Infonetics RESEARCH

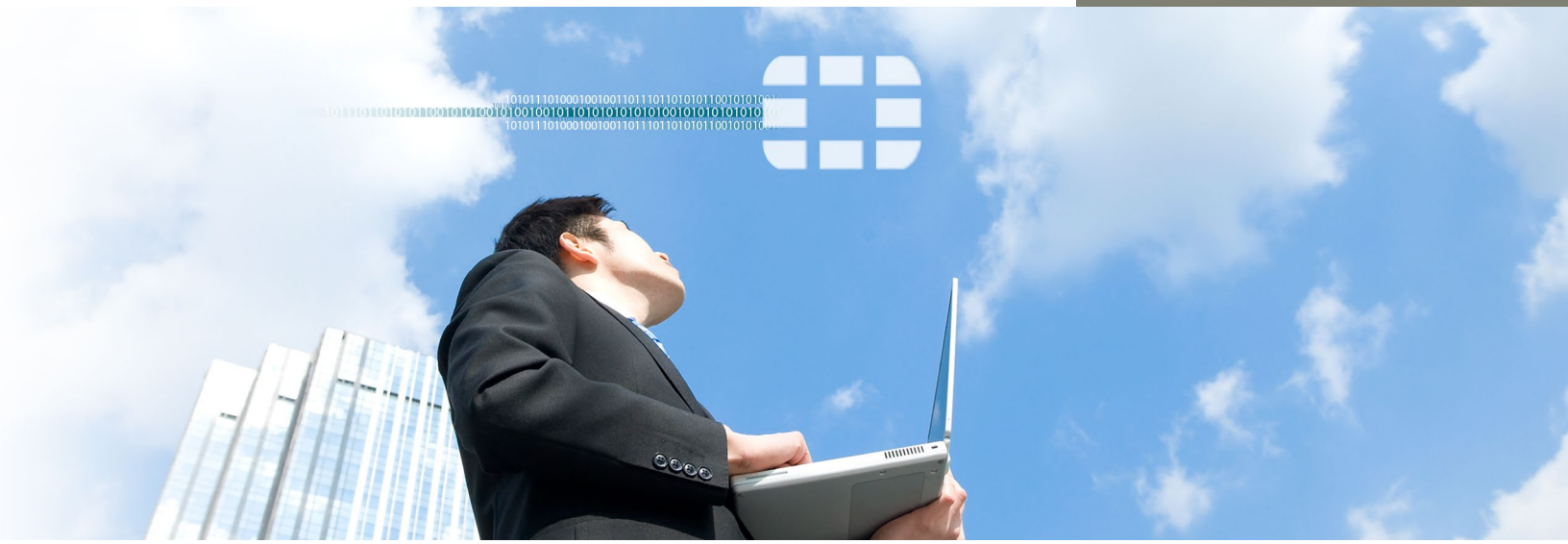
Data Center Security Products

Biannual Worldwide and Regional Market Share, Size, and Forecasts: Excerpts

FORTINET®

Data Center Security –

Virtual Appliances Ready for Prime Time?



Data Center Security – Virtual Appliances Ready for Prime Time?

The adoption of virtualization, cloud, and software-defined networking (SDN) is transforming the enterprise data center and making IT infrastructure more agile and elastic. The resulting increase in IT and business productivity is driving increased activity and traffic, leading to refresh of ever-faster networking and firewall hardware. Yet the abstraction of the network and data flows is also leading a more dynamic environment, creating potential challenges for network visibility and control.

Security virtual appliances, which encapsulate the same firewall and network security engines within a virtual form factor, can be placed closer to virtualized switches and traffic flows to regain visibility and be orchestrated with changes in the logical network so that there are minimal protection or compliance gaps.

Fortinet's strong focus and differentiation based on leading ASIC hardware design has led to rapid growth as third-largest data center security hardware vendor, according to Infonetics Research. Yet Fortinet has also invested heavily in virtual security appliances, with support for all leading hypervisors including VMware, Citrix, Xen, Hyper-V, and KVM, and is now expanding multi-vendor platform support to leading cloud and SDN platforms such as Amazon Web services and VMware's Software-Defined Data Center as well. Fortinet offers one of the broadest virtual appliance lineups with nearly a dozen different virtual appliance solutions available today ranging from our flagship FortiGate firewall and consolidated security to web security, e-mail security, and central management and analytics.

