CLOUDFLARE

白皮书

希望就在前方：

如何在经济不确定性中构建
更好的网络安全态势

内容

摘要

组织面临着经济不确定性，前景变得更加不可预测。这种不确定性通常表现为预算缩减，迫使首席信息官和技术领导者寻找新的前进道路。

幸运的是，如果领导者能通过积极调整预算、重新定义流程以提高效率、并在不大幅增加资源的情况下维持计划的增长，从而渡过难关，那么一旦不确定的时期过去，组织将依然处于有利的地位。

下文中，我们将定义和详细说明创造这些环境和市场条件的各种因素。根据这些见解，我们定义了领导者可以采取的五个步骤，以便找到在不损害安全态势的情况下提高安全实践效率的机会。通过调整 IT 基础设施战略以适应新的经济环境，领导者可以他们的组织未来的成功做好准备。

简介

过去几年里，在计划和执行战略时，IT 领导者需要处理一个接一个危机。他们不得不应对全球疫情大流行及其后续影响、供应链短缺、东欧冲突升级，以及经济衰退。正如斯坦福大学经济学家保罗·罗默 (Paul Romer) 所言，“浪费危机是一件可怕的事情。”（来源）。首席信息官们在支持远程办公人员方面所做的选择将产生持久的、意想不到的好处，使他们的工作场所对支持远程办公具有吸引力。同样，如今领导者们面临日益恶化的经济前景时，他们在安全、网络、远程访问、存储、开发和基础设施方面所做的选择，将有助于他们在未来更强大、更有利地实现安全、可持续的增长。

远程办公兴起伴随着勒索软件和复杂的网络威胁激增，为营收影响、规模和复杂性建立了新的基准（来源）。网络边界不复存在，加上员工流动率的历史性增长，导致了安全漏洞和战略 IT 项目的延迟。这迫使组织不仅要重新思考他们对待招聘和留存的方式，还要重新考虑他们控制系统和机器访问的方法。尽管疫情大流行导致网络犯罪激增（来源），它也让组织及其董事会认识到有效网络安全的迫切必要性。现在是时候让组织采取更具战略性的方法，应对实现安全、高效和可用的混合办公基础设施的长期目标。

企业可以做如下五件事，以便在预算范围内消除业务风险，并提升组织处理即将到来的威胁的能力。

1. 审计现有安全工具以发现重合能力

整合安全供应商可以给组织带来很多好处。尽管没有任何单一的工具会成为 CISO 喜欢拥有的“银弹”解决方案，但许多安全运营商认为自己的公司在太多工具上浪费钱，而这些工具仍然不能给他们提供最佳的防御。支持来自多个供应商的多种工具意味着您的员工将花费宝贵的时间在采购、实现、管理、故障排除和支持大量独立的系统上——而不是保护您的基础设施和数据。事实上，2022 年 6 月在年度 RSA 大会上进行的一项调查发现，“一半 (53%) 的受访企业认为他们浪费了超过 50% 的网络安全预算，但仍然无法补救威胁。43% 的受访者表示，他们在威胁检测和补救方面的最大挑战是工具过剩，而 10% 的组织缺乏有效的工具来补救网络安全威胁（来源）。即使消除这些工具中的一小部分，就可以提高安全性，同时节省宝贵的员工时间。

通过将投资从资本支出转移到运营支出，您还可以立即改善短期现金流，并避免陷入阻碍业务敏捷性的多年资本投资。简化的一种方法是减少对传统硬件的依赖。从传统解决方案转移到“即服务”(as-a-Service) 解决方案，即使预算减少的情况下，也能确保组织的最高优先级计划继续获得资金。购买“即服务”模式还意味着，组织可以受益于原生更快的软件创新周期，并消除频繁修补传统硬件造成的不可避免的痛苦。通过摈弃修补和拥抱创新，您的团队将能专注于使企业真正与众不同的活动上。面对不确定性时，战略性的简化和整合可以帮助组织实现长期成功。

