radware

CASE STUDY: **RETAIL/E-COMMERCE**

Manutan Partners with Radware to Ensure Uninterrupted Service to Its Customers

THE CHALLENGES

As an online retailer, Manutan relies heavily on its e-commerce platforms, website and virtualized infrastructure. It needed to safeguard this infrastructure and mitigate a wide range of cyberattacks that threatened website performance and latency.

THE SOLUTION

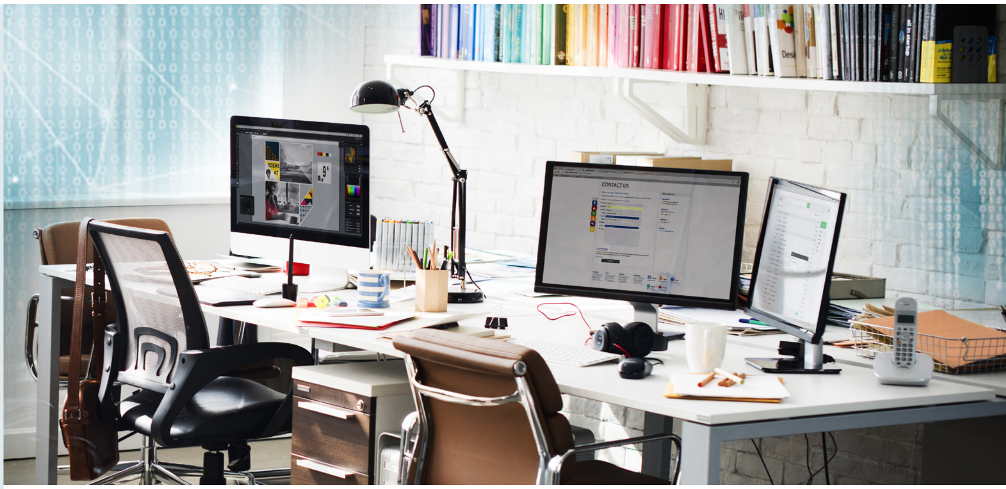
Manutan deployed Radware's Attack Mitigation Solution (AMS) for its machine-learning and automation capabilities, fully managed hybrid deployment model and coverage from a wide range of attack vectors, specifically zero-day assaults.

WHY RADWARE

Radware's AMS is a real-time, behavioral-based cybersecurity solution that protects an organization's applications and networks against known and emerging threats, including DDoS, internet pipe saturation, attacks on login pages, low and slow and encrypted assaults, CDN threats and SSL-based flood attacks.

BENEFITS

The machine-learning and automation capabilities of Radware's AMS have resulted in minimum human intervention and maximum peace of mind for Manutan's network security team and no latency for Manutan's customers.



A family-run company originally founded in 1966, Manutan is now one of Europe's largest multichannel retailers of equipment and consumables to businesses and local authorities. Offering one of the most extensive product ranges in Europe, Manutan satisfies its customers' needs and delivers support and guidance in streamlining their purchases.

THE CHALLENGES

As an online retailer, Manutan's e-commerce platform is the cornerstone of the company's business. Ensuring the complete availability of its website and web-based services, as well as its virtualized phones, email and mission-critical business applications such as ERP, is critical to the company's success. Downtime can result in lost revenue, website/shopping cart abandonments and increased customer turnover rates.

So when Manutan began facing an increasing array of high-profile DDoS attacks that threatened the availability of these services, it required a new cybersecurity solution that could prevent hackers from leveraging zero-day breaches. Minimal network latency is also critically important, so Manutan required a solution that could provide near instantaneous network scrubbing with minimal impact on website performance in the event of a volumetric attack.

Manutan went to market seeking a DDoS mitigation solution that would provide complete coverage against a full spectrum of cyberattacks, including burst, low and slow and volumetric attacks, by leveraging machine learning to automate the detection and mitigation process, thereby minimizing the need for human intervention.

THE SOLUTION

Manutan initiated a proof of concept (POC) with Radware, in addition to evaluating Imperva and Arbor Solutions. Radware was the only vendor to satisfy all of Manutan's POC requirements. Imperva was eliminated due to network latency that was incurred as a result of its "always-on" DDoS model, which always routes traffic through its cloud-based scrubbing centers. In addition, Imperva was unable to accurately distinguish legitimate network traffic from malicious traffic that was coming from a content delivery network (CDN).

Manutan selected Radware's Attack Mitigation Solution (AMS). AMS is a real-time, behavioral-based cybersecurity solution that protects an organization's applications and networks against known and emerging threats, including DDoS, volumetric attacks, attacks on login pages, low and slow attacks and SSL-based flood attacks.

Radware AMS was implemented in a fully managed, hybrid deployment model. This means Radware's DDoS prevention and attack mitigation device, DefensePro, is deployed on-premise, and in the event of a large-scale volumetric attack, network traffic can be diverted to a Radware scrubbing center. The benefit of this deployment model for Manutan is twofold: diversion of traffic to a Radware scrubbing center only when it's necessary and two-way communication between the on-site DefensePro and the scrubbing center. This communication, called DefenseMessaging, continuously updates the scrubbing center with traffic baselines, thereby allowing the scrubbing center to instantaneously begin filtering out malicious traffic, eliminating latency for Manutan customers in the event of network diversion.

"Low latency is mandatory in the e-commerce field," says Eric Thierry, CISO at Manutan. "Where most providers simply route all the traffic to their cloud services, Radware's AMS sets fully automated policies that route the traffic to the mitigation systems only when there is an attack."

In addition to its cloud-based scrubbing capabilities, Radware was selected for its machine-learning and automation capabilities that make it possible to identify zero-day attacks and mitigate them with real-time attack signature creation, eliminating this burden from Manutan's IT department. Automation also served as a prerequisite for the implementation of DevOps/agile software development at Manutan. It was mandatory for the new security solution to automatically detect new applications/versions and autogenerate new security policies and procedures, in addition to understanding any network changes as "friendly" versus "malicious."

Finally, AMS was appealing for its wide spectrum of attack protection, which allows Manutan to detect, mitigate and scrub nearly every type of web- and network-based attack the online retailer faces.

"Radware's powerful machine learning, combined with their hybrid mitigation solution, allows us to get the best of both worlds – minimum human intervention and maximum peace of mind – and it allows our customers to benefit from top performance."

— Eric Thierry, CISO at Manutan

BENEFITS

Since the implementation of Radware's AMS, Manutan has noted that a series of small cyberattacks and one volumetric spam assault have since ceased. AMS' machine-learning and automation capabilities, combined with the hybrid deployment model, have resulted in minimum human intervention and maximum peace of mind for Manutan's network security team and no latency for Manutan's customers.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.