ENTERPRISE DEFENDER

Zero Trust 边缘安全解决方案

可防御的网络边界不复存在，至少是未以任何可辨识的形式存在。如果在当今环境下使用 20 年前有效的安全和访问策略，往好的方面设想，它们可能并不合适，往坏的方面设想，甚至可能会带来危险。这不仅仅只是理论。过去五年间出现的数据泄露事件的数量和规模证明了这一点，其中大部分数据泄漏都是由网络边界之内的信任滥用所导致的。因此，企业如今有必要采用 Zero Trust 安全解决方案，这种解决方案让企业网络内不再有与生俱来的固有信任关系；转变成为基于身份、设备和用户情境，动态地实施安全和访问决策。

ENTERPRISE DEFENDER

Enterprise Defender 基于 Akamai Intelligent Edge Platform 构建，将恶意软件防护功能与适应性应用程序访问、安全性和加速功能整合成网络边缘的一种易用的安全服务。借助 Enterprise Defender，企业不需要硬件或设备，即可转型为 Zero Trust 安全架构，进而改善企业安全态势。只需订阅 Enterprise Defender，即可在改善用户体验的同时，降低风险和复杂性。

工作原理

Enterprise Defender 利用 Akamai 的 Intelligent Edge Platform，保护所有企业应用程序和用户，交付极高的安全性、降低复杂性，同时不影响性能。借助该解决方案，企业可以确保用户安全访问您控制的应用程序，同时降低因用户访问您无法控制的应用程序所带来的风险。

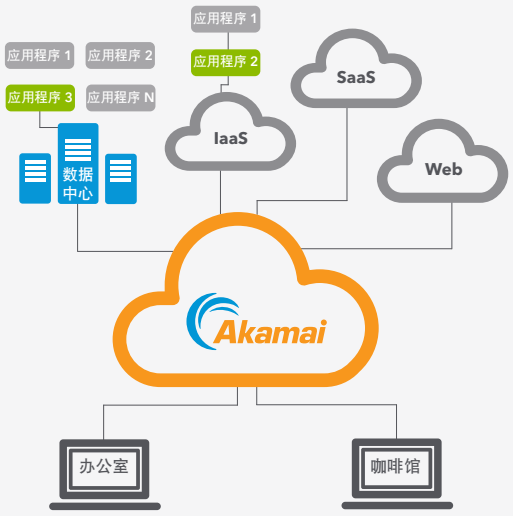
Enterprise Defender 将以下功能整合为一种简单易用的服务，且采用按月按用户数量订阅的服务形式：

恶意软件防护：Akamai 能够主动识别、拦截和抵御恶意软件、勒索软件、网络钓鱼、DNS 数据外泄和高级零日攻击等定向威胁。Akamai 提供了一款安全互联网网关 (SIG) 产品，可支持安全团队确保用户和设备在任何位置都能安全地连接到您无法控制的互联网和应用程序，而不存在传统解决方案固有的复杂性。

安全访问应用程序：Akamai 能确保仅有授权用户和设备可以访问他们需要的内部应用程序，而非访问整个企业网络。这意味着，没有人能够直接访问应用程序，因为这些应用程序不会暴露在互联网中，也不会对公众开放。Enterprise Defender 将数据路径保护、单点登录、身份、应用程序访问和管理可视化以及控制整合为单一的服务。

Web Application Firewall (WAF)：Akamai 为关键 Web 应用程序提供广泛的防护，帮助远离规模和复杂度较高的 DDoS 和 Web 应用程序攻击。Akamai 的 WAF 包含针对网站的强大安全防护，由业界出色的威胁研究团队进行更新，从而帮助企业紧跟不断演变的安全威胁的步调。

应用程序加速：Akamai 支持企业以经济高效的方式交付快速、可靠且安全的应用程序。通过将应用程序交付功能集成于高度贴近世界各地的用户、云和本地工作负载的 Akamai Intelligent Platform 之中，Akamai 能够帮助企业克服通过互联网交付应用程序的相关挑战。



- 应用程序访问、加速和边缘安全控制功能
- 将用户与企业网络隔离开来
- 针对企业应用程序的单点登录和多重身份验证
- 禁止任意位置的用户访问恶意域、网址和内容

ENTERPRISE DEFENDER

业务获益

- **阻止恶意软件的传播和横向移动**
  在基于边界的传统网络中，由于缺乏细分和网络可见性，导致恶意软件在网络中深度渗透。Enterprise Defender 整合了针对特定应用程序的更精细的访问控制功能与主动式威胁防御功能，这加大了恶意软件传播或攻击者获取其他工作负载访问权限的难度。
- **化繁为简，简化运营**
  借助 Enterprise Defender 这类基于云的安全解决方案，企业团队能够替换掉管理/维护成本高昂的虚拟或硬件设备，转而在网络边缘采用简单的安全服务。
- **降低与安全相关的资本支出和运营支出**
  提高安全性总是会导致成本增加。Enterprise Defender 可以改变这种局面；通过提高安全性并利用云技术实现简化，首席信息安全官 (CISO) 和安全团队能够将多种分散的安全控制功能整合在一起，从而降低管理成本。
- **提高可见性，加速漏洞检测**
  企业经常提到的与漏洞有关的抱怨包括“*n* 个月都没有检测出恶意攻击者”，以及“一旦突破了网络边界，恶意攻击者就能在网络中肆无忌惮地到处搞破坏”。Enterprise Defender 整合了更精细的应用程序访问日志记录功能与基于 DNS 的安全控制功能，让企业能够更清晰地了解安全状况和加速漏洞检测。
- **防止内部数据外泄**
  一旦数据落入恶意攻击者手中，企业将面临严重的后果，比如，他们可能因为没有仔细保管个人数据而被罚款，或者因为知识产权或战略计划的被窃而损失收入等等。借助 Enterprise Defender，企业能够采用基于“最低权限”的适应性访问控制功能以及基于 DNS 的可见性和安全性功能，防止内部数据的外泄。
- **支持企业的数字化转型**
  IT 和安全团队可以参与企业的数字化转型。采用基于网络边界的安全模式时，这些团队扮演的是一丝不苟的监管者角色；一旦他们为支持新的云服务、合作伙伴或客户模式而授予企业外围网络访问权限，就相当于他们打开了通往整个企业网络的一扇大门，或者建立了与整个企业网络的连接。而采用 Enterprise Defender 时情况则不同，因为该解决方案仅基于身份和安全情境授权用户访问有限的几个应用程序，而非授权用户访问整个网络。此外，不论用户是位于办公室内还是当地的咖啡馆内，Enterprise Defender 都会禁止用户访问恶意域、网址和内容，从而建立现代化的“随处办公”企业文化。