2. 专注于数据，而非仅工具

领导团队应考虑将重点转移到更好的整合上，不仅包括所有安全工具中的工具，还有其中的数据，以更好地发现模式和异常情况。从历史上看，安全团队一直在不断地添加越来越多的工具集，而没有考虑到位于太多地方的太多数据集带来的长期影响。结果往往是东拼西凑的产品组合，几乎没有互操作性，数据缺乏透明度，带来人为错误的机会，导致较弱的见解和较低的准确性。更不用说团队提取多个数据集、将它们合并在一起并运行查询所花费的时间，这不仅浪费时间，还浪费资源。相反，这些资源可以集中在更具战略性的业务计划上。

虽然团队也许能够找到创造性的方法来解决互操作性挑战，例如手动合并数据集或导入/导出CSV，但重要的是要考虑到，撇开效率不考虑，安全工具的价值在于这些系统消化、创建并提供防御者的数据。如果您的数据无处不在——未分类、不安全、也没有仔细管理——它可能会歪曲从这些数据中获得的可能有影响力的见解，特别是如果在影子 IT 实例存在数据，有可能被完全忽略的情况下。通过整合工具集并仔细考虑安全堆栈的互操作性，您将可以减少人为错误并更好地保护数据。这是因为，即使您投资了当今可用的最好工具，孤立的数据集和影子数据集也会导致较差的见解。

在效率方面，重要的是考虑到在 Zero Trust 时代（“从不信任，总是验证”），更多工具意味着团队在开始工作之前还要花费额外的时间登录、验证和访问系统。员工需要接触更少系统，即可节省时间并更快行动。至关重要的是，要考虑一点：这些系统中的数据，以及他们必须访问多少个系统来完成任何给定的任务，最终促成或阻碍团队及时响应威胁，而非对威胁作出反应。

3. 考虑云计算、“即服务”模型，以最大化创新和最小化复杂性

每个企业都需要创新以保持竞争力，但任何不从事网络安全业务的公司都没有时间、预算或资源来跟上最新的关键通用漏洞、攻击趋势，以及保持整个基础设施安全所需的关键补丁。在可行的情况下采用“即服务”模式，可以让领导者从持续的创新中受益，无需围绕技术债务进行权衡或做出艰难的决定。

同样重要的是，要考虑到一些安全服务会收取超过流量限制的超额费用，一些会收取带宽费。考虑仔细查看您的公司每月或每年支付的费用，以了解实际支付的金额是否比您意识的要多。若然如此，您可以利用这个机会寻找其他不收取超额费用的解决方案，不仅可以帮助省钱，还可以让您的团队拥有一个更可预测的长期支出，以便团队更好地规划未来。

这种性质的云交付服务还为组织提供根据需要扩大和缩小规模的空间，而不必承诺昂贵的硬件，以及随之而来的生命周期管理的所有痛苦。在不确定的时期，企业必须保持敏捷，并对不断变化的市场状况做出反应。当现金流成为问题时，最小化成本或完全消除成本的能力是一种战略优势，这可能意味着勉强生存和蓬勃发展的区别——无论市场状况如何。

4. 提升员工体验

福布斯 (Forbes) 表示：“我们的调查发现，复杂、多步骤的登录流程让员工感到沮丧，浪费他们的时间，影响了工作效率，并促使他们放弃了与工作相关的重要任务……最具讽刺意味的是，近40%员工表示，由于繁琐的登录流程，他们已经拖延、委派或完全跳过了设置新的办公安全应用。这就像用金钱能买到的最坚固、最高、最安全的大门来保护您的家——并用发射激光的龙来加固——然后在晚上不上锁。”不仅防御者难以高效跟踪哪些工具拥有什么功能，太多的仪表盘和数据存放位置也会给组织带来重大的安全风险和可见性缺口。如果企业想要领先于网络安全威胁，就必须考虑到，每一次点击和击键都会占用宝贵的时间、精力，并分散对关键事件的响应。为了创造更好、更精简的员工体验，领导层必须认真研究防御人员需要使用多少工具才能有效地完成工作，以及可以消除或巩固哪些工具来减少防御人员对关键安全事件做出响应（而不仅仅是反应）所需的时间。

当涉及到非技术或非防御岗位的员工时，同样重要的是要考虑到，当远程员工希望加快他们的个人生产力时，他们可能会转向影子 IT 或变通方法。虽然 Zero Trust 控制为构建更安全的组织（尤其是在远程环境中）提供了一条有希望的前进道路，但不可否认，并非所有的 Zero Trust 方法都是生而平等的。员工获取所需信息的过程越复杂，他们就越有可能设法绕过而非遵守安全控制。领导者不仅要理解安全产品的有效性，还要考虑到易用性，因为忽视员工的体验会增加整个组织的风险。

