FROST & SULLIVAN

## FROST & SULLIVAN BEST PRACTICES AWARD

### 5G SECURITY - GLOBAL

# Visionary Innovation Leadership 2019

radware

FROST & SULLIVAN

2019 BEST PRACTICES AWARD

# Contents

# Background and Company Performance

## *Industry Challenges*

One common misconception of 5G is that it is *only* about faster data speeds. Enhanced speeds may be one of the first visible manifestations of these next generation networks, but the goals for 5G New Radio (NR) are much loftier. 5G will not only trigger faster speeds, but also enable ultra-reliable, low latency communications (uRLLC). Moreover, 5G networks will be able to support an extremely large number of connections over small areas (also known as Massive Machine Type Communications or 'mMTC'), which will be particularly attractive for Internet of Things (IoT) deployments. . The sophistication of the 5G architecture, however, comes with a variety of new security risks that are related to the following 5G parameters:

- 5G SBA: For 5G networks to thrive, the underlying architecture will be distributed in the cloud and will no longer be dependent on dedicated appliances. The lack of a well-defined security parameter in 5G leads to deviations to the security threat landscape. In particular, the expansion of the attack surface for 5G creates a need to protect distributed network assets and interfaces. Disaggregation of core network functions to support 5G SBA can expose security vulnerabilities if security is not integrated into 5G deployments from the early stages of network transformation.
- Software Defined Network (SDN): 5G incorporates tools that better support its agile structure. These same instruments, however, increase the number of potential vulnerabilities and threats. For example, the ability to provide network slices on top of a common underlying physical network infrastructure will be a differentiating feature of 5G networks. Network operators can apply security policies on a per-slice basis, or for a set/group of slices. As a result, there will be a significant increase in the number of protected objects that must be secured in 5G. The addition of network slicing makes Distributed Denial of Service (DDoS) protection more complex and requires a DDoS solution that is flexible, automated, and dynamically deployable. Control plane attacks, wherein components such as SDN controllers and APIs can be targeted, are among the emerging security concerns in 5G.
- Newer Traffic Patterns: With 5G, there is a need to monitor both north-south as well as east-west traffic patterns. 5G networks can generate higher traffic patterns on the edge than in the core, which necessitates the need to provide high-performance security at network edges. The end-to-end traffic in 5G can be encrypted and embedded inside IPSec tunnels (for example), which means that security solutions must be able to analyze encrypted traffic flows to identify security threats. HTTP/2 based signaling further exposes 5G networks to a wider range of attacks that originate in the web and make their way into the 5G network environment.
- Proliferation of Cloud Infrastructure and the IoT: Certain 5G network functions are likely to be hosted on the public or private clouds. These could include portions of the MEC architecture, where on-demand workloads can manifest on relatively vulnerable cloud infrastructure. Therefore, appropriate levels of cloud workload protection

capabilities are essential in 5G environments. With IoT expected to extensively permeate the 5G domain, protection from IoT-related threats such as botnets and flash network traffic generated by vulnerable or unprotected IoT devices must be prioritized.

Frost & Sullivan firmly believes that 5G security implementations must be flexible and designed to support highly agile operations in 5G. The key principles for achieving high-speed, effective security operations include:

1) Software-driven security integrated with network orchestration tools for improved visibility, control and response times;
2) Functions consolidation for improved speed of operations;
3) AI-driven automation, including automatic traffic profiling, attack discovery, incident creation and mitigation, and reporting; and
4) Integrations across the security portfolio to provide complete visibility into the carrier network.

## *Focus on the Future and Best Practices Implementation*

**Company Overview**

Radware® (NASDAQ: RDWR), is a global leader of cyber security and application delivery solutions for physical, cloud, and software defined data centers. The company's solutions portfolio secures the digital experience by providing infrastructure, application, and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down.

With 10 of the top 10 world telecom companies, 8 of to 12 world's top stock exchanges, 11 of top 20 world's banks, and 3 of top 8 North American application software companies as customers, Radware is a leading global provider of application availability and cyber-security solutions. Frost & Sullivan's research indicates that Radware is one of the very few security solution providers that have the right set of product capabilities to address the emerging 5G security requirements. The key success factors for Radware are highlighted below.

**Comprehensive Product Line**

Radware offers a full range of Application Delivery and Load balancing, Application and Network Security, Cloud Protection Services and Management and Monitoring Solutions for complete visibility, optimization, resilience, scalability, security and control in next-generation service provider networks. It is taking its differentiated approach based on advanced features such as machine learning and attack life-cycle management ability to optimize service restoration through automated workflows tailored to tenants in a multi-tenant landscape scaling in a new era of 5G innovation.

