AKAMAI 客户案例

Kaneka Corporation

Kaneka Corporation 借助 Secure Internet Access Enterprise 加强自身安全态势，并保护直接传输到互联网的流量

提高整个集团的安全性

Kaneka 是一家综合型化学品制造商，从事多种材料和产品的制造及销售业务，包括化学品、药品、食品、医疗设备和电子材料。

该公司在东京和大阪都设有总部，拥有 3,500 名直属员工，而集团的全体员工队伍包含超过 10,000 名员工。

该公司的物联网解决方案中心全权负责管理整个公司的信息系统和安全性。在商业解决方案事业部负责人 Tetsuro Yabuki 的领导下，该中心一直在积极寻求使用 SaaS/PaaS，并依据“云优先”策略集中部署虚拟化服务器，2011 年，在全公司范围内引入了 Microsoft 365，自那时起，此策略便已开始实施。目前，该公司有大约 90% 的 Windows 服务器部署在 Microsoft Azure 或私有云环境中。除此之外，他们还使用了混合云配置来部署关键业务系统基础架构。

物联网解决方案中心一直在努力解决具体问题，同时也在推进他们的云优先 IT 转型，而他们面对的主要问题是要提高整个 Kaneka Group 的安全性。

全球部署的简易性和速度

Yabuki 表示，由于 Kaneka 一直以来没有发生过任何严重的网络安全事件，因此他们对网络攻击不太关注，普遍缺乏安全意识。

“但是，2017 年发生的一系列令人恐惧的安全事件完全改变了这种状况。”他继续说道。

“虽然每个单独的安全事件并没有达到严重的程度，但网络风险变得十分明显，物联网解决方案中心必须尽快单独解决这些问题。我们制定了一项计划来全面改善 Kaneka 的安全态势，另外还制定了一项策略，以加强整个集团的安全管理，包括我们的海外办事处。”Yabuki 说道。

Yabuki 的全面网络安全计划包括加强安全态势，以应对出站和入站网络流量中的威胁以及可能影响端点设备的威胁。Kaneka 已选择了端点保护平台以及端点检测和响应解决方案，希望为出站流量增加额外的保护层，从而对这些解决方案进行补充。他们决定实施 Akamai 的云端安全解决方案 Secure Internet Access Enternet Enterprise，以此作为这个额外的保护层。

Kaneka Corporation
日本东京
www.kaneka.co.jp/

行业
零售与消费品

解决方案
Secure Internet Access Enterprise

重要影响

- 在两个月内，通过简单的 DNS 变更，在全球范围内提高了出站 Web 流量的安全性
- 快速为直接连接互联网的分支机构提供保护
- 主动拦截和识别被入侵的端点设备

Secure Internet Access Enterprise 服务利用 Akamai 广泛的实时威胁情报来拦截恶意流量，该服务可将恶意 DNS 查询重定向到 Akamai Intelligent Edge Platform，从而主动拦截这些查询。这可以预先防止公司设备连接到恶意网站和命令与控制 (C2) 服务器，从而大大降低了设备被网络钓鱼或恶意软件入侵的风险，避免最终导致公司信息被盗。威胁情报可自动、持续更新，无需管理员进行任何人工干预。

负责整体安全措施的商业解决方案事业部经理 Keiji Fujimoto 向我们讲述了采用 Secure Internet Access Enterprise 的原因。

“我们之所以选择 Secure Internet Access Enterprise，其中一个原因是用于确保安全的 DNS 解决方案使用起来新颖而简单，这确实是一项不可多得的优势。而且，在我们看来，这种解决方案只有全球大型 DNS 提供商 Akamai 才能提供。我们认为这是一项突破性的云安全服务，它充分利用了 Akamai 的优势。”

此外，Fujimoto 认为，Secure Internet Access Enterprise 完全符合 Kaneka 的出站流量保护要求。

“这项网络安全计划的范围还包括在整个 Kaneka Group 内实现安全措施的统一，以及加强我们的安全管理。由于可以轻松方便地引入 Secure Internet Access Enterprise，这有助于加快这些措施的部署。无论我们公司的网络结构如何，Secure Internet Access Enterprise 都能有效阻止恶意通信，这也给我们留下了深刻印象。”

在两个月内完成向海外办公地点的推广部署

Kaneka 已在使用 Secure Internet Access Enterprise 保护其公司网络的所有出站流量点，并几乎完成了向日本境内及海外集团公司部署该解决方案的过程。