5. 寻找不牺牲网络性能的安全服务

这不仅涉及到工具，也事关如何配置和管理这些工具。考虑让您的团队对当前配置和定制进行审计，以发现可能有助于提高性能的机会。如果不可能提高性能，那就考虑从零开始为性能而构建的解决方案——因为事后考虑的性能罕有能实现领导者希望达到的目标。就网络性能而言，重要的是要记住，无法通过编程改善糟糕的架构。这类似于建筑蓝图，一旦打下了基础，重新设计的机会就非常有限一样。网络必须从头开始设计，才能实现终极性能。通过利用一个全球边缘网络的力量，在最接近源头的位置处理数据，将在今天和未来为组织提供战略优势。据《麻省理工科技评论》称，“处理大量数据可能会导致性能问题。作为回应，许多组织正在转向边缘计算，在接近源头的地方处理数据，以实现快速和实时的分析和响应，同时维持隐私和安全需求”（来源）。通过战略性地选择本就基于未来架构打造的解决方案，组织可为其团队提供更好网络性能的战略优势，同时不牺牲至关重要的隐私和安全要素。

总的来说，在不确定的时期，您可以采取以下步骤来建立更好的网络安全态势：

1. 审计现有安全工具以发现重合能力

- 整合重复的能力
- 将投资从资本支出转移到运营支出

2. 专注于数据，而非仅工具

- 工具的互操作性可以带来更好、更准确的数据集
- 更准确的数据集和报告可以带来更好的见解，这对实现业务目标至关重要

3. 考虑云计算、“即服务”模型，以最大化创新和最小化复杂性

- 如果贵组织不从事网络安全业务，则可以从淘汰修补、维护和升级到“即服务”产品中获益良多
- 云计算和“即服务”模型提供了敏捷应对波动不定的经济环境所需的灵活性

4. 提升组织员工体验

- 在太多地方拥有太多工具会造成安全盲点，导致员工沮丧——整合和简化将有助于优化其体验
- 为员工易用性而优化将有助于员工留存，并阻止其转向影子 IT 来完成工作

5. 在当前网络安全堆栈中寻找隐藏成本和性能提升机会

- 审计现有工具以发现优化性能的机会，但请记住，您无法优化一个糟糕的架构
- 采用为全球规模而构建、最接近预期客户所在位置的工具，将使组织能够提供优质、安全的客户体验

Cloudflare 如何提供协助

Cloudflare 成立于 2010 年，也就是 2008 年经济危机后，旨在引领从本地基础设施到云计算的转型。我们怀着一个大胆的目标打造了 Cloudflare 平台：帮助构建一个更好的互联网。Cloudflare 的产品套件可以保护和加速任何连接到互联网的东西，而无需增加硬件、安装软件或更改任何代码。

由 Cloudflare 支持的互联网资产的所有流量都通过其智能全球网络路由，每个请求都使其变得更加更加聪明。我们帮助客户更智能地工作、更好地构建、更快运行并安全地发展壮大。今天，Cloudflare 保护和加速数以百万计的互联网资产。

