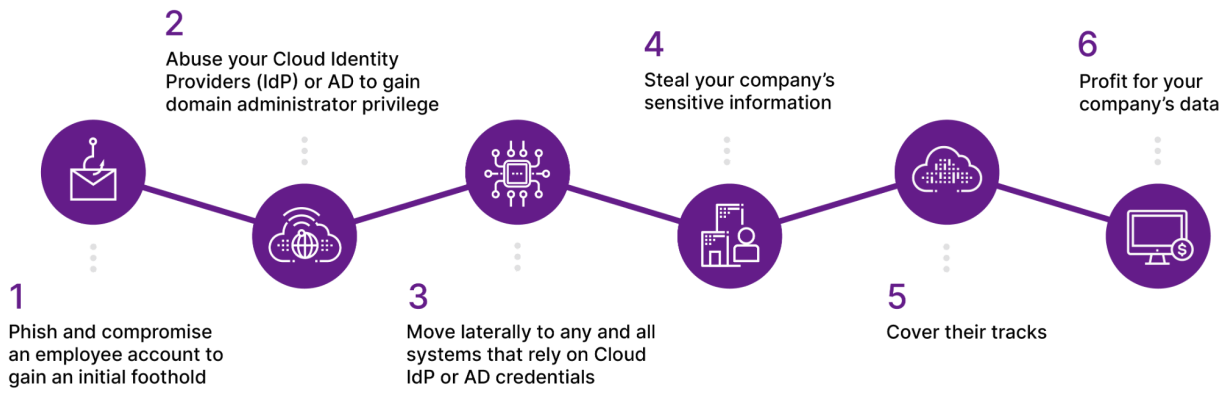
QOMPLX's Identity Assurance software has offered patented detections for Golden Tickets by externally validating the underlying Kerberos protocol and making it stateful. Building on this success, we've now patented and are now offering detections for attacks to cloud authentication, like SAML assertion forgeries.

Enterprises authenticate their employees, customers, and partners before authorizing them to access systems, processes, and data. QOMPLX's Identity Assurance provides solutions for both the Cloud and on-premises servers by validating that each user who requests access is who they say they are, 100% of the time[1]. Identity Assurance disrupts attacks by detecting the techniques common to all large-scale breaches, including credential forgery and privilege escalation.

[1]Deterministic detections, when properly configured.

Q:CYBER

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. Like the $1.4 billion Equifax breach in 2017, most catastrophic data breaches of the past decade follow a similar playbook:



Key features

QOMPLX's Identity Assurance solution ensures that all Active Directory (AD) domain controllers and cloud identity providers (IdPs) correctly verify each authentication transaction and implement the correct protocol, whether that's the Kerberos protocol or the SAML protocol.

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

- **Attack Detection Templates:** Use QOMPLX's 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:** Detect and alert on advanced Kerberos attacks including Silver Ticket, Golden Ticket attacks, DCSync, and DCShadow — with the industries' most accurate detections and stateful Kerberos protocol validation tools.
- **Administrator Console:** Verify that your enterprise's most important control is working as designed, with real time updates. Take action using built-in incident management tools.
- **Asset Discovery:** Identify all Active Directory (AD) and Active Directory Federated Services (ADFS) domain controllers on your network, not just those in your inventory. Ensure that your asset inventory is complete and up-to-date.
- **Connectors:** Using QOMPLX's 50+ connectors, ingest, parse and normalize additional contextual data from popular sources including Windows Event Logs. Send resultant alerts to external log management or SIEM products.

Q:CYBER

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's Identity Assurance helps you:

- **Secure Active Directory:** 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, DC-Sync, DC Shadow, 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's Identity Assurance options*? Contact us today.

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

Why QOMPLX®

QOMPLX is the cloud-native leader in risk analytics. We help organizations make intelligent business decisions and better manage risk through our advanced, proprietary analytics platform. We are the leaders at rapidly ingesting, transforming, and contextualizing large, complex, and disparate data sources through our data factory, in order to help organizations better quantify, model, and predict risk in areas like cyber security, insurance, and finance. QOMPLX is headquartered in Tysons, VA with offices in New York, Denver, London, Cambridge, Oxford, and Montevideo. More information about QOMPLX can be found at https://www.qomplx.com/.