Vulnerability Management (VM)–Global Market Analysis
Adding Actionable Intelligence to Network Scan Technology

Key Findings

- Frost & Sullivan estimates vulnerability management (VM) vendors sold $768.3 million of VM appliances and related services in the base year of the study, 2016, representing an improvement of 13.4% over 2015.
- For 2017, the rate of growth is expected to slightly recede. Anticipated revenues in VM are forecasted to be $849.4 million or a 10.6% improvement.
- In the years 2016–2021, the SaaS form-factor will have the largest product group in terms of revenue. In 2021, SaaS VM is projected to have revenues of $537.5 million.
- Frost & Sullivan expects SaaS to be the fastest rising product group in terms of CAGR with 22.0%, while the CAGR for on-premises physical appliances (both at a company's facilities and in data centers) are expected to fall by 8.4%.
- North America is the region that accounts for most VM sales accounting for 76.8% of all global VM revenues in 2016. In 2021, Frost & Sullivan expects that share to grow to 77.8% of all revenues.
- In 2016, Frost & Sullivan estimates there are VM 74,677 commercial installments. By 2021, Frost & Sullivan estimates there will be 106,015 commercial deployments.
- In 2016, the average selling price (ASP) for VM products to a company is $10,288. In 2021, the ASP will be $11,482.
    - Frost & Sullivan expects the growth in enterprise networks accounts, on a per business basis, to drive up ASP although increased use from cloud services would tend to tamp prices back down.
- Both agentless scanning (the traditional approach) and scanning with agents are needed to provide a holistic approach to vulnerability scanning.

Source: Frost & Sullivan

Executive Summary—Market Engineering Measurements

Total VM Market: Global, 2016

Market Overview

Market Stage	Market Revenue	Market Units/Volume	Average Price Per Unit	Market Size for Last Year of Study Period
Growth	$768 ↑ (In Millions) - Base Year 2016	74,677 ↑ Units - 2016	$10,288 ↓ Base Year 2016	$1,217 ↑ (In Millions) - 2021

Base Year Market Growth Rate	Compound Annual Growth Rate	Customer Price Sensitivity	Degree of Technical Change	Market Concentration
13.4% ↑ Base Year 2016	9.6% ↓ (CAGR 2016–2021)	8 ↑ (scale 1 [low] to 10 [high])	6 ● (scale 1 [low] to 10 [high])	52.6% ↑ (Revenues Top 3 companies)

Decreasing ↓ Stable ● Increasing ↑

Note: All figures are rounded. The base year is 2016. Source: Frost & Sullivan

Market Engineering Measurements (continued)

- A vulnerability assessment (VA) runs a script of known vulnerabilities against an endpoint.
- Vulnerability management (VM) is the formal reporting of what is found after the scan. The VM vendor can shape the report to prioritize vulnerabilities, or to meet internal or external compliance standards.
- If VM vendors only offered this solution, it would still be a fundamental network security technology because the best incident detection strategy is to harden a security surface before a breach occurs.
- An additional value of a VA scan is it can also create an accurate inventory of the OS, protocols, applications/software, ports (network mapping), and services on the machine being tested.
- The collection of the information from a VA scan has real importance:
  - **Detection of vulnerable endpoints.** In a weird way, a criticism of VA scanning is that it is a little too good. Finding vulnerabilities on endpoints is like hunting fish in a barrel (i.e., guaranteed to catch a fish). However, having the technology to bubble up the most dangerous threats is a cross between art and science, and the real difference between VM vendors.
  - **Proof of compliance.** Governmental agencies require National Institute of Standards and Technology (NIST) 800.53 compliance and Federal Risk and Authorization Management Program (FedRAMP) certification before they will do business with a private enterprise. VM reporting is a way to prove compliance.
  - **Enables triage when an event is investigated.** Even in the best networking environments, security incidents and breaches occur. A threat hunter needs to establish what is going on (triage). Contextual awareness is akin to the who/what/where and when in journalism; what endpoints are connected to which servers, and what applications and OS are on suspicious endpoints are necessary to aggregate in network security investigations and VA scans can provide this information.

