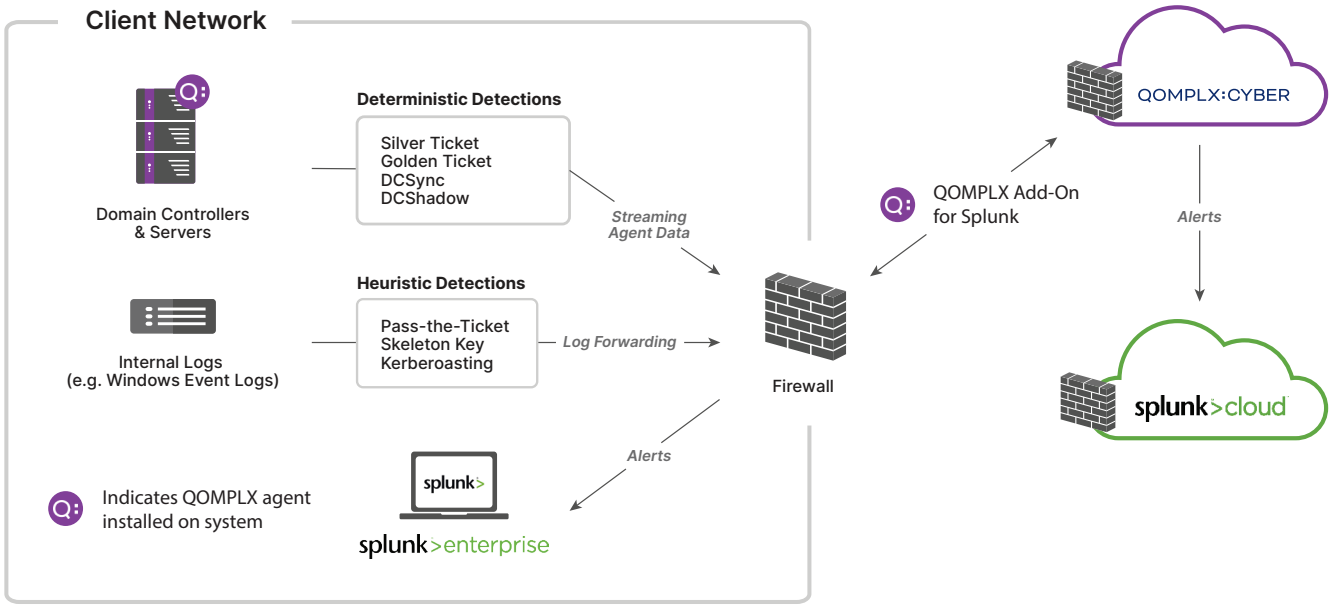
Splunk & QOMPLX
Identity Assurance Solutions Brief

Splunk & QOMPLX Integration

QOMPLX's convenient add-on helps Splunk-based SOCs stop catastrophic cyber attacks more quickly and effectively. The QOMPLX Add-On for Splunk helps users of Splunk® Enterprise and Splunk Cloud™ gain more value from their existing SIEM investments by receiving alerts from QOMPLX's Q:CYBER product, which uses streaming analysis of system logs and Active Directory authentication data to detect identity-based attack techniques involving lateral movement, privilege escalation, and credential compromise.



Elevating Security Operation Center (SOC) Response Capabilities

By providing direct and seamless integration, QOMPLX helps SOCs who use Splunk Enterprise rapidly shut down attack vectors involving critical infrastructures such as Active Directory and the Kerberos authentication protocol, which have been exploited in many of the highest-profile breaches and catastrophic ransomware attacks over the past several years.

With the QOMPLX Add-On, Splunk Enterprise users can view alerts from Q:CYBER directly in their existing Splunk Enterprise or Splunk Cloud instance. Because of the speed and accuracy of these alerts, security teams can use them to quickly confirm suspected attacks or trigger Splunk Phantom orchestration capabilities to respond more promptly and effectively to a potential breach.

Key Features

- **Unique detection:** Q:CYBER is the only solution to offer deterministic detection of Golden and Silver Tickets, DCSync, and DCShadow attacks, in near real-time and without false positives.
- **Timely Alerts:** Most solutions rely solely on batched, heuristic analysis of security log data for detection triggers, generating many false positives and wasting invaluable response time and resources. Q:CYBER's streaming analytics trigger alerts faster, shrinking dwell time to minutes instead of weeks or months.
- **Immediate Time to Value**: Unlike other solutions that require days or weeks of benchmarking, Q:CYBER detection capabilities begin immediately upon agent install and a reset of the KRBTGT service.
- **More Confidence, Not More Noise**: Q:CYBER's proprietary agent data enriches traditional trigger rules with greater context to significantly reduce or eliminate false positives altogether, freeing up analysts to focus on more valuable pursuits.
- **Fast and Simple Integration**: Existing data feeds are augmented seamlessly with Q:CYBER alerts, enabling SOC analysts to correlate events more easily and effectively without having to pivot between applications.

Get more from your SIEM investments
Download the QOMPLX for Splunk Add-On now

Ready to learn more about *QOMPLX Identity 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/.

QOMPLX:
Reimagining Complexity

About Splunk, Inc.

Splunk Inc. (NASDAQ: SPLK) turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, and analyze and act on data at any scale.

splunk>