Akamai

白皮书

11 个根深蒂固的 DDoS 误区

近年来，分布式拒绝服务 (DDoS) 攻击的程度、规模、分布和复杂性显著增加，从一些破纪录的攻击中便可一见端倪。遗憾的是，很多企业在如何自我防御方面仍然抱有一些过时的想法，认为他们的防御措施已经足够，或者更糟糕的是认为他们不太可能成为攻击目标。而真相是：这些攻击的受害者遍布从金融服务、电子商务到游戏的所有主要行业。实际上，对医疗保健、能源和公共事业、教育以及交通等关键公共基础设施的攻击尤其令人担忧。2023 年，Akamai 保护了亚太地区的一家客户，使其成功抵御了一次每秒 900 千兆位 (Gbps) 的大规模攻击。同年晚些时候，Akamai 阻止了一次 634 Gbps、每秒 5500 万个数据包 (Mpps) 的攻击，该攻击采用复杂的攻击媒介组合，是有史以来针对美国金融服务客户的最大规模攻击之一。这是 Akamai 迄今为止抵御的一次最大规模 DDoS 攻击：1.44 Tbps、385 Mpps 的全球分布式攻击，持续了将近两个小时。这些事件清楚地表明，网络犯罪分子继续以关键经济支柱为攻击目标。

虽然这些攻击的规模可能会让一些小型企业认为他们成为 DDoS 攻击目标的风险较低，但事实是，各行各业中的关键业务服务和应用程序都很容易成为目标。由于政治和意识形态动机的黑客崛起，以及 Killnet 和 Anonymous Sudan 等网络犯罪分子团伙提供的 DDoS 服务成本相对较低，这使得几乎每个人都可能成为目标。众多企业需要担心的也不仅仅是最初的攻击。DDoS 攻击正越来越多地被用作烟幕弹来分散网络和安全资源的注意力，而攻击者会尝试同时发起勒索软件 DDoS 攻击 (RDDoS) 或三重勒索活动等其他恶意攻击。最后，令人担忧的是，攻击者越来越多地采用人工智能工具来策划高度复杂而分散的 DDoS 攻击，使得企业及公共机构一方面要确保一致的可用性和性能，一方面还要应对重大的防御挑战。

遗憾的是，随着各种威胁变得愈加复杂并且几乎每天都在演进，很多关于 DDoS 防护的误区仍然存在，其中一些误区甚至得到了安全供应商的支持。所有安全策略都必须将 DDoS 防护作为关键原则，因此了解这些误区所带来的危险对您的 DDoS 防御工作来说至关重要。

误区 1

总容量代表可用的全部抵御资源

虽然总容量很重要，但在忽略重要细节的情况下，简单的网络容量数字可能会让人产生误解。企业在评估 DDoS 防护技术解决方案时需要提出以下问题：

- 有多少网络容量专门用于消耗攻击流量?
- 有多少抵御系统资源**明确专用于**阻止攻击?
- 有多少网络和系统资源可用于向该平台上的所有客户群和每个唯一租户传送安全流量?

这些问题都至关重要，因为如果网络总容量中包含用于满足其他需求（例如内容交付）的容量，则实际 DDoS 防御容量可能只占提供商所声称容量的一小部分。

DDoS 防御容量也不仅仅局限于技术层面。在某些时候，如果技术无法有效发挥作用，是否会有专门的人力资源来进行升级、事件响应和微调抵御措施？最强大的抵御措施需要将自动化和机器智能与人类专业知识相结合，从而提供纵深防护能力。

提示

深入了解提供商的总网络容量与平台稳定性之间的差异，及其有多少容量用于抵御攻击和交付干净流量。这些容量应被视为独立分区。例如，应按用途划分和提供专门的容量，如网络路由攻击流量、阻止或抵御攻击流量以及将安全流量传送回数据中心。

误区 2

互联网服务提供商和/或云服务提供商提供的 DDoS 防护已足够

遗憾的是，很多企业仍然认为其互联网服务提供商 (ISP) 提供的防护措施能够满足所有抵御需求。而真相是：ISP 通常仅提供经过重组、现成且带宽有限的商用 DDoS 防护措施。他们自己的基础架构与您的基础架构一起共享他们的硬件，这意味着容量和 CPU 周期受到限制。如今的 DDoS 攻击规模之大会让这两种基础架构都不堪重负，而 ISP 会对您的流量进行空路由（或黑洞路由），以防止对其他生产资源造成附带损害。通过对所有流量进行黑洞路由，企业会失去来自最终用户的合法流量和服务，导致业务在实际上离线而让攻击得逞。