Source: Frost & Sullivan

Market Engineering Measurements (continued)

- **Generates a golden state.** A golden state is the historical record of the last known good state of an endpoint.

- In the last several years, VM vendors have begun to realize the broader power of their technology.
- There are several examples of this, but one relevant example is the application of behavioral analytics.
- Compared to the "golden state," if there is a statistically significant change in the state of the endpoint between scans, that event can set off an alarm for further investigation.
- The market leaders in VM either have or are developing complementary technologies that leverage vulnerability management such as continuous monitoring and incident detection and response (IDR).
- In the last two years, the investment community has taken notice (see Competitive Factors and Assessment) later in the report.
- This creates a conundrum in the report; it is fair to say that the largest companies in VM, Qualys, Rapid7, Tenable Network Security, Tripwire, BeyondTrust, Beyond Security, and Digital Defense offer more than just VM.
- In the report, the way that these companies are leveraging their VM technologies is compared and contrasted, and covered more extensively in the Vendor Profiles.
- The anticipated mix of products/services offered by VM vendors, and revenue opportunity for the same companies is discussed in Market Overview – Evolution of Vulnerability Management.
- However, *all of the forecasts in the report are dedicated to VM products and services only*.

Source: Frost & Sullivan

Executive Summary—CEO's Perspective

1	VM vendors are using VA scans for more than listing vulnerability scores.
2	VM vendors should expect revenue growth of 9.6% CAGR from 2016–2021.
3	Customers value tools that do more than tell them "there is a problem"—the capacity to triage events is becoming a requisite.
4	VA scanning needs to match the dynamics of heterogeneous networks.
5	While VM vendors compete with other endpoint technologies for security dollars, only proper vulnerability management hardens the security surface.

Source: Frost & Sullivan

External Challenges: Drivers and Restraints—Total Market

Drivers and Restraints

VM Market: Key Market Drivers and Restraints, Global, 2016–2021

		1–2 years	3–4 years	5 years
Market Drivers	No other technology does what vulnerability management does to ensure secure configurations	H	H	H
	Vulnerability assessment scanning has visibility into each discrete endpoint which is the basis of a strong security posture	M	H	H
	Bidirectional integration with other cyber security technologies improves both VM and the integrated technologies	M	M	M
	VM is one of the technologies used to prove compliance	M	M	M
	VM scales to match the architectural needs of heterogeneous networks	M	M	M
Market Restraints	VM scanning/reporting is a static technology, and cyber defenses require a combination of static and dynamic tools	H	H	H
	Vulnerability management alone is not a comprehensive indicator of a network's threat environment	M	H	H
	Vulnerability assessment (scanning) is becoming commoditized	M	M	M
	Other cyber security defenses are better at determining if a breach has occurred	L	M	M