Radware's solution focus areas for 5G include:

- Carrier Edge and Far Edge – to help protect from volumetric DoS attacks on Edge and Far-Edge infrastructure
- Cloud Workload – protection from attacks on carrier workload on public or private cloud
- Critical Service Infrastructure – highly scalable, contextual, real-time protection to maintain service under attack
- API and Signaling – protection from DoS attacks on core services API's and network signaling over HTTP\2
- Connected Devices and NB IOT – protection from connected devices botnet risks and detect NB-IOT anomaly behavior

**Protecting Critical 5G Network Infrastructure Points**

The DefensePro® Attack Mitigation Device and the DefenseFlow® Cyber Command and Control Application are central to Radware's strategy for service provider protection. Radware's solutions can help protect the key interfaces processing both Control Plane and User Plane traffic in 5G. For example, DefensePro and DefenseFlow can be deployed for edge protection at the critical N1/N32 reference points against various types of attacks, including volumetric DDoS attacks and API-level attacks. They can also be used for edge protection at the N3/N6/N9 reference points for protection from DDoS attacks from Edge & Local Breakouts.

**Detection Capabilities for MEC Environments**

For defense capabilities in MEC environments, Radware's solutions can be deployed in lightweight formats that are more closely aligned with how distributed MEC is expected to work. Distributed detection capabilities in 5G can be ensured by using lighter (virtual) form factor appliances as well as the ability to embed these capabilities into other devices such as network routers. By deploying a lightweight cloud native function (micro DefensePro, for example) inside the MEC host, service providers can detect DDoS attacks such as those emanating from a rogue device attached to the network and relay that information to the DefenseFlow application to establish a BGP rule to divert and direct network traffic appropriately.

For third-party exposure of the edge computing platform, a multi-tiered defense for supporting CICD and API/Application defense can be enabled. Over time, this will also be the ideal location for infrastructure-as-a-service (IaaS) solution for real-estate owners and fixed wireless customers. The same software framework is capable of running in public cloud environments and uCPE environments.

**IoT Protection**

For IoT-centric use cases, DefensePro and DefenseFlow can help mitigate risks associated with a wide range of IoT-specific and IoT-generated attacks, including:

1) Attacks from IoT devices to edge and core services;
2) Attacks from external network toward IoT API'; and
3) Attacks on IoT devices from local breakouts.

By using telemetry data and IoT anomaly detection within the cellular and NB-IoT networks, DefensePro can identify IoT threats and facilitate security orchestration with the rest of Radware's solutions inside of the 5G networks. Service providers can also protect against IoT API attacks by using Radware's API protection capabilities (primarily built on technology acquired from the ShieldSquare acquisition).

**Carrier Workload Protection**

Radware offers a cutting edge Cloud Workload Protection Service for carrier workload protection. The agentless, cloud-native implementation delivers comprehensive protection for AWS workloads by detecting promiscuous permissions to cloud workloads, hardening security configurations before data exposure occurs, and detecting data theft using advanced algorithms. By employing AI and ML detection, the solution can help protect the overall security posture of cloud environments, as well as protect individual cloud workloads against cloud-native attack vectors.

**Emergency Response Team**

Radware's Emergency Response Team (ERT) provides round-the-clock support and mitigation services for customers facing application- and network-layer DDoS attacks. The ERT compliments an organization's ability to deal with cyber-attacks by leveraging both security expertise and real-time threat intelligence services. Radware leverages its global network, including honeypots and cloud platforms, to acquire threat intelligence and feed that back into live network environments in real time to block known attackers.

**New Product Innovation**

Radware continues to invest in new product enhancements to ensure that it can address the emerging 5G security requirements of customers. For example, Radware is closely evaluating how it can offer signaling protection for 5G networks. Radware is also expected to introduce IoT monitoring and protection solutions to help secure next-generation connected deployments at scale. Additional examples of new product innovation from Radware include:

- Feature expansion of cloud workload protection service to identify newer types of threats;
- The incorporation of behavioral-based algorithms for keyless protection against HTTPS flood attacks in the Radware DefenseSSL® SSL DDoS attack protection solution; and
- API protection capabilities (primarily built on technology acquired from the ShieldSquare acquisition).

**Strategic OEM Agreements**

Radware's continued focus on establishing, and growing, strategic relationships with various third parties, including leading global-class partners, such as Check Point, Cisco and Nokia will help the company to increase its market footprint. With 5G representing a substantial growth opportunity for core networking providers, the timing could not be better for Radware to help partners differentiate their offerings with integrated products with built-in network security. As service providers implement their MEC plans, new use cases will need to be secured, providing unique opportunities for Radware to emerge as the trusted provider of next-generation security solutions in global 5G markets.

