报告的关键见解

《亚太地区及日本概况》是我们更全面的安全应用程序 SOTI 报告《数字堡垒受到围攻：现代应用程序架构面临威胁》（仅提供英文版）的姊妹篇。请阅读该报告，详细了解攻击者如何利用日益扩大的攻击面发起攻击，同时获取有关如何保障贵企业安全的建议以及对我们研究方法的说明。

概述

在过去二十年里，Web 应用程序在数量和功能上呈指数级增长，不仅简化了业务运营，改进了客户体验，还通过实时通信、数据分析和流程自动化等功能推动企业实现了增长。作为应用程序间通信基石的 API 也得到了蓬勃发展，现在有望迎来指数级增长。

应用程序几乎深入到了企业的方方面面，它们让数万亿的连接变得更容易，但也给攻击大开方便之门。在本期《亚太地区及日本概况》中，我们将以 2023 年 1 月到 2024 年 6 月为时间跨度，全面分析影响应用程序的各类威胁，包括网络攻击、分布式拒绝服务 (DDoS) 攻击以及对关键工作负载的威胁，并重点介绍它们对您的影响。

从 2023 年第一季度到 2024 年第一季度，亚太地区及日本 (APJ) 针对应用程序和 API 的网络攻击增长了 65% 并且愈演愈烈，于 2024 年 6 月达到 48 亿次攻击的峰值。在该地区中，金融服务和商业行业遭受的网络攻击最多，这与上一期报告的情况一致。

亚太地区及日本遭受的第 7 层 DDoS 攻击增长了五倍，在此期间的攻击总数达到了 5.1 万亿次，仅次于北美地区。社交媒体是受影响最大的行业，由于地缘政治事件和紧张局势，黑客行动和民族国家相关攻击者导致针对该行业的第 7 层 DDoS 攻击增加。

勒索软件和针对应用程序及它们之间内部工作负载的其他攻击成为一个日益尖锐的问题。各企业正在转向基于软件的微分段技术，以获取保护不断扩大的攻击面所需的监测能力和精细控制能力。