# H-CYBER TRUST

(SERVIÇO DE ARQUITETURA ZERO TRUST)

CYBER EFFECT - NÍVEL 1 - REATIVO

## DESCRIÇÃO

O Serviço de Arquitetura Zero Trust (ZTA) é um serviço de estratégia de Cibersegurança empresarial baseado nos princípios da confiança e concebido para prevenir violações de dados, e limitar o movimento lateral interno de malware ou acessos não autorizados. A nossa framework (baseada na NIST 800-207) garante a criação de uma ZTA, baseada em componentes lógicos e criação de cenários de vulnerabilidades e ameaças. Apresenta também um percurso para as organizações que desejem migrar para uma abordagem baseada na conceção da confiança na infraestrutura de rede, discutindo políticas organizacionais relevantes que possam ter impacto, ou influenciar uma estratégia de arquitetura de confiança.

## PROPOSTA DE VALOR

Este serviço permite que o cliente tenha uma abordagem end-to-end. A ZTA garante a segurança de recursos e dados da organização que engloba identidades (pessoas e entidades não pessoais), credenciais, gestão de acessos, operações, endpoints, ambientes de datacenter e infraestruturas de interligação. O foco inicial é restringir os recursos com base na necessidade de acesso, garantindo o mínimo de privilégios necessários para realizar da função.

## CARACTERÍSTICAS DO SERVIÇO

O serviço ZTA é fornecido, com base nas seguintes características:

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

# H-CYBER TRUST

(SERVIÇO DE ARQUITETURA ZERO TRUST)

CYBER EFFECT - NÍVEL 1 - REATIVO

➤ **Todas as comunicações são seguras, independentemente da localização do ativo na rede.** A localização da rede não implica confiança. Os pedidos de acesso de recursos localizados na infraestrutura de rede da empresa (por exemplo, dentro de um perímetro de rede tradicional) devem satisfazer os mesmos requisitos de segurança, que os pedidos de acesso e comunicação de qualquer outra rede não pertencente à empresa. Todas as comunicações são feitas da forma mais segura, protegendo a confidencialidade e integridade, e fornecendo mecanismos de autenticação (2FA).

➤ **O acesso aos recursos individuais da organização é concedido numa base em per-session.** A confiança no requerente é avaliada antes do acesso ser concedido. Isto pode significar apenas "algum tempo antes" para esta transação específica e pode não ocorrer diretamente antes de se iniciar uma sessão, ou realizar uma transação com um recurso.

➤ **O acesso aos recursos é determinado por uma política dinâmica - incluindo o estado da identidade do cliente, a aplicação, e o ativo requerente - e pode incluir outros atributos comportamentais.** Uma organização protege os recursos definindo que recursos possui, quem são os seus membros (ou capacidade de autenticar utilizadores de uma comunidade federada), e que acesso aos recursos esses membros necessitam.

➤ **A organização assegura que todos os dispositivos próprios e associados, se encontram no estado mais seguro possível e monitoriza os ativos, para assegurar que se mantêm nesse estado.** Nenhum dispositivo é de confiança. Aqui, "estado mais seguro possível" significa que o dispositivo está no estado mais seguro praticável e continua a executar as ações necessárias para a sua missão. Uma organização que implemente uma ZTA vai receber por parte da Hardsecure, a monitorização do estado dos ativos e respetivas atualizações que terão de ser efetuadas.

➤ **Toda a autenticação e autorização de recursos são dinâmicas e rigorosamente aplicadas antes do acesso ser permitido.** Este é um ciclo constante para obtenção do acesso, identificação e avaliação de ameaças, adaptando-se e reavaliando continuamente a confiança na comunicação em curso. Uma organização que implemente uma ZTA deverá ter sistemas de gestão de identidade, credenciais de acesso e gestão dos ativos de forma atualizada. Isto inclui a utilização de autenticação multifatorial para o acesso a alguns ou todos os recursos da organização.

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

# H-CYBER TRUST

(SERVIÇO DE ARQUITETURA ZERO TRUST)

CYBER EFFECT - NÍVEL 1 - REATIVO

## VALOR ACRESCENTADO

- Redução da superfície de ameaça.
- Utilização maximizada e autoridade na autenticação.
- Maior visibilidade em toda a atividade do utilizador.
- A capacidade de fornecer acesso de forma dinâmica.
- Redução da capacidade de um hacker em se mover lateralmente dentro da sua organização.
- Possibilidade limitada na exfiltração de dados.
- Proteção contra ameaças internas e externas.
- Melhoria da postura geral de segurança tanto no local como na cloud.
- O serviço está disponível em diferentes cenários:
  - Arquitetura Pure Zero Trust.
  - ZTA Híbrido e Arquitetura Baseada no Perímetro.
  - Migração de um sistema/rede operacional para a ZTA.

## PEDIDOS DE PROPOSTA / INFORMAÇÃO

Para informações adicionais ou mais esclarecimentos, por favor entre em contato através de um dos seguintes meios:

**Formulário "Hardsecure – Serviço de Arquitetura Zero Trust"** (disponibilizado na página do serviço no website)

**Comercial da Hardsecure:**
(+351) 218 278 126
geral@hardsecure.com

# H-CYBER TRUST

(SERVIÇO DE ARQUITETURA ZERO TRUST)

CYBER EFFECT - NÍVEL 1 - REATIVO

**Website:**
www.hardsecure.com (Formulário **“Solicitar Proposta”**)

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa

www.hardsecure.com

(+351) 218 278 126
geral@hardsecure.com