**Competitive Comparison**

The competitive intensity is only expected to increase in 5G security markets. However, Frost & Sullivan believes Radware has significant first mover advantages in 5G, and is strategically well positioned to strengthen its current leadership status.

Frost & Sullivan's research indicates that DDoS protection will acquire greater significance in 5G security, given the scale and intensity of such attacks is expected to dramatically increase in 5G environments. With proven expertise in delivering advanced, SDN-compatible security through distributed detection, distributed mitigation, and centralized control, Radware is positioned favorably to help service providers secure their high-performance 5G networks. The ability to offer an unparalleled level of flexibility and agility for a wide variety of use cases is a clear strategic advantage for Radware. Moreover, Radware offers service providers a path to migrate their security products to a fully distributed and cloud-enabled architecture (fundamental to 5G)– another clear differentiator for the company.

## *Conclusion*

By integrating the various components to provide complete, 360-degree attack coverage, Radware offers a market leading implementation for 5G security. Innovative product architecture, highly proven implementations, and a dedication to investment in new product enhancements are core reasons for the current and future success of Radware. With its strong overall performance, Radware has earned Frost & Sullivan's 2019 Visionary Innovation Leadership Award for 5G security.

## Significance of Visionary Innovation Leadership

A Visionary Innovation Leadership position enables a market participant to deliver competitive products and solutions that transform the way individuals and businesses perform their daily activities. Such products and solutions set new, long-lasting trends in how technologies are deployed and consumed by businesses and end users. Most importantly, they deliver unique and differentiated benefits that can greatly improve business performance as well as individuals' work and personal lives. These improvements are measured by customer demand, brand strength, and competitive positioning.


## Understanding Visionary Innovation Leadership

Visionary innovation is the ability to innovate today in light of perceived changes and opportunities that will arise from Mega Trends in the future. It is the ability to scout for and detect unmet (and as yet undefined) needs and proactively address them with disruptive solutions that cater to new and unique customers, lifestyles, technologies, and markets. At the heart of visionary innovation is a deep understanding of the implications

and global ramifications of Mega Trends, leading to the correct identification and ultimate capture of niche and white space market opportunities.

### *Key Benchmarking Criteria*

For the Visionary Innovation Leadership Award, Frost & Sullivan analysts independently evaluated 2 key factors—Focus on the Future and Best Practices Implementation—according to the criteria identified below.

**Focus on the Future**

Criterion 1: Focus on Unmet Needs
Criterion 2: Visionary Scenarios through Mega Trends
Criterion 3: Growth Pipeline
Criterion 4: Blue Ocean Strategy
Criterion 5: Growth Performance

**Best Practices Implementation**

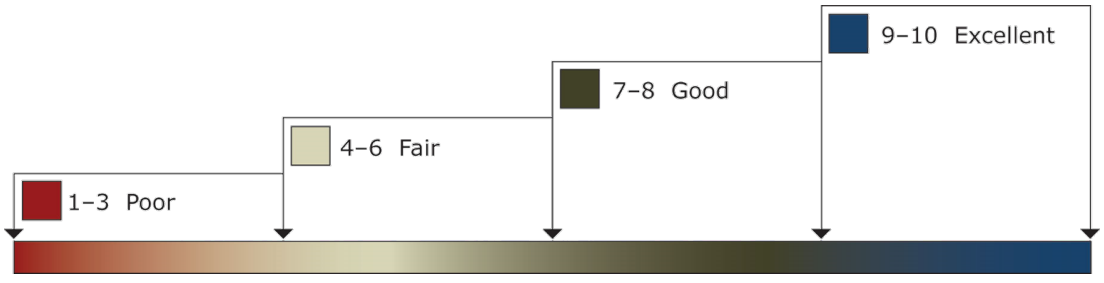
Criterion 1: Vision Alignment
Criterion 2: Process Design
Criterion 3: Operational Efficiency
Criterion 4: Technological Sophistication
Criterion 5: Company Culture

## Best Practices Award Analysis for Radware

### *Decision Support Scorecard*

To support its evaluation of best practices across multiple business performance categories, Frost & Sullivan employs a customized Decision Support Scorecard. This tool allows research and consulting teams to objectively analyze performance according to the key benchmarking criteria listed in the previous section, and to assign ratings on that basis. The tool follows a 10-point scale that allows for nuances in performance evaluation. Ratings guidelines are illustrated below.