此外，虽然云服务提供商 (CSP) 通常允许客户在 CSP 的云环境内设置自己的控制措施并保持对其安全态势的主权，但大多数 CSP 本身通常会拒绝承担任何责任，并最终向客户收取非法 DDoS 流量的费用。考虑到现代 DDoS 攻击的规模和程度，这会给受害者带来巨额的超额费用。

提示

仔细查看 DDoS 防护条款并就这些条款与您的 ISP 或 CSP 进行协商。此外，确定您的 ISP 是否将强大的本地 DDoS 防护硬件与云端备份相结合，从而能够在本地抵御规模小但速度快的 DDoS 攻击，同时可以通过云 DDoS 防护服务来正确抵御大规模容量耗尽型攻击。

误区 3

所有抵御时间 SLA 都是一样的

有时数字可能会让人产生误解。抵御时间 (TTM) 是安全供应商经常推销的一个数字。TTM 理想上是指在不影响合法流量和用户的情况下阻止或拦截恶意 DDoS 流量的速度。事实证明，这其中有很大的解读空间。例如，某个供应商可能不会将流量激增视为 DDoS 攻击，除非它至少持续五分钟。因此，SLA 计时器可能在您已遭受攻击后才会启动。由于平均攻击持续时间不到五分钟，因此您便可以看出问题出在哪里：这意味着，宣传的 10 秒抵御时间实际上可能为 5 分钟以上。

其他一些供应商则将缓解时间定义为部署缓解措施规则所需的响应速度。它不反映停止攻击的时间，也不反映控制措施的激活质量或一致性。归根结底，您关注的是**在尽量减少对合法用户或服务影响的情况下**，保障面向互联网的资产安全并使其恢复运行所需的时间。请务必仔细阅读供应商 SLA 的详细说明。

提示

深入研究 SLA 中所列缓解措施的时间细节。具体算法应如下所示：重要的真实时间 = 检测攻击的时间 + 应用抵御控制措施的时间 + 拦截/阻止攻击的时间 + 抵御措施的质量/一致性。选择提供**真正的零秒 SLA** 的供应商，以便在不影响合法用户的情况下抵御 DDoS 攻击。

Akamai

误区 4

空路由/黑洞路由及速率限制是可接受的防御措施

空路由（或黑洞路由）是一些 DDoS 抵御提供商采用的一种常见且相当原始的防御响应。如果某项资产受到攻击并且该攻击容量使其他客户或服务面临风险，则提供商可能会尝试将该资源的流量丢入虚拟黑洞中来防止附带损害。但这真的有用吗？从攻击者角度来看，吸入黑洞意味着任务完成，即致使目标资产有效离线。其他客户可能最终也会离线或遭遇到性能下降，具体取决于提供商的基础架构。

很多安全提供商可能还会提供另一项初步的 DDoS 防御响应对策，即在共享环境中对客户流量设置速率限制。但为了让客户感觉到资产或服务仍在运行而减少 20% 到 40% 的合法流量，这对遭受攻击的客户来说并非一种成功的局面。在应对第 3、4 和 5 层的 DDoS 攻击时，速率限制作为二级或三级对策是有效的。应对第 7 层 DDoS 攻击时，将速率限制作为初步控制措施会更有效，但您应当始终首先依赖专门的抵御手段。无论 DDoS 攻击影响开放系统互联模型的哪一层，您都应该让自己的数字基础架构 100% 受到有效保护而免受 DDoS 攻击，绝不能只有不超过 60% 的部分受到保护。

提示

询问提供商平时或在受到攻击时，对流量进行黑洞路由或速率限制的频率如何。弄清楚提供商何时（在何种情况下）会对流量进行黑洞路由，以及您需要满足哪些条件才能让自己的服务得以恢复。