Kaneka 的海外办公地点和总部的信息系统分布在四个地区：南北美洲、欧洲/非洲、马来西亚和日本/亚洲。日本率先部署了该系统以加强安全方面的管理，其他三个地区的相应信息安全团队也紧跟日本的脚本，在全球范围内部署了 Secure Internet Access Enterprise。

“跨地区合作实施 Secure Internet Access Enterprise 的过程十分轻松。虽然我说的是实施，但我们需要做的只是更改递归 DNS 查询目的地。因此，海外部署的过程十分顺利，我们能够在两个月内完成此项目。” Fujimoto 回忆道。

为直接互联网连接提供保护

对于位于日本的集团公司，Yabuki 和他的团队拜访了那些没有使用 Kaneka 数据中心的公司，并与他们进行了合作。这些公司没有使用 Kaneka 数据中心，也就是说，他们在各自的环境中运行系统，并拥有直接连接互联网的独立出站流量点。

除了为 Kaneka 自身部署 Secure Internet Access Enterprise 外，他们现在还使用 Secure Internet Access Enterprise 来为直接连接互联网的办公地点传输的出站流量提供保护。

Fujimoto 表示：“在 Kaneka，尽管我们目前只允许某些办公地点直接连接到互联网，但我们仍需要一种方法来保护这些地点的出站流量。Secure Internet Access Enterprise 使我们能够如此轻松地实现此目标，对此我很感激。”

> 利用 DNS 作为安全措施的理念不但具有突破性，也合乎逻辑。这是只有 Akamai 这样的公司才能提供的解决方案。

Keiji Fujimoto
Kaneka Corporation 物联网解决方案中心商业解决方案事业部经理

快速识别被入侵的设备

如今，整个 Kaneka Group 都采用了 Secure Internet Access Enterprise，而且 Kaneka 及其全部集团公司都能主动阻止所有设备与恶意网站和 C2 服务器的通信，这让物联网解决方案中心能快速检测和确认任何进行恶意通信的设备。Yabuki 表示，公司因此能够立即采取行动来处理所有 Kaneka Group 公司中存在风险的设备。

Yabuki 说：“只要集团中存在一台‘风险设备’，就有可能在未来发酵成重大问题。借助 Secure Internet Access Enterprise，我们能够在整个集团内识别这些类型的设备，这带来了巨大的成效。”

Fujimoto 补充道，企业中偶尔有人会启动一台很久没有使用过的设备，然后这个设备会被识别为存在风险。

Yabuki 又指出：“这些情况下，您可能会使用一台感染了恶意软件的旧设备，并且设备不在信息系统部门的控制范围内，而您对此毫不知情。当这样的安全风险在现实中出现时，使用 Secure Internet Access Enterprise 可以带来另一个好处——能够快速检测该设备，拦截来自该设备的通信，并停止该设备的运行。”

“安全措施是一个重要的业务因素。”Yabuki 继续说道。“因此，我们认为，我们必须考虑到我们的销售规模和声誉，并以与之相符的方式投资改善安全性。Kaneka 突然发生网络安全事件的原因，可能与最近的宣传活动导致的认知度大幅提高有关。公司的价值越大，网络风险自然也会增加。因此，在继续改进保护公司价值的措施时，我们还必须着重利用 Secure Internet Access Enterprise 这样的创新技术。

kaneka

该公司成立于 1949 年 9 月，它是一家从 Kanegafuchi Spinning Company, Ltd. 分离出来的公司。在成立之初，该公司名为 Kanegafuchi Kagaku Kogyo Co., Ltd.（2004 年变更为现在的名称）。该公司最初是一家化学品制造商，负责开发聚氯乙烯 Kanevinyl。如今，该公司提供了广泛的化学品、功能树脂、发泡树脂、食品、药品、医疗设备、电子材料、太阳能电池和合成纤维。近年来，该公司提出了让世界变得健康的概念，此概念也用于为保护全球环境做出贡献，比如开发可在海水中 100% 生物降解的生物降解聚合物 PHBH，以及提供补充材料（比如辅酶 Q10 的还原形态），还从事生产和销售乳制品，比如 Milk for Bread 产品：https://www.kaneka.co.jp/。

 | 支持 | 2023 年 2 月