

深入分析 商业网络vs.大型企业网络安全

引言

今天企业商界最常用的缩略语是"SMB", 一般来说, 绝大多数的厂商以公司的年收入或其雇员人数来区分小型企业和中型企业, 然而, 当涉及到 IT 安全时, 这些判断方法都是不恰当的。与其尝试区分哪些是商业网络, 倒不如厂商花时间和精力分析和评估这些企业的安全需求和每个企业可用的资源, 这样, 他们就能针对这些企业的特定需求提出合适每个企业的解决方案。

当提到保护公司企业的网络资产, 商业网络和大型商业网络有着同样的安全需求, 但商业网络的可利用的人员和预算十分有限, 与大型企业相比之言, 安全厂家更喜欢销售"企业级-系列"的产品给商业网络客户, 然而, 这是他们真正需要的吗? 商业网络缺乏的资金储备, 业绩等特性都是与大型商业网络无法比拟的。

同样的安全需求

因为通过互联网传播的网络威胁是不分好坏的, 它们不会区分哪些是商业网络, 哪些是大型商业网络。因此, 不论其大小, 任何与互联网相连的公司将面临同样的威胁。各种规模的企业将面临的通过入栈和出栈的 HTTP 流量威胁。同样的, 今天几乎所有的企业员工都依靠电子邮件进行日常的通信。因此, 他们将面对的大范围的和越来越多的电子邮件传播的威胁。如果企业拥有自己的邮件服务器或 Web 网站, 必须在合适的地方部署安全网关, 以保护电子邮件和 Web 服务器。

也可以这样说, 各类型企业的应用服务器, 数据库, 或其他相关的网络基础设施。不论大小, 所有企业-包括商业网络和大型商业网络的重要的资产, 都面临着同样的网络威胁, 他们唯一重要的区别是他们的业务规模大小。

不一样的资源基础

商业网络和大型商业之间的主要不同在于公司的人员和企业资产, 虽然商业网络有着与大型商业网络同样的总体安全要求, 但他们所拥有的较少的资源远不及大型商业网络 - 使他们的网络安全需求得不到解决。

一个大型的大型商业网络将拥有一个全面的 IT 安全部门来管理持续的网络安全需求, 这意味着大型企业的复杂的系统部署将有效地保护着公司网络的每个地方的资产; 同时也意味着企业通过调整公司的安全策略, 迅速地改变的现在所面临的网络威胁; 最重要的是, 这意味着他们能时刻监测着公司网络的流量, 包括分析日志文件来了解哪里有异常的流量。一个大型的企业将有足购的资金来购买他们的系统和足够的人员来管理他们。

与此相反，一个商业网络可能会或不会有一个全面的 IT 部门-几乎大部分商业网络没有聘请一个专业的安全专家。因此，很多情况是大部分商业网络只有一个员工负责 IT 需求，包括网络安全，另外一些简单的 IT 需求通过外包解决。

商业网络经常没有时间和资金来实施一个复杂的企业级安全解决方案，即使有像大型企业一样有一个合适的价格和 6 个月的部署，绝大部分的商业企业都不愿意或不能承诺有如此高水平的付出，因此，他们几乎都需要能立即见效。

不一样的安全策略

面对着这些资源的挑战，商业网络自然要作出一些艰难的安全决策，而他们将根据企业的实际情况尽最大的努力作出合适的时间和预算来部署多层次的，积极的，详细的安全系统，商业网络必须评估他们可以负担的费用，以及他们能有能力地维护该系统。

如果系统需要定期进行大量的人工操作，即使是世界上技术最好的系统对于商业网络来说也是没有用的，由于只有一个或几个 IT 人员专注于网络安全，一个复杂的系统提供多余的信息，例如 SMTP 和 HTTP 流量的异常日志文件，因为 IT 人员没有时间去审查这些记录，使这些信息并无用处。同样地，一个复杂的系统要求长达数月的部署和实施，对于商业网络需要快速部署网络安全解决方案以及运行并不是一件好的事情-这受到 IT 人员的限制。