Impact: H High M Medium L Low

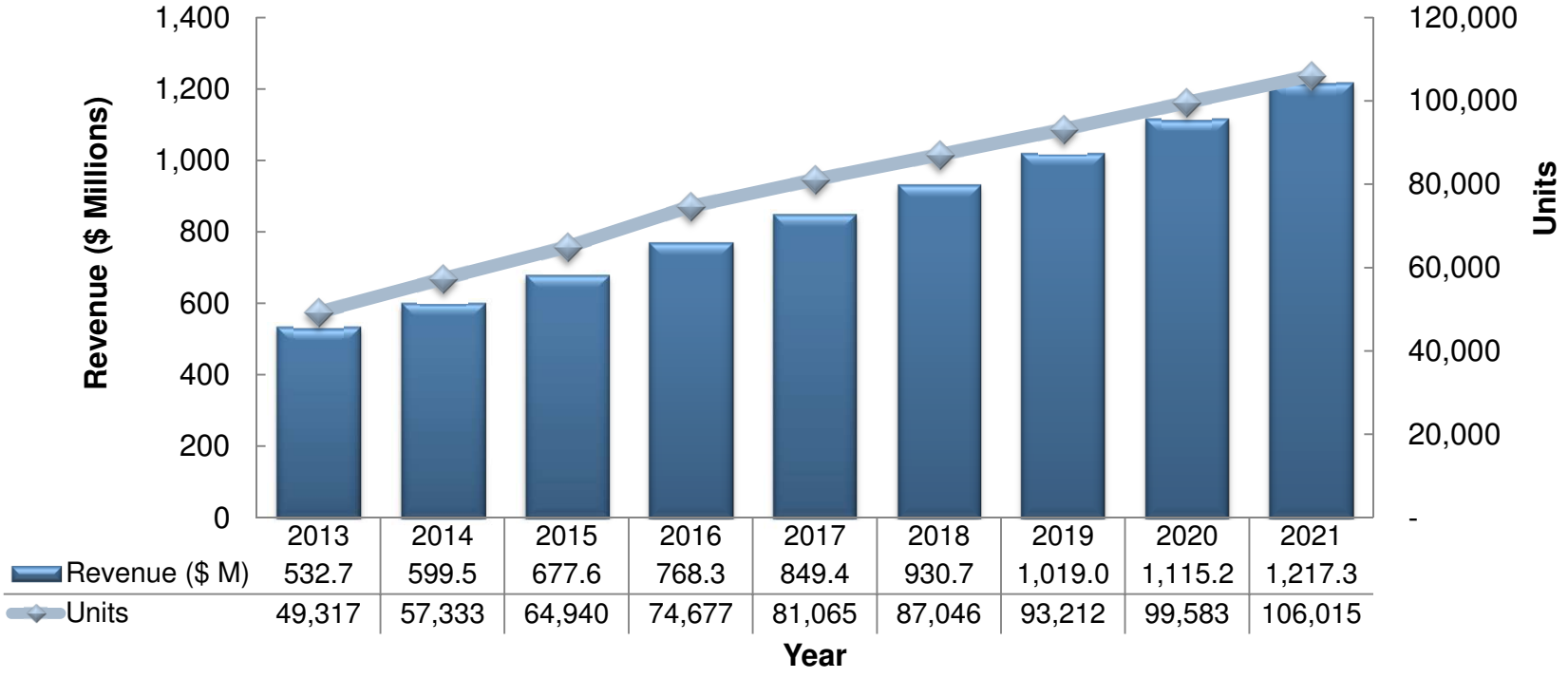
Note: Drivers & Restraints are ranked in order of impact. Source: Frost & Sullivan

Forecasts and Trends—Total Market

Total VM Revenue Forecast and Unit Shipments

Cloud-based scanning solutions have helped create new opportunities for unit shipments in 2014–2016.

Total VM Market: Revenue Forecast and Unit Shipments, Global, 2013–2021



	2013	2014	2015	2016	2017	2018	2019	2020	2021
Revenue ($ M)	532.7	599.5	677.6	768.3	849.4	930.7	1,019.0	1,115.2	1,217.3
Units	49,317	57,333	64,940	74,677	81,065	87,046	93,212	99,583	106,015

Note: All figures are rounded. The base year is 2016. Source: Frost & Sullivan

Competitive Differentiation

Points of Competitive Differentiation

Best Scan Engine—Digital Defense, Inc. Naturally, any vulnerability management vendor is going to claim its methodologies reduce the possibility of false positives. However, in Nessus remote security scanning, the emphasis is placed on VA scanning of the endpoint.

- Nessus scanning looks at either a range of IP addresses (most common), domain name system (DNS), Network Basic Input/Output System (NetBIOS), or media access control (MAC) addresses.
- The traditional scans (look-up schedules if you will) are a logical way to assess endpoint environments, are manageable, and align with CVE threat reporting and how VM vendors accumulate vulnerability data. Essentially, conventional scanning depends upon the reliability of the network mapping between host devices and endpoints.
- The problem is that an enterprise network is a highly dynamic environment. There are any number of reasons that host devices can be reconfigured or lost between VA scan events.
- Digital Defense, Inc. (DDI) takes an entirely different focus to VA scanning. DDI focuses the scan on active (live) hosts and utilizes its ability to dynamically track changes to these hosts over time, even as its characteristics change.
- The enterprise network undergoes significant changes over time including OS updates, internal server array configurations, and regroupings of user asset groups. In the upcoming Vendor Profile: Digital Defense, Inc., other scenarios about how the mapping between endpoints and servers could become misaligned is discussed.
- On an operations level, the changing server environment is problematic; for network security appliances and systems on dynamic ranges, the possibility of drift is acute.

