CASE STUDY: **MANUFACTURING**

European Manufacturer Turns to Radware Azure Cloud DDoS Security Solution

BUSINESS NEED

A well-known European manufacturing company required protection for its complex, globally-distributed network comprised of data centers, remote offices and Azure cloud-hosted applications in preparation of a high-profile sponsorship event. Each asset type had radically different requirements and faced different threat profiles. Traditional DDoS mitigation vendors did not have the flexibility or scope to offer full, cost- effective protection for all asset types.

SOLUTION

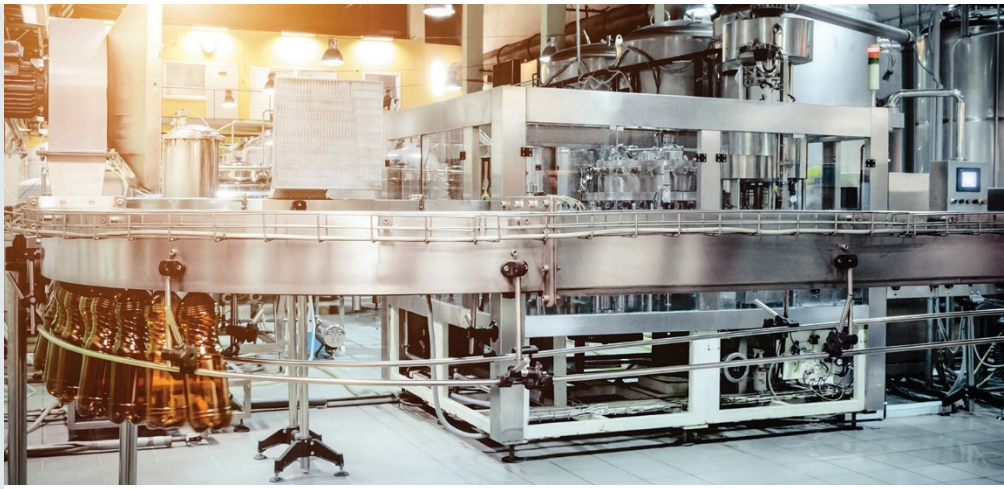
Radware implemented a combination of Azure DDoS cloud and premise-based DDoS and WAF solutions. The data centers were protected with a hybrid DDoS solution, combining a premise-based appliance with scalable Azure cloud protection. Smaller non-critical remote sites were protected with Radware's on-demand cloud DDoS service.

WHY RADWARE

Radware is the only DDoS mitigation provider using native Azure detection mechanism including Azure Monitor and Azure Insight.
As a result, Radware was the only provider who could tailor its offering specifically to the needs of the customer and Azure workloads.

BENEFITS

With the flexibility provided by Radware, the enterprise manufacturing company was able to safeguard all assets both in Azure and in its' internal data centers. Radware's security services blocked several major attacks during the high-profile event, with no impact on availability or performance of any assets.



This European manufacturing company was facing a dilemma: how best to protect its worldwide operation against DDoS and application attacks. As a well-known household brand, the customer's network and applications were globally distributed in Azure as well as in private clouds. Different infrastructure assets had different requirements under various operational scenarios, resulting in each asset requiring different protection coverage.

The problem, however, was that most vendors did not support this level of granularity in their product offerings. All vendors were constrained by their inability to offer Azure based attack detection utilizing Azure native API's, and the inability to provide seamless automation from detection to mitigation. Their limited offering set – usually only cloud-based DDoS or only hardware-based DDoS, and without application coverage in Azure, had surprising limitations in the scope of coverage they could offer. Moreover, the company's previous security vendor had suffered a major breach the previous year.

Perplexed, the customer turned to Radware, who was the only security provider able to offer the breadth and depth of protection required across the Azure Cloud and their private cloud applications.

©2018 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this press release are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.