Business Brief

提高现有网络安全工具的效能

尽管企业在网络安全工具上花费巨大，并且这些工具为优秀技术团队所开发，但也阻挡不了每天有超过500万条数据记录丢失或被盗。

究其原因，并非是现今网络安全工具设计不当或功能不全所致，更不是IT部门偷懒或对安全性问题漠不关心。恰恰相反，大多数情况是由于网络流量激增超过了安全工具的处理能力，管理员只能采用采样的方式或者关闭某些高级功能来维持应用性能。另一个常见问题是安全工具和IT人员在数据采集时面临“盲点”，导致他们无法获取其用于检测和响应外部攻击和内部事件所需的全部数据。

为了能在不购买更多安全工具或增加人员的前提下解决这些问题，Gigamon提供了专为网络安全打造的下一代Network Packet Broker，即GigaSECURE安全交付平台（Security Delivery Platform）。GigaSECURE 安全交付平台可保护安全工具不被网络流量击垮，并实现对动态数据的全面可视化，进而提升现有安全工具效能。

借助流量智能和负载均衡来实现高性能

当流量增加时，管理员经常关闭SSL解密、深度数据包检测及其它重要安全功能，防止安全设备成为瓶颈，阻塞网络或者降低应用性能。GigaSECURE安全交付平台使用流量智能为每个安全工具过滤不需要的流量，例如，把只包含邮件的流量导流至邮件安全产品，或者将包含视频流的数据包只分发至视频检测工具。此外，GigaSECURE 安全交付平台还提供动态负载均衡功能，可协调多个设备之间的处理能力。管理员可在不降低网络性能的前提下确保安全工具全效运行。

解密后可与所有工具共享

根据国际非营利性宣传数字版权和法律组织电子前线基金会(Electronic Frontier Foundation)的调查显示，半数以上的网站流量都是在HTTPS和变种SSL上进行加密传输的。但某些安全工具无法解密SSL流量，要其它工具来解密流量需要付出“昂贵的”成本。在这种情况下，管理员会选择不对SSL 流量进行检测而直接送入企业。这一局限为攻击者将恶意软件和CC通信隐藏于加密流量大开方便之门，因为他们明确知道这种操作不会被检测到。

GigaSECURE安全交付平台可按照企业需要对流量进行解密和再加密，无须考虑这些流量是经由哪个位置进入企业的。解密流量可提供给企业全部安全工具进行检测，然后重新加密提供给串接防御工具，如IPS。恶意软件和CC流量不再使用SSL加密来规避安全工具的检测。

消除网络盲点

大多数安全工具只能访问那些流经所在网段的动态数据。要关联全部数据达到识别高级攻击的目的变得异常困难。由于无法对数据中心东西向流量以及运行于虚机之上的应用服务之间的流量形成可视化，外围安全工具受到极大限制。

GigaSECURE安全交付平台可获取传统服务器、虚拟服务器集群的虚机以及网络设备如交换机、路由器之间的流量，然后将这些流量分发至企业的全部安全工具，从而形成全面可视化。此外，借助安全信息和事件管理系统（SIEM）及安全分析工具，可对网络任何位置上高级攻击的所有指标形成可视化。反恶意软件工具、防火墙、入侵检测系统和数据泄漏防御工具等产品可获取到检测恶意软件所需的所有数据，发现来自外部攻击者的横向移动和通信，并追踪流氓软件内部人员的可疑行为。

简化管理以减少错误

随着网络的发展，其分段也更加细化，大多数企业不得不购买更多安全设备。这些安全设备不仅昂贵，还使得安全基础设施更加复杂和难以管理。复杂性会引发更多错误，并难以从整个企业中捕捉数据并对其加以分析。

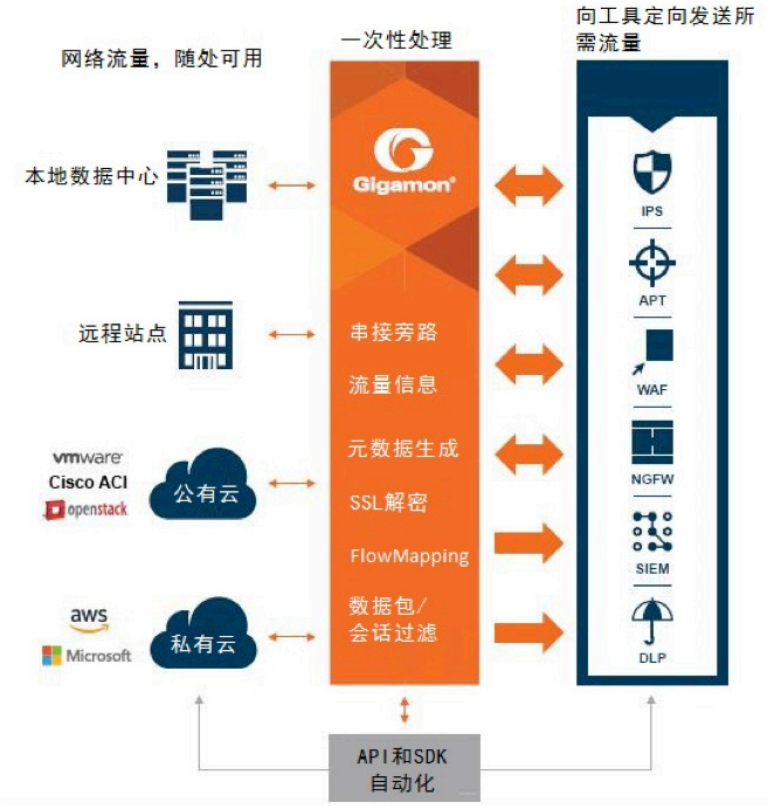
但GigaSECURE安全交付平台仅需要使用原有四分之一的安全工具就可能实现全面的保护。它通过卸载诸如处理器密集型任务，过滤每个工具的流量以及跨工具负载均衡流量等技术来实现这一目标。工具越少复杂性便越低且越易于管理，从而有利于实现更精准的配置、更可靠的更新、更好的安全数据采集及其它可提高现有安全工具效能的技术。

GigaSECURE安全交付平台

参阅本图，GigaSECURE安全交付平台：

- 简化对企业网络流量的访问
- 可将特定流量分发至相应的串接或带外安全工具
- 卸载特定工具上的诸如SSL解密之类的处理器密集型任务，并去重
- 利用流量情报优化网络流量，或者从网络流量中提取元数据并将其发送至相应安全工具
- 提供可编程接口，可与安全和基础设施栈实现集成，对基础设施变动、事件以及早期IOC做出动态响应

作为下一代Network Packet Broker，GigaSECURE安全交付平台专为安全工具而打造，可实现物理、虚拟以及云环境中安全工具的更有效运行。对于串接威胁防御工具来讲，GigaSECURE安全交付平台可强化安全态势、简化IT并降低成本。它还提供对企业周界活动的全面可视化，以便所有安全工具均可快速检测，分析和阻止网络攻击。它通过从企业中的任何位置获取网络流量并在将精确数据提供给企业内外部的特定安全工具之前应用流量智能，从而解决了局部可视和盲点问题。



如欲了解有关GigaSECURE安全交付平台帮助客户提高安全性并降低成本的秘诀，敬请浏览Gigamon公司网站：**www.gigamon.com**

3254-02 03/18

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com