误区 5

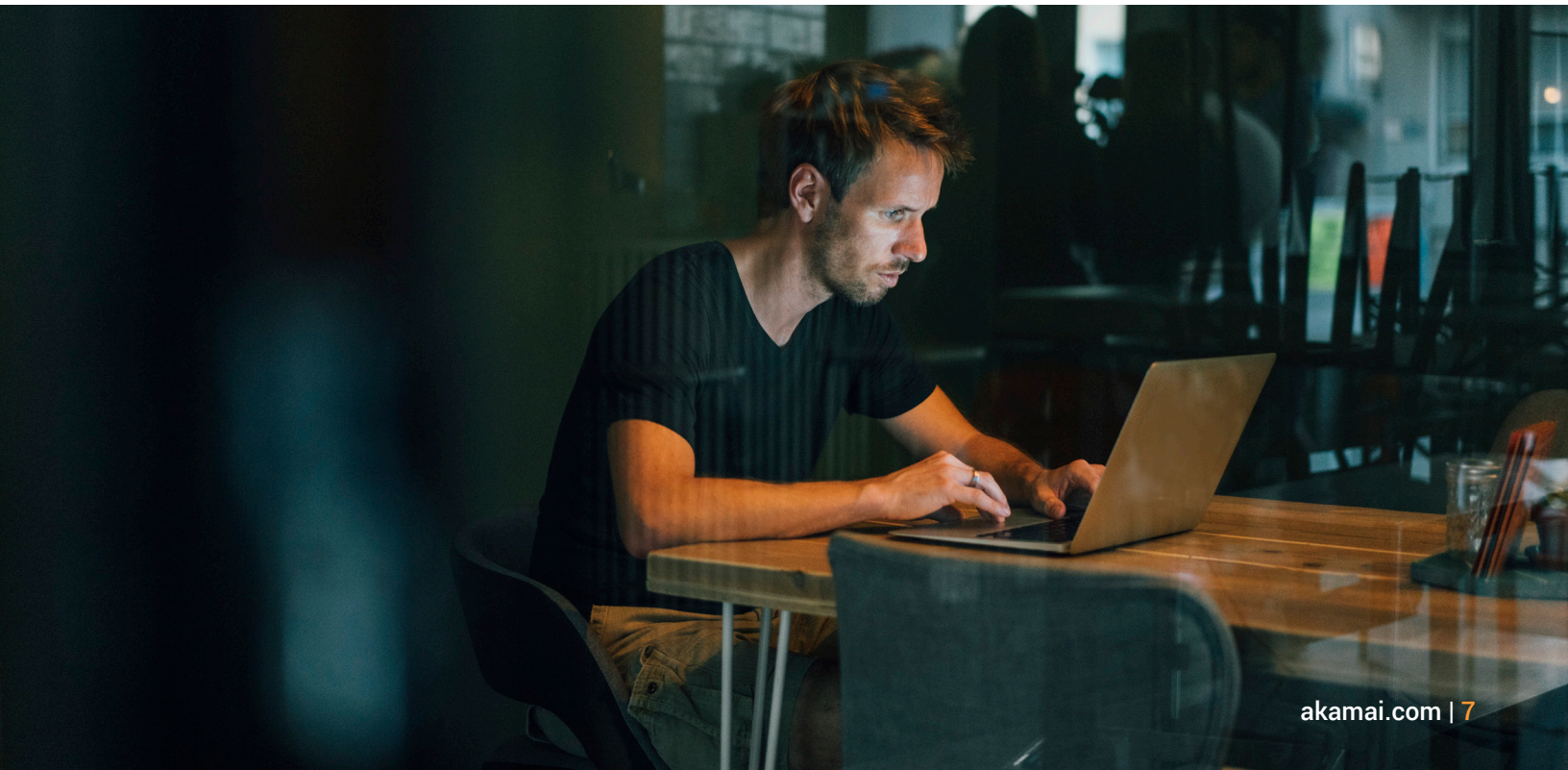
跟谁共享云平台并不重要

所有企业都需要安全保障。即便是经常受到攻击的争议型企业（如赌博和成人内容网站等灰色产业）也需要 DDoS 安全防御措施。甚至推动犯罪活动和恐怖袭击的企业也从合法云供应商处购买了网络安全方案。

您很容易认为这些网站对您来说不重要。但如果您的企业与非法企业或经常受到攻击的企业共享云平台，则遭遇附带损害的可能性会大大提高。供应商的资源可能被占用或不堪重负，致使您的企业面临风险。