In the following report from Infonetics Research, Principal Analyst Jeff Wilson discusses the drivers for security virtual appliance growth in the data center and why virtual appliance adoption growth will far outpace that of traditional data center hardware security appliances in the coming years.

INFONETICS RESEARCH REPORT EXCERPTS

Data Center Security Products

Biannual Worldwide and Regional Market Share, Size, and Forecasts: 1st Edition

Report Excerpts

May 2014

By Analyst Jeff Wilson

Infonetics RESEARCH

Table of Contents

List of Exhibits

TOP TAKEAWAYS: THE MOVE TO SDN AND NFV SIGNAL MAJOR CHANGE IN DATA CENTER SECURITY MARKET

Enterprises and service providers are upgrading data centers to support huge increases in traffic and handle the massive waves of attacks they face every day; they're investing in data center security solutions now because they need to increase overall security throughput, increase their ability to handle sessions/connections, add new threat protection capabilities, and add security to their virtualized/cloud environments. Historically data centers have been protected by big-iron security solutions and complex webs of security appliances and load-balancing infrastructure, but as more providers virtualize their data centers and roll out SDNs and NFV, we're forecasting a fairly significant revenue transition: from hardware appliances to virtual appliances and purpose-built security solutions that interface directly with hypervisors, with SDN controllers via APIs, or orchestration platforms.

VIRTUAL SECURITY APPLIANCES: READY FOR PRIME TIME?

Revenue for virtual security appliances was up 8% in 4Q13 over 3Q13, hitting $158.8M, and it will reach $1.3B by CY18, a 5-year CAGR of 17%. Revenue was up 17% in CY13 reaching $586.2M over CY12. These numbers are based on market size and forecast data for the firewall, content security, SSL VPN, and IDS/IPS space, as well as direct input from virtual appliance vendors themselves; virtual security appliance performance reflects the growth of those base markets in addition to aggressive rollouts of server virtualization, SDN, and NFV.

The world has never been more tuned-in to broad privacy and security issues, and the recent revelations about the NSA and PRISM are forcing consumers and businesses around the globe to reevaluate their security posture, preferred vendors, and deployment strategies. The most recent revelation that the NSA has been secretly siphoning data from Google and Yahoo data centers worldwide puts a laser-focus on the need for security at all levels of the data center (from layer 1 transport all the way up to individual applications and data).

