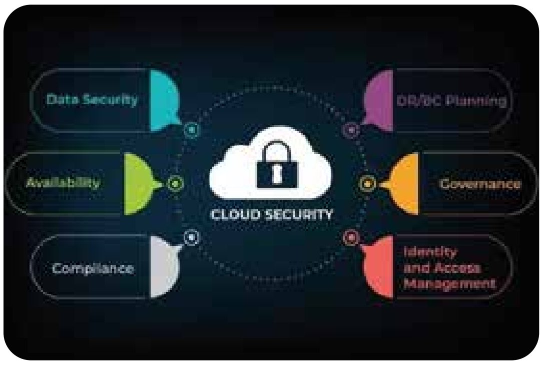
HALO Zero Trust Cybersecurity

Overview



Cloud computing attracts different users owing to its high resources elasticity and scalability which provide important savings in terms of investment and manpower.

Cloud minimizes the need for user involvement by masking technical details such as software upgrades, licenses and maintenance from its customers.

HALO's vast experience in securing complicated multilevel secure networks for militaries working in allied and coalition operations gives us the edge against traditional approaches when designing an efficient, secure, but authorized user-accessible solution.

Challenges and Threats

A Zero Trust Architecture (ZTA) is not a single architecture. It is a set of guidelines for the design of systems and operations that intends to tighten the security to protect industrial and enterprise assets.

Data Security

Our attention to data security and privacy in the cloud means your information is secure for its confidentiality, integrity and availability.

There are several cyber-security threats that may face the cloud services availability. To ensure the safety and the availability of data, HALO works with end users to develop and maintain an appropriate action plan for risk management to deal efficiently with these threats and to guarantee the cloud based services continuity.

Cloud Network Infrastructure Security

Our secure designs can accept trustful network traffic and block malicious network traffic.

Cloud Applications Security

Cloud applications security is akin to web applications security when hosted in data centers. Most providers propose single sign on (SSO) as a solution to allow users to access multiple individual cloud services. However, it is hard to implement SSO solutions correctly.

HALO's authentication methods require a secure software layer. To ensure cloud applications (APIs) security, we employ a rigorous testing process to simulate threats well beyond traditional methods used to meet accepted industry standard. We go beyond, using independent experts to validate our solution, and find and fix problems before any attacker can see our networks.

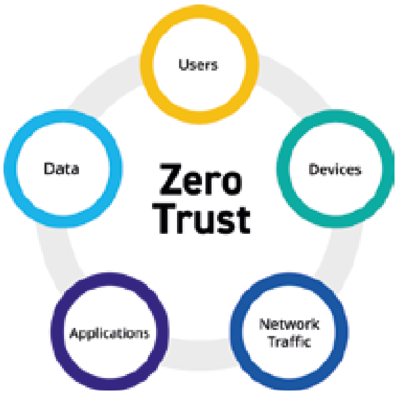
Zero Trust Architecture

A Zero Trust Architecture (ZTA) is not a single architecture. It is a set of guidelines for the design of systems and operations that intends to tighten the security to protect industrial and enterprise assets.

The traditional approach has focused on stopping attackers from getting in, physically or electronically. This doesn't help prevent internal attacks or attacks where an external intruder poses as an internal user.

Essentially, HALO's solution trusts no one (Zero Trust) until they are authenticated and have proven who they are and that they should have access to the requested resource.

HALO's Zero Trust Architecture or Zero Trust Access describe products or services that creates the boundary around one or more applications. It shields the application or service from public view and only allows access to users and devices that have explicit verifiable access.



Where **Innovation**
meets **Infrastructure**
and **Productivity**
meets **Progress**

HALO INTERNATIONAL FZE

Cyberattack Leaders

Global average weekly cyberattacks increased by 7% in Q1 2023 compared to the same period in 2022, with each organization facing an average of 1,248 attacks per week. This increase was led by new support tools such as ChatGPT. Cybercriminals have begun using ChatGPT for code generation and allowing less-skilled actors effortlessly launch cyberattacks.

The Education and Research sectors were the most heavily targeted, experiencing a 15% increase and followed by Military and Government who were also up by 3%.

The APAC region experienced the most significant year-over-year increase, with a surge of 16%, reaching an average of 1,835 attacks per organization.

IoT Threats

Connected smart devices have been gaining momentum. These include sensors, wearable devices, etc. These devices, also known as the Internet of Things (IoT), have to be based on the existence of a safe, secure, and capable network.

HALO's team is experienced in protecting commercial, government and military networks from IoT threats.

Security

Suppliers have had trouble going beyond their traditional domains like device authentication and network reliability. Since breaches can occur at the device, level, app, storage, and data level, HALO tests for IoT vulnerabilities.

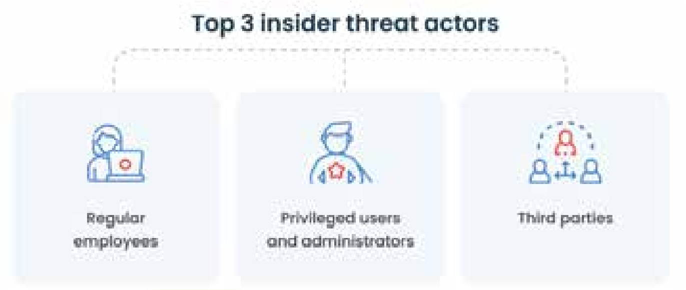
System's health monitoring

IoT is introducing highly technological sensors that can monitor a system's health status. These tools do more than simply alert the operator to a malfunction. They combine sensor input and data analytics to offer predictive analytics data for failures or malfunctions long before they appear.

Data storage

Using military based procedures, HALO's data storage capability for operations complies with many technical specifications above standard commercial solutions.

Insider Threats


Top 3 insider threat actors
Regular employees
Privileged users and administrators
Third parties

Regular Employees

Regular employees have limited but they can still harm your organization. They can misuse corporate data, install unauthorized applications, send confidential emails to the wrong address, or become the victim of a social engineering attack.

Privileged Users

Privileged users are administrators, C-level executives, and others with a high level of access privileges. Privileged users hold the keys to your organization's critical infrastructure and sensitive data, which is why they can deal great insider threat damage to your organization.

Third Parties

Third parties are vendors, subcontractors, business partners, and supply chain entities that have access to your IT systems or data. Third parties may fail to follow your organization's cybersecurity rules or violate them through malicious actions. Also, hackers can breach a poorly secured third-party vendor to get inside your protected perimeter.