提示

仔细研读云安全供应商可接受的使用政策，确保您不会跟高风险目标共享安全平台资源。另外，重温误区 1 和误区 2 之后关于容量和能力的提示。



误区 6

Web 应用程序防火墙足以提供 DDoS 防护

Web 应用程序防火墙 (WAF) 通常是更广泛的 Web 应用程序和 API 保护 (WAAP) 解决方案组的一部分，它提供针对应用层（第 7 层）攻击的有效 DDoS 防护。虽然它们可能提供一些基本的网络层（第 3 层）或传输层（第 4 层）防护，但这不足以全面保护所有 IP、端口和协议。

DDoS 攻击有多种类型和形式，能够以基础设施层（第 3 层和第 4 层）、HTTP(s) 应用层（第 7 层）以及 DNS 基础架构为目标。此外，攻击者通常会动态切换攻击，例如，先从 DNS 开始攻击，并随后扩展到其他层或协议。真正的 DDoS 防护来自于纵深防御策略，该策略采用具有特定优势和能力的强大解决方案平台，为第 3 层、第 4 层、第 7 层和 DNS 提供保护。任何一种解决方案本身都无法始终覆盖所有阵地，并且可能会导致您的企业容易受到攻击并因过度抵御合法流量或服务而面临更高风险。

提示

确保您的 DDoS 防护解决方案并未偏向于某种特定类型的 DDoS 攻击或实施设计。最佳防御措施来自于单一供应商，该供应商应当能够提供多种专用 DDoS 防护功能来维持互操作性，并由统一的快速响应安全服务团队提供支持以保护您的生产资源。当这些资产在混合网络和云托管环境中部署时，情况会变得复杂。防护服务必须与网络或部署模型无关。