控制

这个集成全球网络具备强大功能，提供全面的连接性、安全性和计算能力，并让您掌控策略。

灵活性

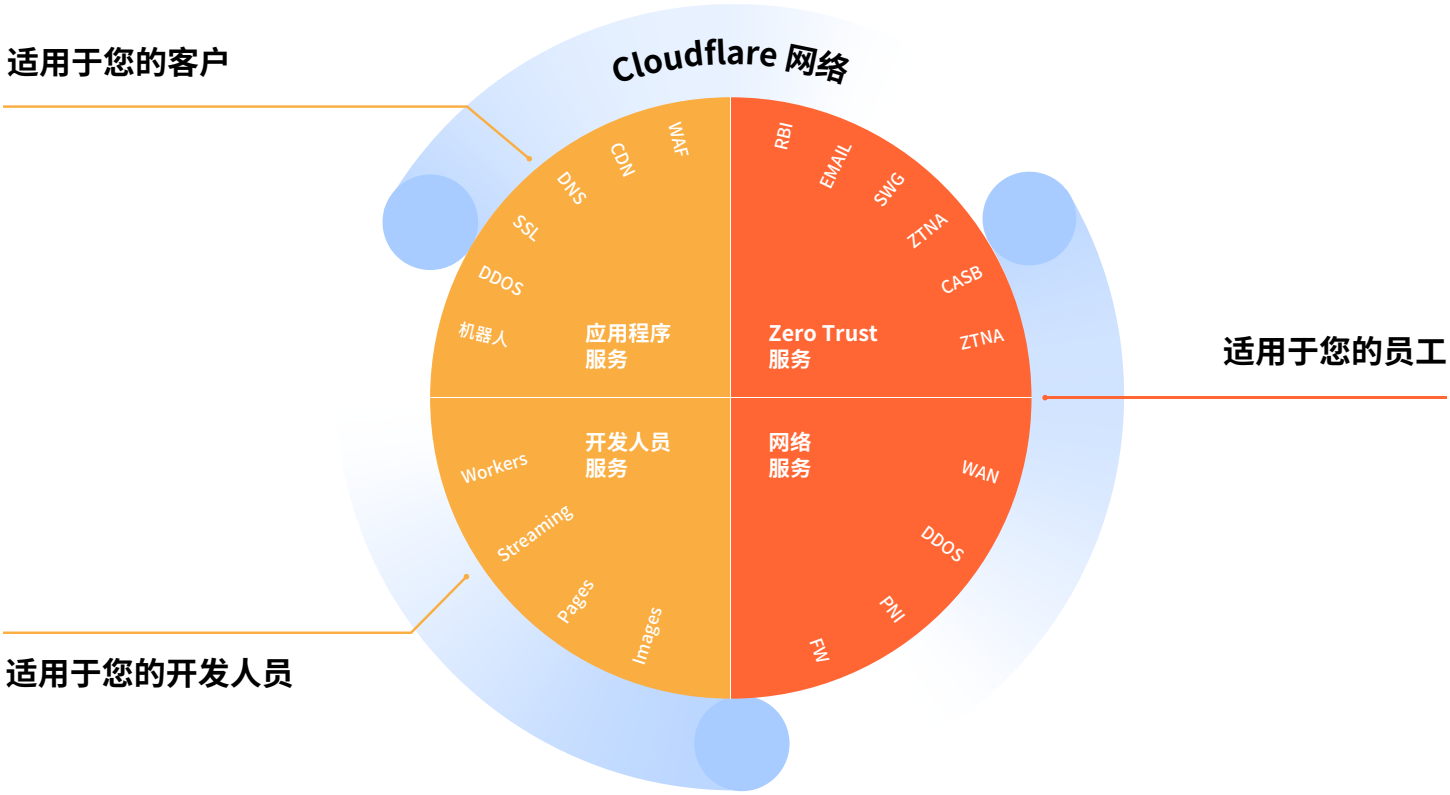
云原生服务意味着没有提前的资本支出投资。根据业务波动轻松增加或减少使用量。

可预测性

可预测的账单——没有任何意外成本，例如无限的出口费用。不必现在就为明年交付的硬件投入资本支出。

Cloudflare 全球网络使您连接到互联网的一切都安全、私密、快速和可靠。

- 保护网站、API 和互联网应用
- 保护企业网络、员工和设备
- 编写并部署在网络边缘运行的代码



关于 Cloudflare

Cloudflare 创立于 2010 年，旨在引领本地基础设施到云的转型。我们的使命是帮助构建更好的互联网，基于对此大胆计划的充分理解，我们从头开始构建了 Cloudflare 的平台。Cloudflare 的系列产品保护和加速任何在线互联网应用程序，而不需添加硬件或安装软件，也不需要改动任何代码。

Cloudflare 驱动的互联网资产所有流量都通过其智能的全球网络路由，每个请求都有助于提升该网络的智能程度。我们帮助客户更智能地工作、更好地构建、更快运行和安全地发展。今天，Cloudflare 保护和加速数以百万计的互联网资产。

若要了解更多信息，请访问 www.cloudflare.com

010 8524 1783 | enterprise@cloudflare.com | cloudflare.com/zh-cn

REV:BDES-4771.2023OCT4