Source: Frost & Sullivan analysis.

Points of Competitive Differentiation (continued)

Best Scan Engine—Digital Defense, Inc. (continued)

Scan-to-Scan Endpoint Correlation	Servers - % Change over 90 Days	Clients - % Change over 90 Days
IP Address	4%	36%
DNS Hostname	46%	42%
NETBIOS Hostname	34%	20%

Source: Digital Defense, Inc.

- The table above demonstrates what could happen in a typical enterprise network. While no singular set of software upgrades, service disruptions, or server array groupings is particularly destructive, over time, the network landscape changes appreciably.
- In another sample network, DDI considered an environment where there were 40,000 servers and 60,000 client devices. In this scenario, the one year drift showed that there could be as many as 15% server duplicates: another 15% of servers had stale VM data, and client machines could be mismatched as much as 83% of the time.
- Conventional VM scanner and analytics may be able to see the drift. However, the analytics engines would have to accumulate IP addresses, NetBIOS, DNS hostnames, and MAC addresses and correlate the results over several scans to reconcile the genuine host mapping against the true NMAP.
- Self-evidently, the missed associations show up as false positives.

Source: Frost & Sullivan analysis.

Points of Competitive Differentiation (continued)

Best Scan Engine—Digital Defense, Inc. (continued)

- The DDI scan engine works on the principle of real-time event-based tuning. DDI's VA scanner (named Network Intelligence Reconnaissance Vehicle (NIRV)) is event driven and can adjust its plugin sets and auditing mechanisms in real time as it learns more information about the host and network.
- Information is gleaned from each host, service, and application and is reused throughout the scope of the assessment, allowing for a more thorough audit of its peers.
- With NIRV, the host is fingerprinted meaning the scan initiates explicit testing based upon the characteristics of the host, helping fine-tune the testing of network assets. Additionally, when a new host is discovered, the DDI scan engine automatically triggers basic Web Application Scanning and password auditing.
- The client can further refine the efficacy of DDI Frontline VM. Scan creation includes a number of configurable elements to best accommodate scanning needs. These include:
  - General Settings – The settings include scan name, recurrence, start time/date, email notifications, import to Active View, and business group access to scan results.
  - Scan Policy – Policy parameters can be customized or set to default. The scan speed can be set too.
  - Scan Targets – A company can schedule full or partial network scans. Settings include ad-hoc individual IP(s) for ranges/ports, pre-configured asset group(s), and dynamically generated asset group(s).
- Even in mature network environments, host characteristics are not always readily understood (or altogether known). In this event, DDI's scanning technology includes an "auto fragile" mode, to ensure printers and devices can be scanned without impacting operations.

Source: Frost & Sullivan analysis.

Vendor Profile: Digital Defense, Inc.

Overview

- Digital Defense, Inc. (DDI) started as a professional services and consultancy company that focused on cyber network security. In 1999, DDI began to offer software appliances as an extension from the tools that it used and continues to use in professional services.
- Products and services offered by DDI include:
  - Vulnerability Scanning/ Management
  - Web application penetration testing
  - Professional services (e.g. risk, wireless, and physical security assessments)
  - The combination of DDI's certified Security Analysts, patented scanning technology and proprietary cloud-based vulnerability management platform forms the company's Vulnerability Management as a Service (VMaaS) delivery model.

  *- Penetration testing

  * - Social engineering

  * - Security awareness education
- The profile focuses on the technologies comprising the Frontline™ Vulnerability Manager, and DDI's approach to threat detection.

Product

- Digital Defense was the original vulnerability-management-as-a-service (VMaaS) provider.
- Vulnerability management is offered as a client-managed (VM) or DDI managed service (VM-Pro) which includes the expertise of a Personal Security Analyst (PSA) to project manage the full vulnerability lifecycle from initial discovery to successful remediation.
- DDI's vulnerability management solution includes the ability to assess and manage vulnerabilities on external/perimeter devices, cloud and private cloud infrastructures and internal assets with the aid of a scanning appliance referred to as a Reconnaissance Network Appliance (RNA).