误区 7

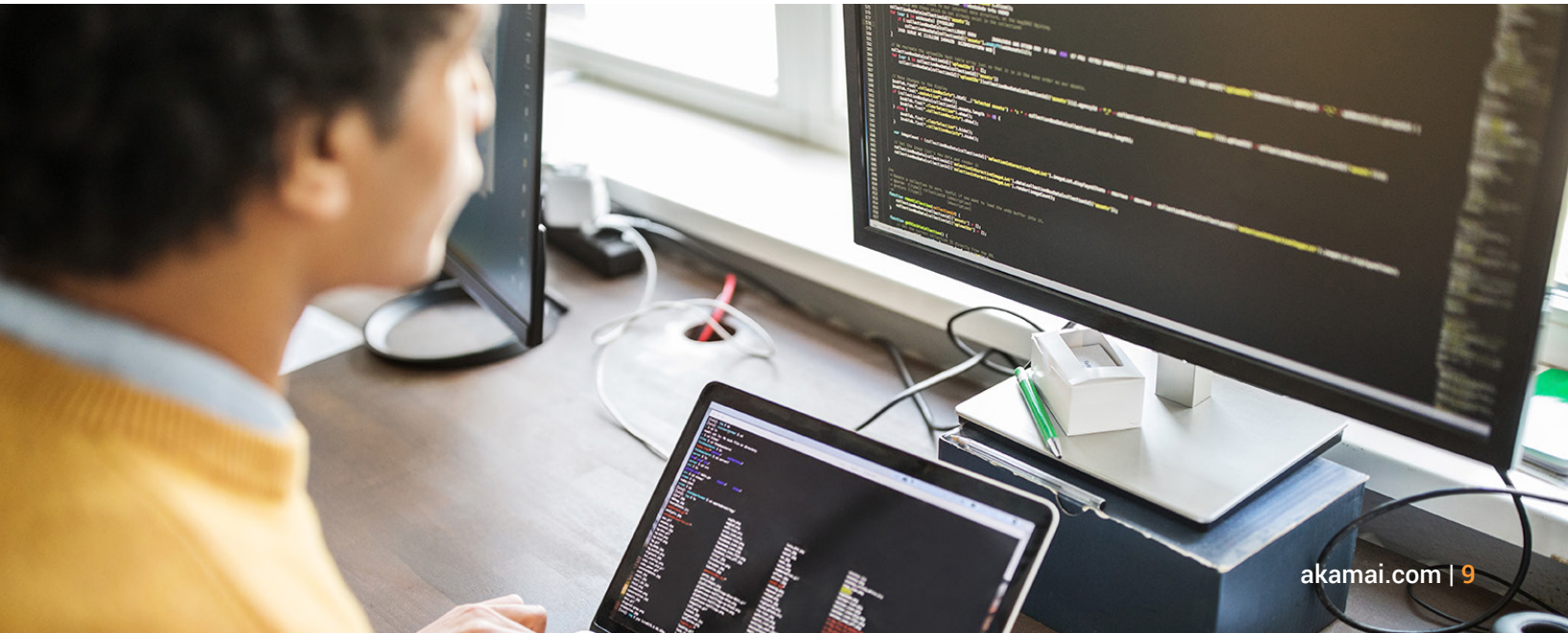
一体式安全平台 = 更好的安全体验

一些提供商在单云平台上提供各种服务。这可能会在短期内降低部署和集成安全控制措施的技术复杂性，但如果环境的其他部分遭遇中断，则共享同一后端基础架构和网络的多项服务很容易受到平台中断、附带损害和恢复能力问题的影响。通常，由于其单平台方法存在局限性，像这样的一站式供应商会牺牲功能性。

专门构建的 CDN、DNS 和 DDoS 防护平台或解决方案采用透明网络，旨在应对特定技术和安全挑战，这意味着能够提供更高质量的抵御措施并大规模提升性能，从而优化防御态势。

提示

请记住，不必为实现统一的安全体验而共享同一基础架构。多元化防御方法使用可以提供无缝用户体验以及高性能安全抵御措施的底层架构。



误区 8

IPv6 不需要 DDoS 防护

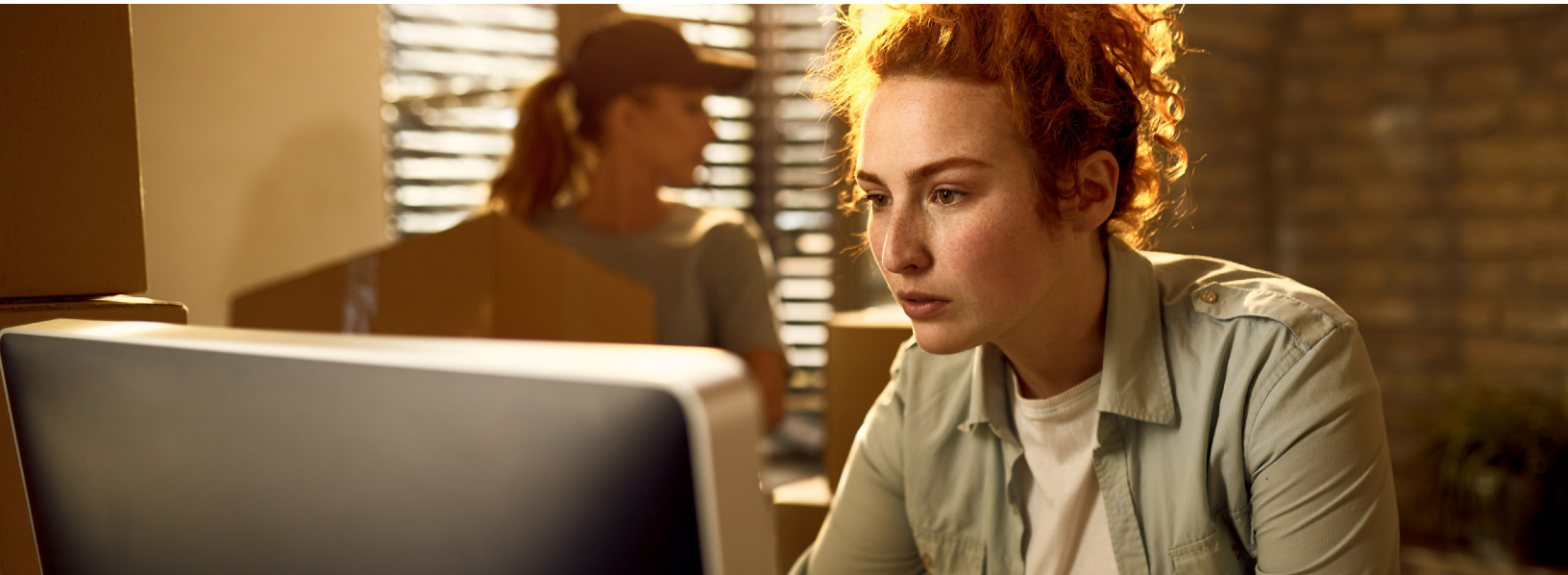
根据 Google 的数据，大约 45% 的互联网流量来自于支持 IPv6 的设备。在 DDoS 攻击方面，IPv6 相比 IPv4 有了一些改进，例如更大的地址空间和 IPsec 等内置安全功能，但它无法从根本上防范这些类型的攻击。

