Identity Assurance for Cloud Tech Spec

Protect your cloud-based authentication

For nearly 10 years, QOMPLX's Identity Assurance software has been the world's foremost line of defense against Golden Ticket and Kerberos attacks. Now, Identity Assurance's new Cloud Identity Forgery detections bring world-class safety and security to your company's cloud identity providers (IdPs), like Active Directory Federated Services (ADFS).

QOMPLX's Identity Assurance for Cloud combines advanced data science techniques with data to capture SAML forgeries relevant to your cloud IdPs.

Approach and methodology

QOMPLX's Identity Assurance software offers new Cloud Identity Forgery detections for SAML tokens by using a ledger and making it stateful. By keeping a record of transactions, Identity Assurance knows users are who they claim to be, 100% of the time with no false positives.[1]

Identity Assurance validates that each user who requests access is who they say they are. Enterprises authenticate their employees, customers, and partners before authorizing them to access systems, processes, and data. Identity Assurance disrupts attacks by detecting the techniques common to all large-scale breaches, including credential forgery and privilege escalation.

Hackers abuse trust in federated authentication environments, like ADFS and AWS, to steal protected data. Once a hacker has gained initial access to your cloud network, stealing your company's data is practically effortless:

- First, hackers leverage privileged access in the cloud environment,
- Then, moving laterally, they subvert the security mechanisms organizations use to grant access to cloud resources,
- Finally, they seize administrator credentials and take control of cloud resources.

Hackers are not exploiting a vulnerability in ADFS, AD, or even AAD (Azure Active Directory). Rather, they're abusing the trust established across the integrated components, which is why authentication is so crucial to security.

[1] Deterministic detections, when properly configured.

Cloud and third-party applications rely on the credentials authenticated by directory services software, like those found in AD and ADFS, to permit SSO (single-sign on). Directory services providers may also manage Windows server and desktop configurations, enforce desktop and network security policies, and keep inventories of technology assets. These are, in effect, a security policy enforcement point, a lightweight configuration management database, and source of group entitlements. AD and ADFS are commonly the most critical infrastructure asset any organization manages.

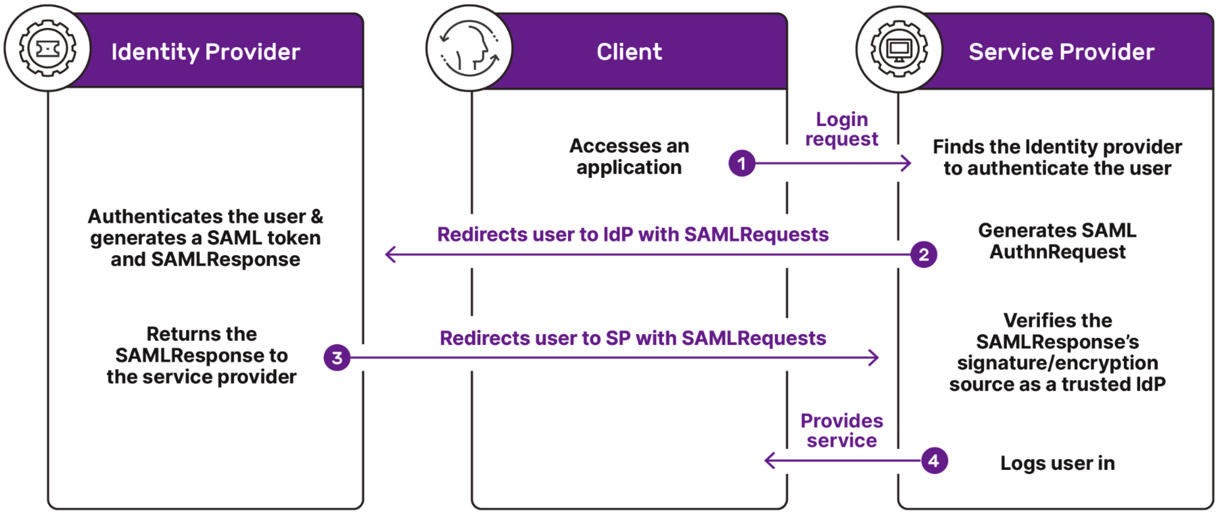
Identity Provider
Client
Service Provider
Accesses an application
1
Login request
Finds the Identity provider to authenticate the user
Authenticates the user & generates a SAML token and SAMLResponse
Redirects user to IdP with SAMLRequests
2
Generates SAML AuthnRequest
Returns the SAMLResponse to the service provider
3
Redirects user to SP with SAMLRequests
Verifies the SAMLResponse's signature/encryption source as a trusted IdP
Provides service
4
Logs user in

Figure 1

As Figure 1 demonstrates, as bad actors dig deeper into networks, SAML becomes a very attractive target for privilege escalation and achieving persistent, undetected access using methods such as SAML.

Credential forgery and privilege escalation techniques have become common factors in every large-scale attack and cyber breach of the past five years. Before now, such techniques have been virtually impossible to detect without the focused efforts of experienced incident responders conducting manual forensic analysis.

Identity Assurance works because it focuses on validating the protocol. Identity Assurance delivers a response in minutes, not days, to a company's security team so that they may respond quickly and decisively to an attack.

More so, Identity Assurance's detections give clients a context-rich picture of user behavior over time for confident and timely detection of these other AD-based and cloud-based attacks. including:

Deterministic Detections:

- Golden Ticket Detection
- Silver Ticket Detection
- DCSync Detection
- DCShadow Detection
- Cloud Identity Forgery (aka, "Golden SAML") Detection

Heuristic Detections:

- Skeleton Key Detection
- Pass-the-Hash Attack Detection
- Overpass-the-Hash Attack Detection
- Kerberoasting Detection
- ASRepRoasting
- Member Added to Sensitive Group
- Excessive Failed Logon Attempts (Password Spraying)
- Account Name Enumeration (Kerberos)
- Successful Zone Transfer from Unknown Source
- PowerShell Encoded Command Execution
- PowerShell executed in the background
- Discovery using built-in Windows utilities
- Service Installed on a Sensitive System
- Suspicious use of regsvr32
- Honey Account Login
- Honey Account Ticket Request
- AdminSDHolder Modified

Ready to learn more about *QOMPLX's Identity Assurance for Cloud*? 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/.