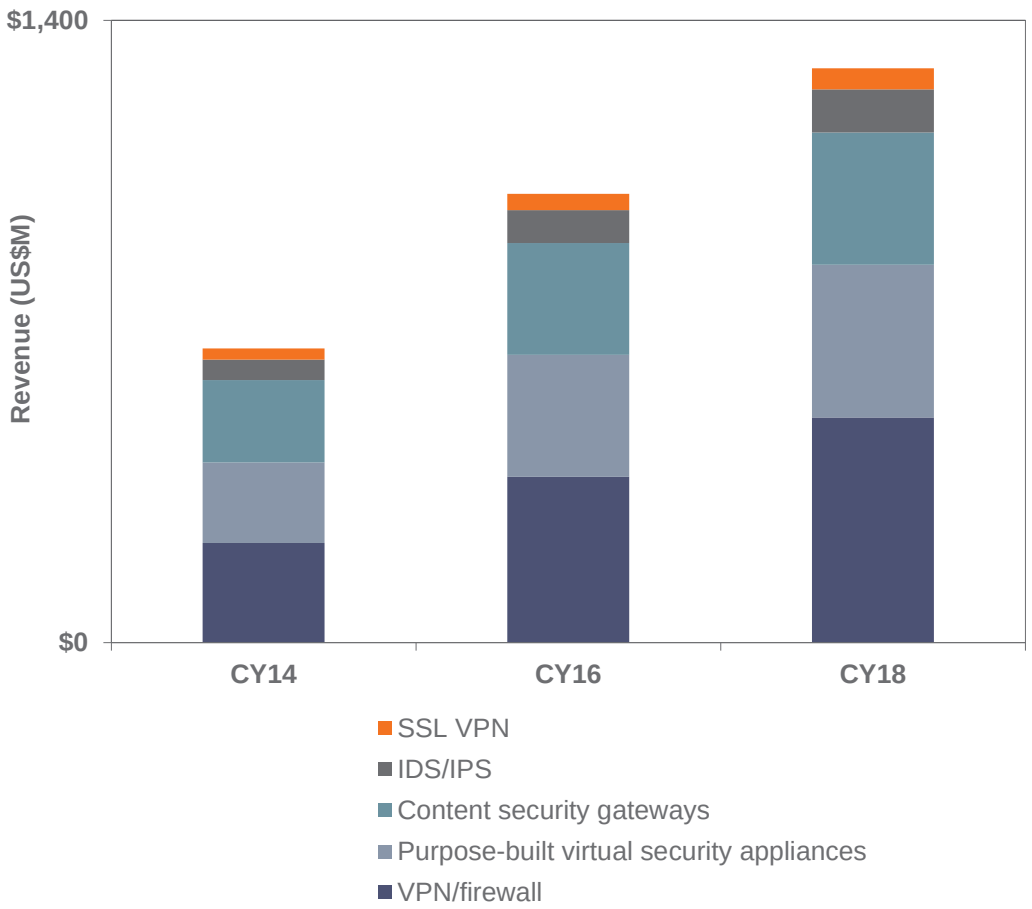
This nascent market is primed for tremendous growth over the next 5 years because of the combined impact of:

- Increasing volume and variety of security threats
- Buildout of cloud infrastructure
- Service provider data center upgrades
- Rapid adoption of server virtualization
- Rollout of SDNs and NFV
- Enterprise and government data center consolidation
- New security challenges presented by virtualized environments
- The cost and ineffectiveness of traditional security solutions in virtualized environments
- Availability and rapid maturation of virtual appliance solutions from a wide variety of vendors

Long-Term Forecast by Category: Revenue Doubles between 2013 and 2018

We expect a growth spike predicted in virtual appliance revenue starting in 2015 (and a corresponding growth decline in the hardware appliance space) due to the deployment of the next generation of network infrastructure using SDN and NFV progressing through the second half of 2013 and all of 2014. Once the new network infrastructure is in place, security spending will begin, and this drives new growth; after the spike in 2015, we predict growth to level back off to where it was in 2012–2013. Though SDN and NFV are hot topics in networking, and will force vendors who build networking products and applications to offer new form factors and re-architect some of their solutions, security vendors have been working on adapting threat detection and mitigation solutions to work in virtualized environments for over 5 years, and are familiar with the idea of mapping their security products to whatever API(s) become the most commonly used, so for security vendors, working with OpenFlow, OpenStack, or whatever other open or closed SDN/NFV technologies are widely deployed is an evolutionary change, not a revolutionary one.

Exhibit 1 **Virtual Security Appliance Revenue by Category**



Juniper, Trend Micro, Cisco, Check Point, F5, Blue Coat, Citrix, IBM, Symantec, HP, IBM, Enterasys, Fortinet, WatchGuard, VMware, Microsoft, and just about every vendor with a toe in security or server virtualization now has a virtual appliance offering. Most vendors started by porting their existing platforms to VMware (and then Microsoft and Citrix), but a few have jumped in and developed (or acquired) new solutions for virtualized environments. The breadth and depth of the offerings vary, but nearly all security vendors have increased their product development and marketing focus for virtual appliances significantly over the last 3 years in an attempt to ride the wave of cloud infrastructure spending, and now the hyper-focus on SDNs and NFV.