DDoS 攻击能够同时以 IPv4 和 IPv6 网络为攻击目标，通过利用大量流量让这两种网络不堪重负、利用漏洞或使用与 IP 版本网关的各种攻击媒介即可实现。网络犯罪分子已经在利用 IPv6 大幅扩展的 IP 空间来发动更大规模的容量耗尽型 DDoS 攻击。在某些情况下，攻击者向网络中的随机地址发送流量，不仅可以在物理网络层上引发广播风暴，还会占用和耗尽路由器或网络资源。

当前，IPv4 与 IPv6 之间分化进一步增加了复杂性，因为通常无法假设 IPv6 环境是干净的。

提示

针对 IPv6 的 DDoS 防护需要与 IPv4 类似的策略和技术，包括网络监控、流量过滤、速率限制和采用专门的 DDoS 抵御服务。



误区 9

您无需多层防御措施

大多数企业实际上并不相信该误区，但有时他们会将该误区当成事实来制定防御策略。保护您的家园时，锁上前门并不意味着您可以让后门和窗户大敞四开。真正的 DDoS 防御措施通过构建多个安全层来实现，这些安全层能够无缝协作来阻止攻击者一次性实现其目标。

卓越的 DDoS 防御措施从网络云防火墙开始，它能够减轻防火墙到网络边缘的负载。然后是混合 DDoS 防护模型，它将提供基于硬件设备的本地防护措施来应对短暂但凌厉的 DDoS 攻击，而对于大规模、复杂的容量耗尽型 DDoS 攻击，它会改为采用基于云的专用防护措施。此外，也需要利用类似的分层策略来保护您的 DNS 基础架构，该策略包括使用能够在网络边缘动态实施安全策略的代理服务，以及通过主模式或从模式下的权威 DNS 解决方案对其进行进一步分层。最后，您必须利用提供 WAF 功能的强大 WAAP 解决方案来保护自己的所有应用程序和 API。

提示

将各具特色、各有所长的最佳技术和解决方案层层叠加，构建全面的纵深防御策略，让网络犯罪分子的攻击难以得逞。

误区 10

每个安全运营中心都提供相同级别的支持

很多供应商都宣称提供安全运营中心 (SOC) 支持。但拥有一个全天候的 SOC 并不是最重要的。最重要的是，当您的资产受到攻击时，您能够享受到所期望的专业服务。在评估 DDoS 防御提供商时，要考虑的一些关键因素包括：

- 在遭到攻击之前、攻击期间和攻击之后，您能得到哪类支持和分析服务？
- SOC 如何配备人员以确保防御的连续性？
- 在联系 SOC 时，您联系的是能执行抵御操作的实际分析人员，还是仅负责问题升级的人员？
- 提供商是否有接受了抵御措施培训的安全专业人员，还是这些人员只是将流量路由到现成抵御设备的“交通警察”？
- 对方是否提供定制化的行动手册？

安全提供商的 SOC 应作为企业事件响应团队的有效扩充，从而实现其真正的价值。

提示

对您将从服务提供商 SOC 获得的预期支持服务品质进行评估。除了提供攻击检测和缓解措施之外，确定对方是否还提供集成和测试、事件故障排除、事后分析（经验教训总结）和设计支持，从而帮助您缩小攻击层面。