Source: Frost & Sullivan

Vendor Profile: Digital Defense, Inc. (continued)

Product (continued)

- The RNA can be installed as either a hardware or virtual appliance depending on the client's preference and environment.
- An advantage to using a cloud-based delivery mechanism is clients log onto an Internet accessible portal.

Key Differentiations in Scan Technology

- Earlier in the report, Digital Defense was cited with a Point of Competitive Differentiation for Best Scan Engine.
- Frontline VM addresses the reality that enterprise networks are a dynamic environment.
- The illustration on the following page shows how the results of traditional VA scanning can be compromised.
- Digital Defense has a proprietary technology that is used to first scan for changes or to discover new hosts in the network; the theory is without true comprehension of the hosts, false positives and an over reporting of assets is inevitable.
- By focusing on Host Discovery, fingerprinting, and explicit testing based upon characteristics of the host, Frontline VM yields few false positives, and cuts down on the possibility of abrasion to the endpoints.
- The patent-pending Network Host Correlation (also referred to as scan-to-scan reconciliation) solves the issues associated with poor host matching algorithms that introduce "ghost" assets into the network asset inventory often found with other remote unauthenticated scanning.
- A side benefit to Network Host Correlation is it eliminates the need for credentialed or agent-based scanning which also reduces false positives.

Source: Frost & Sullivan

Vendor Profile: Digital Defense, Inc. (continued)

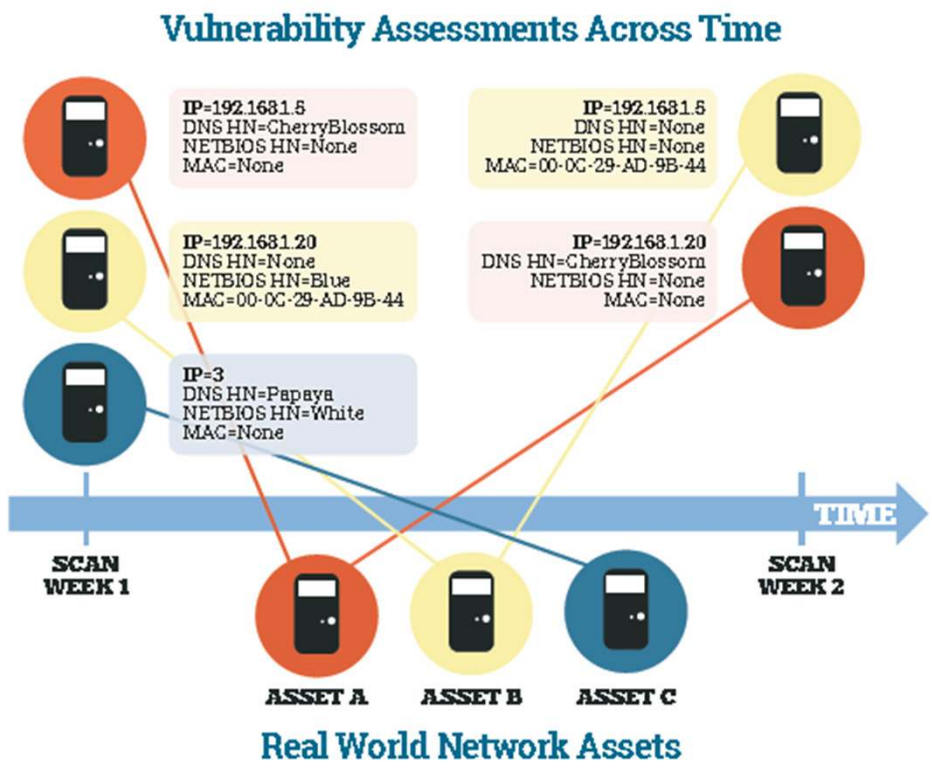


FIGURE 3: Matching Assessed Hosts to their Correct Real World Assets

In this example, Assets A and B have been re-deployed or re-configured since week 1, and Asset C has either been removed from the network (either temporarily or permanently) or was powered down/offline at the time of the second test.