在这些似乎难以克服的挑战，再加上其安全意识较低，许多商业网络将挑选经济、简单和自动化而不是功能强大的和效益的安全解决方案。

为商业网络提供合适的安全

绝大多数的安全厂商并没有在传统的企业市场上妥善处理针对 SMB 的 IT 安全需求的市场，相比大型企业而言，商业网络从安全厂商这里只获得很少和有用的硬件支持，因此效果并不理想。绝大多数的厂商只是在企业级产品的基础上进行简单地裁剪特性和功能，从而尝试建立适合商业网络市场的价格，例如：一个企业级的 URL 过滤产品包括有 5000 万的地址黑名单，针对商业网络版本的可能只裁剪到 500 万，一个企业级的反恶意软件的引擎包括 50 万个恶意软件特征，针对商业网络版本的可能只裁剪到 3000 个特征，-只涵盖了“Wildlist”，“Wildlist”是安全业界公开的一张流行病毒列表。或者，企业级的 Email 过滤产品可以根据内容、特征来过滤垃圾邮件和其它恶意软件，而当它面向商业网络时，则被缩水至只能通过已知的垃圾邮件的实时黑名单来进行过滤。

一些安全厂商甚至将他们的产品明显地减少功耗和功能，当一个企业级的安全系统采用最佳的软件和技术组成时，商业网络的产品却采用开源代码的安全软件，裁剪成商业网络的

版本，使产品不太可靠或用户界面不太友好。最重要的，这些裁剪的产品为商业网络做成一个重大的安全隐患，使商业网络比大型企业的网络的安全差很多。

商业网络的需要

绝大多数的商业网络的关键业务应用主要是电子邮件和 Web 的访问，当选择一个涉及 email 的安全系统时，企业必须寻找这些应用需求。

为商业用户提供全面全方位的保护

商业网络面临着与大型企业一样的威胁和挑战，企业应该寻找能全球性范围 24 小时更新新的威胁的扫描 Web 和电子邮件内容安全公司。企业经常寻找“零时差”保护，或在星期日也能够识别邮件威胁。现在，各类企业均需要“零时差”保护。

高性能解决方案

为了能达到高效率，Web 和电子邮件安全扫描速度必须够快，很多互联网网关保护解决方案需花很长一段时间来处理入栈和出栈的通信，严重地影响了网络通信的质量，使用户感觉到沮丧。

业务持续性

一个有效的互联网网关安全解决方案，不仅要防止已知的威胁，它还必须要防止实验室未检测出来的恶意软件和垃圾邮件的威胁。

直观的管理

商业网络没有更多的 IT 资源来花费以应对复杂的安装，维护安全软件包，繁琐的升级，或用户授权许可的问题，解决方案必须是用户友好界面的同步部署和维护，该解决方案还必须有直观的 Web 图形化配置界面和图形统计摘要。

结束语

当提到保护公司企业的网络资产，商业企业 SMB 和大型企业有着同样的安全需求，但他们之间却有着不同层次的区别，如人力和资金等资源，例如，“企业级-系列”是一个很好的产品，它为企业提供全面的稳健的保护。然而，这并不意味着该企业级产品适合商业网络，商业网络的安全解决方案应该是基于成长型的，专为满足商业网络需求的基础建立的，最重要的是，商业网络的产品必须提供和企业级产品同一层次的安全保护。

NETGEAR® ProSecure™ STM 内容安全网关解决方案

NETGEAR® ProSecure™ 采用特有的技术，通过爆发扩散的速度和广泛程度来检测并阻止爆发。通过这种方式，可以在垃圾邮件和恶意软件爆发产生的极短时间内检测出来，并且实时地阻止所有相关的信息。

ProSecure™ STM 平台采用了专利的串流扫描技术，能够在数据流进入网络的时候马上进行扫描。NETGEAR STM 使用单一的平台即可实现对垃圾邮件、恶意软件、安全破坏或不必要的应用程序进行扫描，通过串流扫描技术，能够实时地扫描大量的数据。这使得局域网中的用户可以接收到安全的 Email 和 Web 内容但却没有任何延时。

ProSecure™ STM 平台使用主动防御系统来避免漏洞从发现到修复之间的时间差。NETGEAR 的解决方案中采用“法医式鉴定方法”来识别进出网络数据流中的可疑的特征，并抵制这些特征直到它们能够更精确匹配。