Manufacturers: Coopetition's the Name of the Game

The vendor landscape in the virtual security appliance market is varied and pulls from 3 primary groups:

- **Traditional security product manufacturers,** including Check Point, Citrix, F5, Juniper, Cisco, Stonesoft, Trend Micro, IBM, HP, Enterasys, WatchGuard, SonicWALL, Symantec, etc., offer specialized "virtual" software versions, software updates to existing appliances that interface with hypervisor or specialized security APIs, or standalone "virtual version" appliances that perform this function. Traditional vendors cover a wide range of security technologies, and each are uniquely positioned (HP and IBM are both major players in the server space for example). Juniper's acquisition of Altor blurred the line between traditional security vendors and standalone players, and was the first consolidation event of many. The list of traditional vendors offering products in this space grows longer every quarter.
- **Standalone players** like Catbird, Reflex, Wedge, and Vyatta offer software and/or hardware platforms built from the ground up to manage security issues related to virtualized server infrastructure or SDNs/NFV. Specialized players offer platforms that have traditional security functionality (firewalls, content security, IDS/IPS) but also configuration, management, and compliance for virtualized environments. There are already partnerships between standalone players and the other players in this space.
- The **server virtualization platform vendors** themselves (VMware, Citrix, and Microsoft) walk the line between integrating security functionality, selling add-on security functionality, and developing APIs so third party vendors can interact with their platforms. VMware has already made several acquisitions in this space (like BlueLane), and is directly competing with their vShield product offering, but offers a security API, but also has direct partnerships with many of the vendors mentioned above. Coopetition will be a long-term trend in the virtual security market.

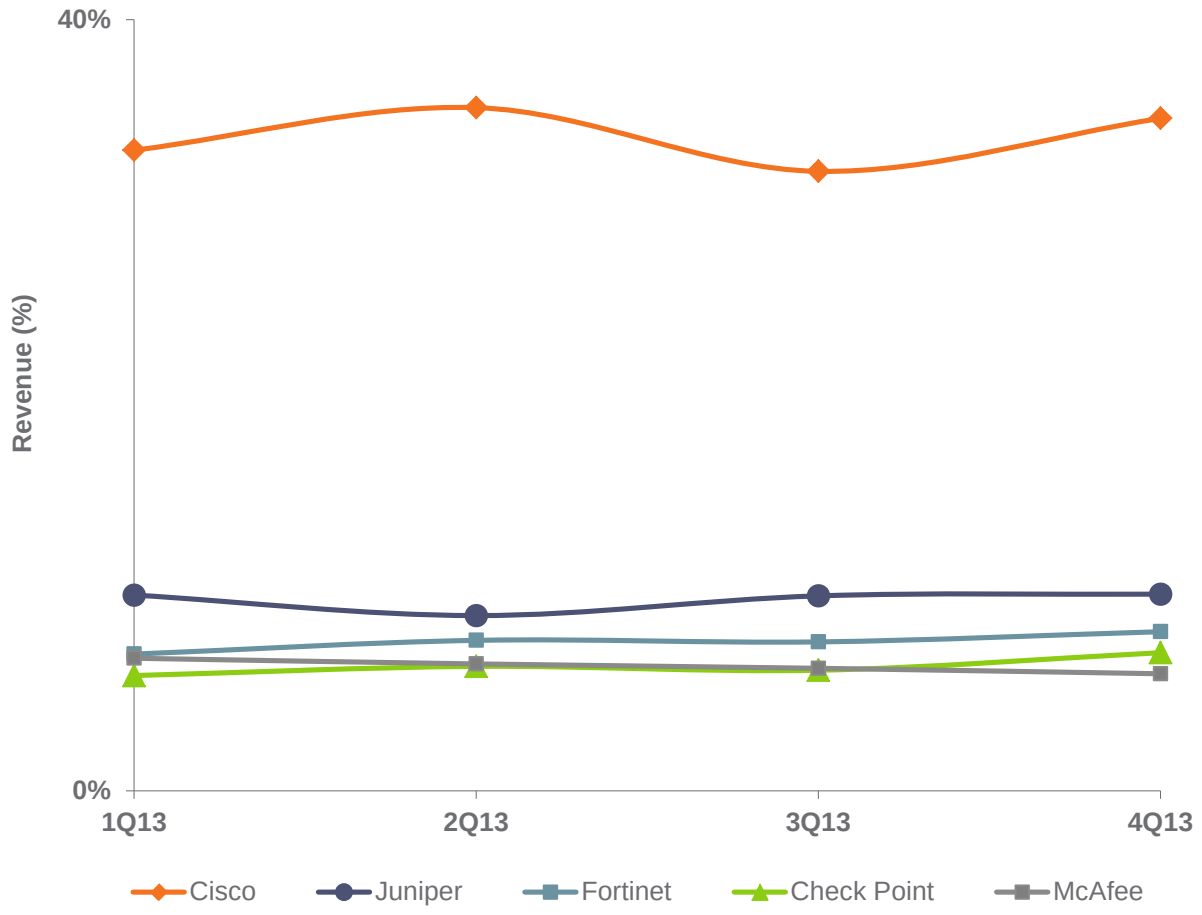
We're not yet publishing market share in this segment, since it's very immature, and most vendors provide only very broad guidance on quarterly performance.

