

Maccabi-Dent Enhances Web Security with Radware's Cloud Application Protection Services & Web DDoS Protection



CUSTOMER

Maccabi-Dent

INDUSTRY

Healthcare – Dental Network

CHALLENGES FACED

- Manual security processes with frequent rule approvals.
- Limited API protection and vulnerability to DDoS attacks.
- Operational inefficiencies due to resource-intensive on-prem WAF.
- Slow response times and scalability issues.

WHY RADWARE ERT MANAGED SERVICE?

- **Advanced Web DDoS Protection:** Real-time behavioral-based detection and automated mitigation.
- **Comprehensive API Security:** mTLS validation and header-based request filtering.
- **Fully Managed Cloud Solution:** Reduces operational effort with automated protection.
- **Faster Threat Response:** Immediate mitigation, ensuring business continuity.

Overview

Maccabi-Dent, Israel's largest dental network with 61 clinics, faced growing web security challenges due to operational inefficiencies, limited API protection, and vulnerabilities to DDoS attacks. Relying on an on-premises F5 WAF, the organization struggled with manual rule approvals and slow mitigation responses, impacting operational agility.

To enhance its security posture, Maccabi-Dent migrated to Radware's Cloud Application Protection and Web DDoS Protection after a successful proof of concept (POC). The fully managed, cloud-based solution provided automated, real-time protection, reducing operational overhead and improving business continuity.

Challenges

The dental network previously relied on F5 WAF on-premises to protect their applications. However, this solution presented several operational and security challenges:

- **Manual Effort & Resource Constraints:** Each new image or web page required manual approval, consuming significant human resources.
- **Complexity in Onboarding New Team Members:** The approval process was difficult to train new employees on, adding operational inefficiencies.
- **Limited Protection of API-based apps:** The organization experienced web DDoS attacks on its API-based applications.
- **Inadequate Client Verification:** Inability of F5 WAF to implement two-layer validation for client verification.
- **Vulnerability to Network-Level DDoS Attacks:** Attackers could target the application layer while reaching the WAF, causing potential disruptions

Solution

Maccabi-Dent decided to migrate to **Radware's Cloud Application Protection** and **Web DDoS Protection** after conducting a POC. The decision was influenced by two key factors:

- **Superior DDoS Protection:** Radware's behavioral-based DDoS mitigation technology offered real-time signature creation, an advantage over competitors.
- **API Security Enhancements:** Radware provided API behavioral protection, mTLS validation, and header-based request filtering, features that F5 and Imperva lacked. With Radware's fully managed service, Maccabi-Dent eliminated the need for manual rule approvals, reducing operational effort and boosting efficiency.

Feature	Previous On-Prem WAF (F5)	Radware Cloud Application Protection & Web DDoS Protection
Deployment	On-prem, resource-intensive	✔ Fully managed cloud-based service
DDoS Protection	Limited behavioral-based detection	✔ Behavioral-based detection & real-time signatures
API Protection	Lacked behavioral API security	✔ Advanced API protection (mTLS, header validation)
Operational Complexity	High – manual approvals for changes	✔ Low – automated threat detection & mitigation
Scalability	Limited to on-prem apps	✔ Supports both on-prem and cloud applications
Mitigation Speed	Slow (manual adjustments needed)	✔ Automated & real-time mitigation

Benefits

With Radware's Cloud Application Protection and Web DDoS Protection, Maccabi-Dent has achieved a more secure, scalable, and efficient security posture for its critical web applications:

- **Stronger DDoS and API protection** with behavioral-based security mechanisms.
- **Reduced operational effort** – no need for manual approvals or rule adjustments.
- **Scalable cloud-based security** covering both on-prem and cloud applications.
- **Improved response time to threats**, ensuring business continuity.

Conclusion

Maccabi-Dent now protects 10 applications with Radware's cloud-based solution and plans to expand coverage to additional applications, including cloud-based services that were previously unprotected due to on-prem WAF limitations. By migrating to Radware's fully managed Cloud Application Protection and Web DDoS Protection, Maccabi-Dent has significantly strengthened its security posture, reduced operational overhead, and improved response times to emerging threats. The automated, real-time protection has also enhanced business continuity and simplified security management.

To learn more about how Radware's Cloud Application Protection and Web DDoS Protection can safeguard your organization, [contact us now](#).

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.

© 2025 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document 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.

