AKAMAI 检查清单

Zero Trust 平台功能

一个有效的 Zero Trust 平台将曾经独立的解决方案（包括 Zero Trust Network Access (ZTNA)、微分段、DNS 防火墙和威胁搜寻）整合到一个集成的单控制台平台中。Zero Trust 的快速有效部署意味着您可阻止勒索软件攻击、满足严苛的合规性要求、保护分布式工作团队以及您的混合云基础架构。这份检查清单可用于评估供应商能力，也可以作为一份核查列表，用来确定通过单个平台实现 Zero Trust 需要满足的要求。

类别 1：平台要求

您的 Zero Trust 平台解决方案应当灵活、可扩展，并且易于管理。

- [ ] 具备与流量需求匹配的可扩展性，提供持续保护并且不会导致性能下降
- [ ] 能够与客户目前部署的现有安全工具（例如，SIEM、SOAR、EDR、CMDB 等）进行集成
- [ ] 覆盖异构数据中心——混合和多云环境、旧版系统、最终用户设备、Kubernetes 集群、虚拟机、物联网/运营技术环境等
- [ ] 支持各种混合架构（云、虚拟、本地）的灵活部署模式
- [ ] 能够适应基于代理的部署和无代理部署（物联网/运营技术、PaaS）
- [ ] 支持 Windows、Linux 和 macOS 以及旧版操作系统
- [ ] 具备审核日志功能，以确保记录所有操作

类别 2：监测能力要求

深度监测能力对于了解环境、识别可疑连接以及快速、精确地对威胁做出响应来说至关重要。

- ☐ 通过单个平台即可实现对所有应用程序和工作负载流以及任意环境（容器、无服务器、IaaS 或 PaaS）中用户到应用程序访问的地图式可视化
- ☐ 提供历史和实时数据流，以便进行调查和取证
- ☐ 可以与第三方防火墙和硬件（例如，交换机设备）进行互操作
- ☐ 能够从各种第三方来源（例如，CMDB、EDR 和云 API）收集数据，以制定上下文标签和规则
- ☐ 标记辅助，最好利用 AI 技术来提高速度和准确度

类别 3：策略要求

东西向（微分段）和南北向 (ZTNA) 策略将根据可以在各种应用场景（例如，勒索软件保护、远程工作团队保护、零日响应及合规）中使用的属性，从一个位置进行应用。

- ☐ 由软件定义并分布在整个企业中的策略，而不需要创建阻塞点的内部物理防火墙
- ☐ 根据各种工作负载属性而不是仅根据 IP 和端口制定的规则
- ☐ 实施以应用程序为中心的精细策略，以深入端口、进程甚至服务级别为工作负载提供保护
- ☐ 提供开箱即用模板和自定义模板的策略建议引擎，最好利用能够加速策略创建的 AI 技术
- ☐ 通过或不通过代理实施的策略
- ☐ 基于全面数据流映射的策略控制
- ☐ 根据行业最佳实践进行预配置以降低全局风险的策略
- ☐ 适用于虚拟化、IaaS 和 PaaS 环境中混合云的策略
- ☐ 与工作负载关联，并且能够在工作负载移动、迁移或发生变化时遵循其要求的策略
- ☐ 适用于在办公室工作以及远程工作的用户的访问策略

类别 4：Zero Trust 组成功能要求

在集成到统一 Zero Trust 平台的各种功能中，Zero Trust Network Access 和微分段是最重要的基础支柱。利用这些技术，企业可以部署 Zero Trust 控制措施，同时不会对员工和业务连续性产生不利影响。

- ☐ 统一的访问和网络策略引擎（组合的东西向和南北向控制措施）
- ☐ 通过 FIDO2 多重身份验证 (MFA) 实施强身份验证
- ☐ 能够通过监控和过滤 DNS 流量来保护 IT 环境及用户免受各种威胁的侵扰
- ☐ 持续检测隐蔽威胁并监控安全态势
- ☐ 跨平台的工具共享信号，可确保在任何情况下都能阻止攻击者，即使他们已成功突破访问机制也是如此
- ☐ 采用能够跟踪和隔离攻击者的动态欺骗系统
- ☐ 能够查询端点或服务器以确定是否存在漏洞，从而实现对勒索软件的快速检测抵御

类别 5：集成 AI 要求

要想有效实施 Zero Trust，很多方面都可以使用 AI 技术来进行简化。这将加快并简化策略创建、合规、事件响应和漏洞评估。

- ☐ 利用自然语言与网络日志进行通信，以帮助缩短事件响应、完成合规范围界定工作等的时间
- ☐ 利用 AI 技术根据您的独特流量模式生成标签和策略建议，以简化整个策略过程
- ☐ 将自然语言转换为语法，以快速查找网络中的漏洞，而不必研究 IoC 或编写自定义查询
- ☐ 适用于高级检测方法的 AI 威胁搜寻机制，可查找传统工具未发现的异常和恶意活动

如需了解详情，请访问 Akamai Zero Trust 安全。