- The illustration to the left shows how assets can be lost or changed in the time between VA scans.
- Scan engines are designed to scan devices against their IP address, domain name system host name (DNS HN), Network Basic Input/Output System (NetBIOS HN), or MAC address.
- In an enterprise network, any number of variables can create problematic scan conditions.
  - Servers are frequently reconfigured.
  - New software OS is pushed to devices/servers.
  - Routing tables are changed.
  - Semi transient devices drop on and off the network.
  - The device was powered down at the time of the scan.
  - Devices that have agents uploaded can be dropped from the network if the agent fails or degrades.
  - Sudden power failures or latencies and bottlenecks can disrupt scans.
- The illustration shows how devices could be dropped or suddenly show up as assets associated with different servers.

From the Whitepaper: Is Your Security Ecosystem Inaccurately Portraying Your Information Security Risk?

Used with Permission Digital Defense, Inc.

Source: Frost & Sullivan

Vendor Profile: Digital Defense, Inc. (continued)

Beyond Scan Technology

- Vulnerability management is more than the detection and reporting of vulnerabilities. Customers come to expect visibility, benchmarking, internal/external compliance reporting, bidirectional support in the form of integration with, or APIs for, other cyber security tools, and the beginning of remediation.
- Frontline VM can be set to configure scan parameters, schedule assessments, access scan results, manage vulnerabilities, view vulnerability description and solutions, sort, search and filter results and generate detailed technical, executive and summary reports from filtered search results from assessments or the Active View. (Active View is a vulnerability management database that correlates data across scans or hosts).
- The extensive filtering capabilities lead to granular vulnerability reporting. DDI incorporates a Security GPA® grading system that incorporates not only the risk ratings of vulnerabilities identified on the host, but also weighs-in the criticality of a host to the network for a more holistic risk value.
- Security GPA is intuitively easy (the grade is A-F and is based on a scholastic 4.0 GPA scale). The Security GPA can be tracked by host or network, over time and across the “DDI Cloud” for an at a glance aggregate comparison of security posture.
- Frontline VM services are offered as three service modules: Frontline VM, Frontline VM-Pro, and Frontline PCI-Pro. For compliance purposes, many customers choose PCI-Pro.
- DDI has been a certified PCI standards Approved Scanning Vendor for 11 years.
- If clients use the PCI-Professional managed service, they receive the expertise of a Personal Security Analyst to help guide clients through PCI compliance. DDI works with clients to identify those issues that may prevent certification and perform regular scanning to help clients achieve PCI compliance.

Source: Frost & Sullivan

Vendor Profile: Digital Defense, Inc. (continued)

Beyond Scan Technology (continued)

- Digital Defense will offer that by way of cleaning up false positives, it becomes a valuable network security tool made more valuable in mature IT/security network environments; the thinking is that the elimination of false positives helps tools that communicate bi-directionally.
- Frontline VM includes a RESTful API to enable integration with other network security platforms and third-party applications. A Software Developer Kit or SDK is available to assist organizations wanting to take advantage of the Frontline VM API.
- Current integrations include ServiceNow, Microsoft ADFS (SAML 2.0), Splunk, IBM QRadar and ZenDesk. Several other integrations are being pursued or are in nascent stages.
- Initiating the remediation process is the last operation expected from a VM platform. The Frontline VM interface includes remediation solutions/recommendations for each vulnerability identified along with associated resources (such as CVE references or links to vendor provided patches).
- Automated remediation is available via integration to existing patch management solutions through a RESTful API.

Final Notes

- Digital Defense has a varied clientele—customers use Frontline VM on networks from tens of hosts to large enterprise customers. DDI's most successful vertical market is financial and banking services.
- Digital Defense has a wide range of pricing modules and service levels. DDI VM solution prices are based on scope (internet-facing or full network devices), the number of targets to be scanned (live hosts, not IP ranges), and frequency of scanning (one-time, annual, quarterly, monthly or on-demand).
- Lastly, Digital Defense has significant partnerships for white-labeled services.

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of Appliances. Our Appliances acknowledge, when ordering or downloading, that Frost & Sullivan research services are for Appliances' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to nonAppliances without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan

331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Source: Frost & Sullivan