

## AKAMAI 解决方案简介

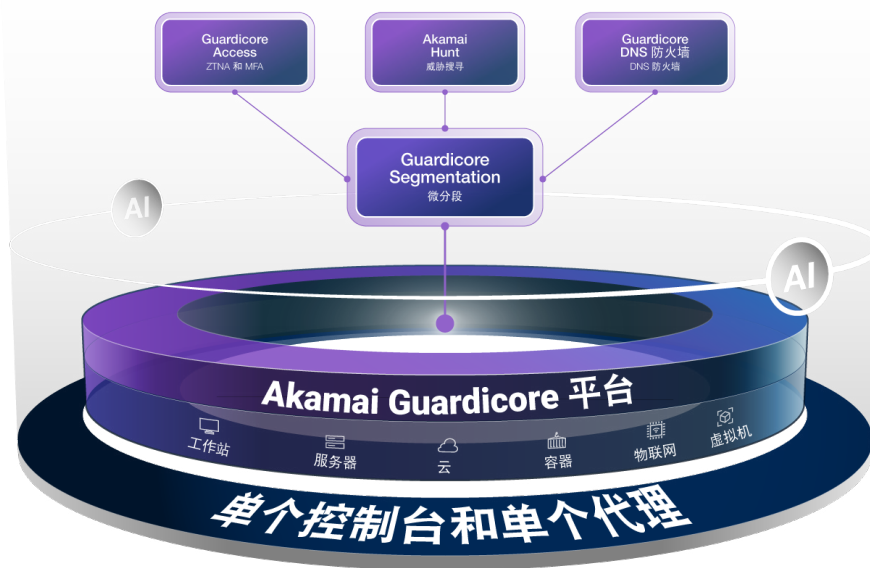
# Akamai Guardicore 平台： Zero Trust 安全

对于大多数企业来说，实施 Zero Trust 过于复杂且费用极度昂贵，尤其是在这些保护措施必须覆盖本地和云端资产以及远程办公或办公室办公的员工时更是如此。为此，我们构建了 Akamai Guardicore 平台，以便企业利用单个控制台和单个代理来高效解决 Zero Trust 各方面的问题。

随着网络威胁变得日益复杂并且监管要求日趋严格，许多企业在保持运营效率的同时还要确保网络安全，因而压力巨大。Akamai Guardicore 平台提供了全面的 Zero Trust 解决方案，可为企业提供有效实施可靠 Zero Trust 安全模式所需的工具和功能，从而化解这些挑战。

Akamai Guardicore 平台将出色的微分段、Zero Trust Network Access (ZTNA)、DNS 防火墙及威胁搜寻技术整合到一个平台中，以此实施 Zero Trust 项目。通过整合这些技术，企业可有效简化 Zero Trust 工作，进而显著减小攻击面并增强整个企业的安全态势。

## Akamai Guardicore 平台



### 微分段

Akamai Guardicore 平台中的一项关键技术是微分段。传统上，网络安全依赖于基于边界的防御措施，这些措施注重保护网络的外部边界。但是，随着网络威胁的发展演变，边界防御措施已不足以抵御复杂的攻击，这一点变得愈发明显。

## 优势



### 整合式基础架构

快速部署、轻松扩展，同时对性能的影响极小。



### 广泛、全面的监测能力

获得对网络资产和通信的全面见解。



### 统一的策略引擎

通过单个 UI 简化各种环境中的策略实施。



### 模块化灵活性

利用专门针对您的业务需求量量身定制的模块化组件。



### 全面防护

保护您的所有本地和云端资产以及在家和办公室工作的用户。



### 出色的解决方案

将出色的微分段和 ZTNA 技术相结合，以增强安全态势。



微分段另辟蹊径，将网络划分为更小、更易于管理的网段，并根据最小权限原则对每个网段应用安全策略。这种精细的安全方法可确保即使一个网段受到攻击，网络的其他部分仍然受到保护。利用 Akamai Guardicore Segmentation，每项资产（包括本地数据中心、云实例、旧版操作系统、物联网设备、Kubernetes 集群等）都能受到保护，甚至不必更改控制台。

## Zero Trust Network Access

除了微分段之外，Akamai Guardicore 平台还提供了 Zero Trust Network Access (ZTNA) 功能。ZTNA 是一种采用 Zero Trust 原则的安全模式，这意味着默认情况下不信任任何用户或设备，即使该用户或设备位于企业网络内也是如此。对资源的访问权限将改为根据严格的身份验证、设备态势及其他情景因素进行授予。此方法可以最大限度地降低发生未经授权访问的风险，并帮助企业防范数据泄露和内部威胁。

## DNS 防火墙

Akamai Guardicore 平台的另一个关键组成部分是 DNS 防火墙。DNS（域名系统）是互联网的基础组成部分，负责将人类可读的域名转换为 IP 地址。但它也是网络攻击的常见目标，因为很多的恶意软件变体依赖 DNS 与命令和控制服务器进行通信或者依赖它来泄露数据。通过部署 DNS 防火墙，企业可以拦截恶意的 DNS 查询并阻止恶意软件与恶意域进行通信，从而降低发生数据泄露和其他网络威胁的风险。

## 威胁搜寻

最后，Akamai Guardicore 平台还提供了一项自适应分段服务，让企业能够主动识别在安全威胁并采取抵御措施，避免这些威胁升级为严重事件。威胁搜寻涉及在网络内主动搜索入侵迹象，例如异常行为或入侵指标 (IoC)。通过利用威胁搜寻工具和技术，企业在面对网络攻击者时可以先发制人，保护自己宝贵的资产不会遭到破坏。

除了其核心功能之外，Akamai Guardicore 平台还具备一些关键优势，让它从市面上众多的安全解决方案中脱颖而出。该平台提供轻量级整合式基础架构，可最大限度地减少代理增加和控制台疲劳，让企业能够更高效地部署和管理自己的安全堆栈。此外，该平台还提供了广泛、全面的网络资产和通信监测能力，让安全专业人员能够获得对其网络环境的全面见解，并快速、有效地对威胁做出响应。



在 Gartner® Quick Answer: What Is Zero Trust Networking? (作者: Andrew Lerner、John Watts, 发布日期: 2023 年 9 月 13 日) 报告中, “Gartner 建议实施微分段和/或 ZTNA, 以实现 Zero Trust 网络 (ZTN) 态势。”\*

\*GARTNER 是 Gartner, Inc. 和/或其附属机构在美国和全球的注册商标和服务标志, 已获许可可在本文中。保留所有权利。

如需了解详情, 请访问 [Akamai Zero Trust 安全](#)。



扫码关注·获取最新 CDN 前沿资讯