RATINGS GUIDELINES




The Decision Support Scorecard considers Focus on the Future and Best Practices Implementation (i.e., the overarching categories for all 10 benchmarking criteria; the definitions for each criterion are provided beneath the scorecard). The research team confirms the veracity of this weighted scorecard through sensitivity analysis, which

confirms that small changes to the ratings for a specific criterion do not lead to a significant change in the overall relative rankings of the companies.

The results of this analysis are shown below. To remain unbiased and to protect the interests of all organizations reviewed, Frost & Sullivan has chosen to refer to the other key participants as Competitor 1 and Competitor 2.

| *Measurement of 1–10 (1 = poor; 10 = excellent)* | | | |
|---|---|---|---|
| **Visionary Innovation Leadership** | Focus on the Future | Best Practices Implementation | **Average Rating** |
| | | | |
| **Radware** | **9.2** | **9.2** | **9.2** |
| Competitor 1 | 8.5 | 8.5 | 8.5 |
| Competitor 2 | 8.0 | 8.0 | 8.0 |

## *Focus on the Future*

### Criterion 1: Focus on Unmet Needs

Requirement: Implementing a robust process to discover customers' unmet or underserved needs and create the products or solutions to address them effectively.

### Criterion 2: Visionary Scenarios through Mega Trends

Requirement: Incorporating long-range, macro-level scenarios into the innovation strategy, thereby enabling first-to-market growth opportunity solutions

### Criterion 3: Growth Pipeline

Requirement: Best-in-class process to identify and prioritize growth opportunities leveraging both internal and external sources.

### Criterion 4: Blue Ocean Strategy

Requirement: Strategic focus on creating a leadership position in a potentially uncontested market space, manifested by stiff barriers to entry for competitors.

### Criterion 5: Growth Performance

Requirement: Growth success linked tangibly to new growth opportunities identified though visionary innovation.

## *Best Practices Implementation*

### Criterion 1: Vision Alignment

Requirement: The executive team is aligned with the organization's mission, vision, strategy, and execution.

### Criterion 2: Process Design

Requirement: Processes support the efficient and consistent implementation of tactics designed to implement the strategy.

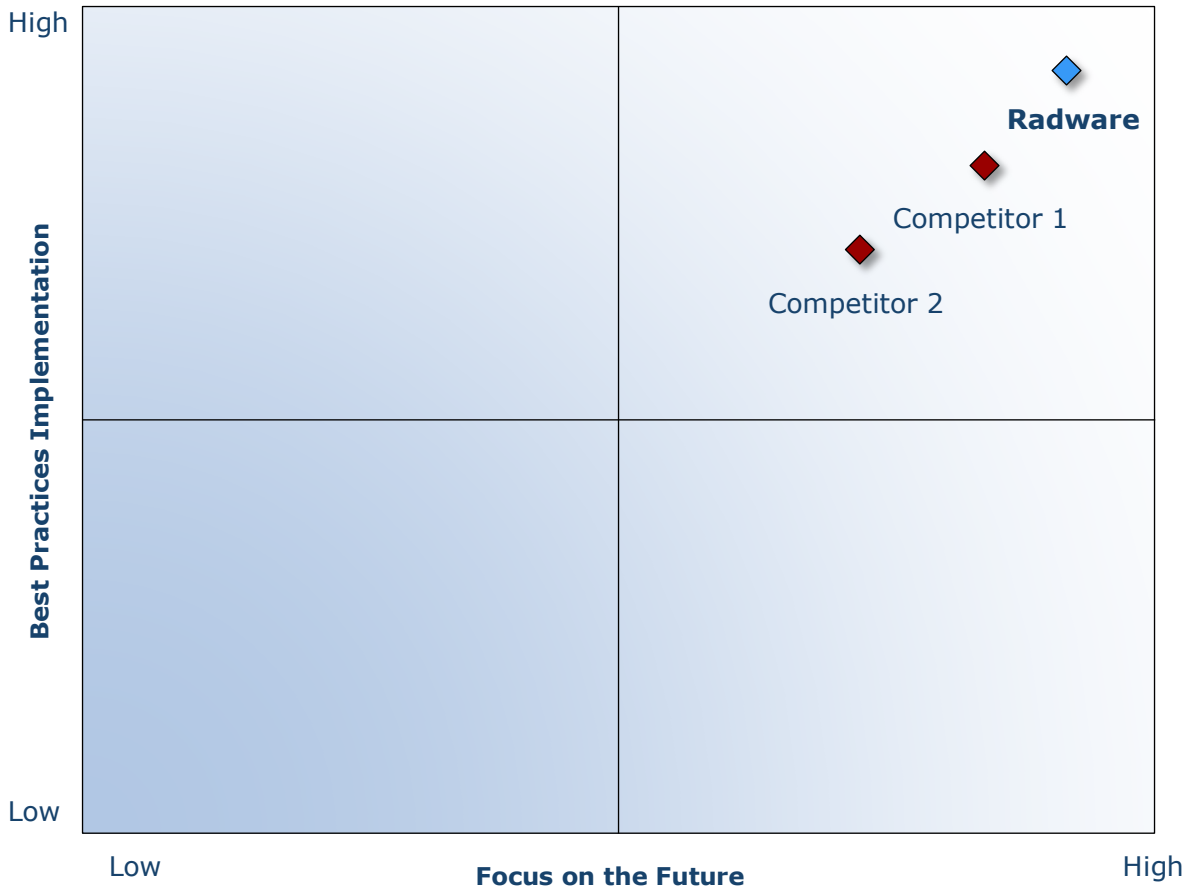
**Criterion 3: Operational Efficiency**
Requirement: Staff performs assigned tasks seamlessly, quickly, and to a high quality standard.

