MDR that really works

Dental healthcare company successfully gains control over Active Directory across all offices after replacing a major MDR vendor

1.
A leading consumer retail dental healthcare company needed visibility and to clean its active directory while also implementing authentication controls, and detecting high-risk misconfigurations

2.
The client's previous vendor provided generic reporting that lacked context and best practices for a hygienic Active Directory

3.
QOMPLX provided a view of their active directory and instituted an identity-centric strategy that reduced the risk of breaches

Challenge

With roughly 400 offices serving more than 8 million patients, our client had limited resources to manage a sprawling active directory rife with vulnerabilities. And when their former vendor delivered generic reports that lacked context, action items, and a comprehensive plan to identify and respond to threats, preserving their cybersecurity became a race against crime.

Whether it's size, shape, or function, in dental healthcare, every tooth has a specific purpose and one misalignment can be painful. As our client that focuses on tooth replacement solutions knows all too well, the same principles of customization, proper maintenance, and tireless vigilance also apply to cybersecurity.

INDUSTRY:	Healthcare - Dental
HEADQUARTERS:	North America
EMPLOYEES:	1000+
OFFICES:	Across the U.S. Mid-Atlantic area
KEY PRACTICE AREAS:	■ Dental ■ Healthcare ■ Health Diagnostics
ANNUAL REVENUE:	USD<$10 million

Solution

The client selected QOMPLX for its:

- **Attention to detail:** Beyond a standard summary with toplines and alerts, QOMPLX provides expert analysis, contextual alert data, and actionable steps so companies can act and plan with confidence
- **Attack Surface Monitoring via Q:SCAN:** Assigns a risk score indicative of an organization's level of external exposure and helps identify threat vectors that when addressed, will lower the score
- **Managed Detection and Response (MDR):** Identity-centric managed detection and response that monitors, hunts, detects, and responds to threats
- **Privilege Assurance:** Monitors active directory risks including vulnerable users and groups, attack paths, and often-exploited misconfigurations.

Impact

Driving an identity strategy focused on Active Directory was instrumental in helping our client remove outdated users and groups, identify risks, and eliminate often exploited attack vectors.

To gain the insight needed for its identity threat prevention and protection, the QOMPLX security operations center provides our client with a contextualized report that details their entire environment and includes recommended action items to keep malicious actors at bay.

Now, our client has complete visibility into their active directory ecosystem, allowing them to focus on other business priorities.

> With an accurate active directory, air-tight authentication controls, and detection against active directory privilege exposures, our client can smile again.

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.