hardsecure
WE MAKE SECURITY

H-CYBER TRUST

(ZERO TRUST ARCHITECTURE SERVICES)

CYBER EFFECT - LEVEL 1 - REACTIVE

h·cyber TRUST

SERVICE DESCRIPTION

Zero Trust Architecture (ZTA) is an enterprise cybersecurity strategy services that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement. Hardsecure services (based on NIST 800-207) grant the creation of a ZTA, based on logical components, possible deployment scenarios, and threats. It also presents a general road map for organizations wishing to migrate to a zero-trust design approach to network infrastructure and discusses relevant organizational policies that may impact or influence a zero-trust architecture strategy.

VALUE PROPOSITION

This service enables the customer to have a ZTA end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure. The initial focus would be on restricting resources to those with a need to access and grant only the minimum privileges (e.g., read, write, delete) needed to perform the mission.

SERVICE FEATURES

The ZTA is designed and deployed with adherence to the following zero trust features:

- **All data sources and computing services are considered resources.** A network may be composed of several different classes of devices. A network may also have small footprint devices that send data to aggregators/storage, software as a service (SaaS), systems sending instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

hardsecure
WE MAKE SECURITY

H-CYBER TRUST

(ZERO TRUST ARCHITECTURE SERVICES)

CYBER EFFECT - LEVEL 1 - REACTIVE

All communication is secured regardless of network location. Network location does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a traditional network perimeter) must meet the same security requirements as access requests and communication from any other non-enterprise-owned network. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.

Access to individual enterprise resources is granted on a per-session basis. Trust in the requester is evaluated before the access is granted. This could mean only "sometime previously" for this particular transaction and may not occur directly before initiating a session or performing a transaction with a resource. However, authentication and authorization to one resource will not automatically grant access to a different resource.

Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes. An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need.

The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible. No device is inherently trusted. Here, "most secure state possible" means that the device is in the most practicable secure state and still performs the actions required for the mission. An enterprise implementing a ZTA should establish a CDM (Continuous Diagnostics and Mitigations) or similar system to monitor the state of devices and applications and should apply patches/fixes as needed.

All resource authentication and authorization are dynamic and strictly enforced before access is allowed. This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually re-evaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place. This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER TRUST

(ZERO TRUST ARCHITECTURE SERVICES)

CYBER EFFECT - LEVEL 1 - REACTIVE

The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture. An enterprise should collect data about network traffic and access requests, which is then used to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.

ADDED VALUE OF OUR SERVICE

- Reduced threat surface
- Maximized use and authority of authentication
- Increased visibility into all user activity
- The ability to dynamically provide access based on current use case
- Reduce an attacker's ability to move laterally within your organization
- Limit possibility for data exfiltration
- Protection against both internal and external threats
- Lowered reliance on point solutions designed to detect/stop specific types of threat activity
- Improved overall security posture both on-premises and in the cloud

The Service is available in different scenarios:

- Pure Zero Trust Architecture
- Hybrid ZTA and Perimeter-Based Architecture
- Migration of an operational system/network to ZTA

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER TRUST

(ZERO TRUST ARCHITECTURE SERVICES)

CYBER EFFECT - LEVEL 1 - REACTIVE

SERVICE QUOTE REQUEST

For further information, please contact us using one of the following means:

“Hardsecure – Zero Trust Architecture Services” form (available on the service page on the website)

Contact Hardsecure Account Management:
(+351) 218 278 126 (PT)
(+44) 204 538 6686 (UK)
(+1) 202 2318 9859 (USA)
geral@hardsecure.com

Website:
https://en.hardsecure.com (**"Request Proposal"** form).