**Criterion 4: Technological Sophistication**
Requirements: Systems enable companywide transparency, communication, and efficiency.

**Criterion 5: Company Culture**
Requirement: The executive team sets the standard for commitment to customers, quality, and staff, which translates directly into front-line performance excellence.

## *Decision Support Matrix*

Once all companies have been evaluated according to the Decision Support Scorecard, analysts then position the candidates on the matrix shown below, enabling them to visualize which companies are truly breakthrough and which ones are not yet operating at best-in-class levels.



# Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan analysts follow a 10-step process to evaluate award candidates and assess their fit with select best practices criteria. The reputation and integrity of the awards are based on close adherence to this process.

| | STEP | OBJECTIVE | KEY ACTIVITIES | OUTPUT |
|---|---|---|---|---|
| 1 | **Monitor, target, and screen** | Identify award recipient candidates from around the world | • Conduct in-depth industry research<br>• Identify emerging industries<br>• Scan multiple regions | Pipeline of candidates that potentially meet all best practices criteria |
| 2 | **Perform 360-degree research** | Perform comprehensive, 360-degree research on all candidates in the pipeline | • Interview thought leaders and industry practitioners<br>• Assess candidates' fit with best practices criteria<br>• Rank all candidates | Matrix positioning of all candidates' performance relative to one another |
| 3 | **Invite thought leadership in best practices** | Perform in-depth examination of all candidates | • Confirm best practices criteria<br>• Examine eligibility of all candidates<br>• Identify any information gaps | Detailed profiles of all ranked candidates |
| 4 | **Initiate research director review** | Conduct an unbiased evaluation of all candidate profiles | • Brainstorm ranking options<br>• Invite multiple perspectives on candidates' performance<br>• Update candidate profiles | Final prioritization of all eligible candidates and companion best practices positioning paper |
| 5 | **Assemble panel of industry experts** | Present findings to an expert panel of industry thought leaders | • Share findings<br>• Strengthen cases for candidate eligibility<br>• Prioritize candidates | Refined list of prioritized award candidates |
| 6 | **Conduct global industry review** | Build consensus on award candidates' eligibility | • Hold global team meeting to review all candidates<br>• Pressure-test fit with criteria<br>• Confirm inclusion of all eligible candidates | Final list of eligible award candidates, representing success stories worldwide |
| 7 | **Perform quality check** | Develop official award consideration materials | • Perform final performance benchmarking activities<br>• Write nominations<br>• Perform quality review | High-quality, accurate, and creative presentation of nominees' successes |
| 8 | **Reconnect with panel of industry experts** | Finalize the selection of the best practices award recipient | • Review analysis with panel<br>• Build consensus<br>• Select recipient | Decision on which company performs best against all best practices criteria |
| 9 | **Communicate recognition** | Inform award recipient of recognition | • Present award to the CEO<br>• Inspire the organization for continued success<br>• Celebrate the recipient's performance | Announcement of award and plan for how recipient can use the award to enhance the brand |
| 10 | **Take strategic action** | Upon licensing, company is able to share award news with stakeholders and customers | • Coordinate media outreach<br>• Design a marketing plan<br>• Assess award's role in strategic planning | Widespread awareness of recipient's award status among investors, media personnel, and employees |

# The Intersection between 360-Degree Research and Best Practices Awards

## *Research Methodology*

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of the research process. It offers a 360-degree view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, resulting in errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry players and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS


## About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, helps clients accelerate growth and achieve best-in-class positions in growth, innovation, and leadership. The company's Growth Partnership Service provides the CEO and the CEO's growth team with disciplined research and best practices models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages nearly 60 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on 6 continents. To join Frost & Sullivan's Growth Partnership, visit http://www.frost.com.