误区 11

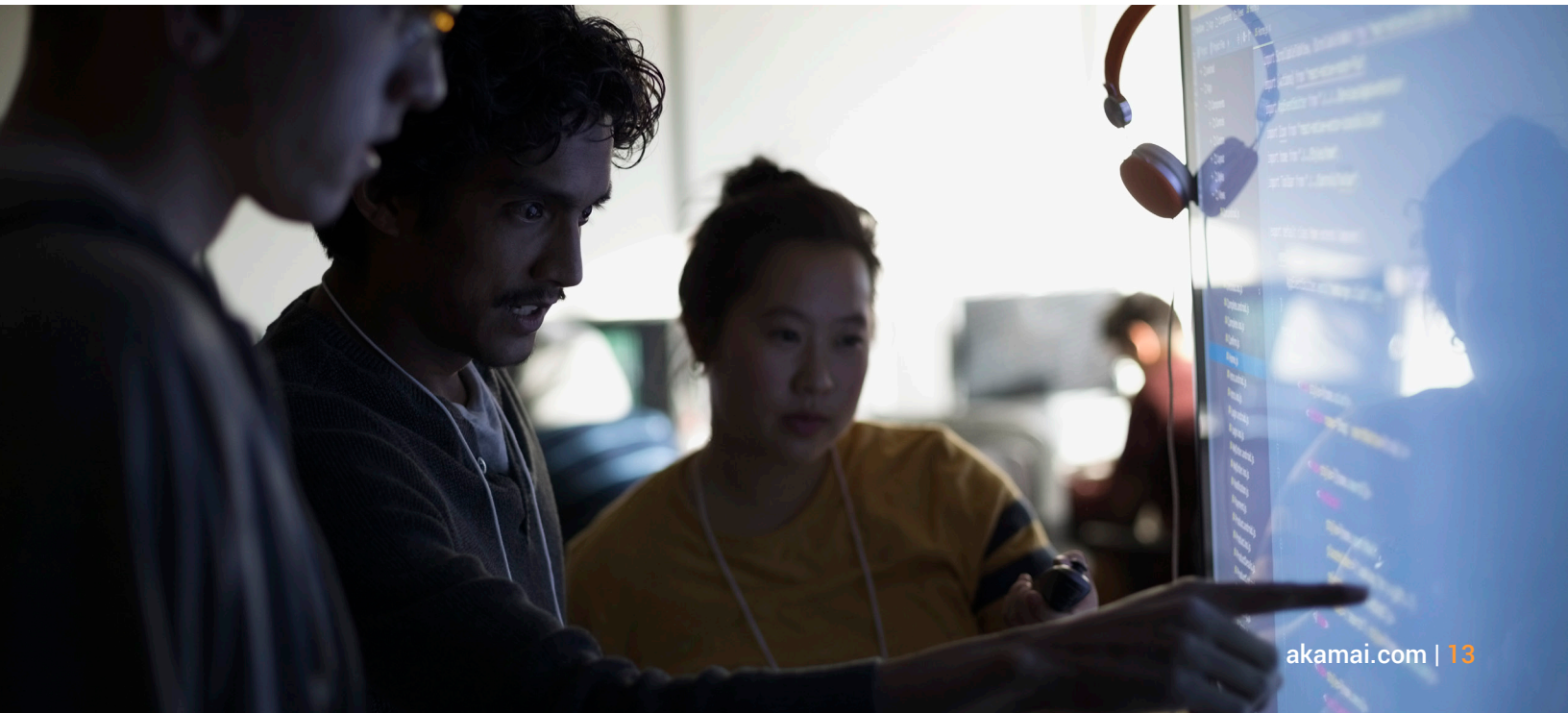
DDoS 是一种老旧的攻击方法，因此采用最廉价的保护措施就足够了

“天下没有免费的午餐”这句格言可能最适合用来描述 DDoS 防护。虽然低价看起来很有吸引力，但往往会产生一些隐性成本。

有些供应商提供较低的标价，但对其能够防御的攻击数量或规模会有所限制。一旦您遭遇过多或过大规模的攻击，对方会要求您升级到更高（且更昂贵）的服务层才能为您终止攻击，而这时您往往一心只想恢复业务，只能任由对方宰割。成熟的 DDoS 安全供应商允许客户在“不间断”和“按需”DDoS 防护配置之间进行灵活选择，并允许在这两种配置之间无缝切换，从而在提供一流防护能力的同时保持较低的运营成本。在对比供应商和价格时，请确保您了解其中的利弊及其对 DDoS 安全态势的影响。

提示

签约之前，务必弄清楚报价中包含哪些内容。



DDoS 安全防护非常复杂，在当今快速演变的环境中需要投入大量的时间和资源。昨天有效的措施可能今天或明天就不再有效。与最终用户、客户和员工保持互联是贵企业取得成功的基础。这里没有犯错的余地，也没有必要独自承担尝试实现 DDoS 安全性的高昂成本。作为全面、灵活且值得信赖的 DDoS 防护平台，Akamai 将倾力为您提供全方位支持。

详细了解 Akamai DDoS 安全解决方案。

Akamai 安全性服务简介

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2024 年 10 月。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