Data Center Firewall Vendor Spotlight: Fortinet

Among the traditional security product manufacturers, market share for security appliances in the data center fairly closely mirrors overall market share for security solutions. Cisco led data center security appliance revenue market share in 4Q13, and Juniper was in second place. Fortinet took the third spot, Check Point jumped up to fourth, and McAfee Rounded out the top 5.

Fortinet took third due to their strong position in many mid-sized data centers and excellent price/performance position (their recently launched 3700D has been wildly successful in some high-profile data center deals).

Exhibit 2 **Data Center Security Appliance Market Share**



End-User Adoption of Virtualization in the Data Center, and Data Center Security Plans

The strong forecast for virtual appliances in this service is based on the fact that existing rollouts of server virtualization, SDNs, and NFV within enterprises and carriers will get significantly larger between now and 2018, and that the rollout of public and private cloud infrastructure (to meet the demand of IT organizations to move to the cloud) will drive sales of new security solutions. In early December of 2010, the US Federal Government OMB announced a major IT initiative to drastically reduce the number of data centers (from over 2,000 to about 800), and to aggressively migrate to the cloud; one example of the kind of aggressive moves toward cloud and virtualized infrastructure on the horizon beyond the obvious cloud providers like Amazon that we see in the trade press daily.

Users are looking to balance their investments in appliances, virtual appliances, and server software to get strong, consistent security at a cost that can be justified, and a keen understanding of the interplay between those key security products in the data center is a critical part of accurately forecasting the market. To help sort through the complex issues involved in sizing the data center security space, we conducted a survey covering end-user plans for data center security, and in March 2014 we published a report based on interviews with 104 medium and large organizations in North America who operate their own data centers, titled *Data Center Security Strategies and Vendor Leadership: North American Enterprise Survey*. Key findings that were directly applied to the market sizing and forecast in this service include:

- Respondents favor a multi-layered model for deploying security in the data center; more than half of respondents are already using hardware appliances, virtual appliances, and server software.
- The most significant transformation affecting enterprise data centers today is the adoption of server virtualization technology, and many respondents consider it to be an important driver.

Technology Drivers

The adoption of server virtualization within data centers at small, medium, and large organizations around the world and the rollout of the infrastructure required to deliver IT services in the cloud is driving significant change in the technical requirements for security solutions. Virtualized server environments (from a single virtualized server in a wiring closet at an SMB running a mix of apps to a massive data center used to deliver cloud services) present unique challenges. As enterprises and carriers around the globe move to virtualize more of their infrastructure with the deployment of SDNs and NFV, there will be even larger changes in security architecture. We believe the following are key drivers in the data center security space:

- Inter-VM threats are a significant new issue; security devices sitting in front simply can't see threats when traffic is travelling between virtual machines on a single physical server.
- In the past, preventing inter-VM threats meant installing individual security technologies/licenses per virtual machine, which does work to prevent threats from crossing VMs and can be incredibly expensive and impossible to manage.
- As virtualization vendors continue to develop and improve security APIs that allow security products outside the virtual (or physical) server to have visibility into traffic, security architectures will continue to change.
- In small environments where virtualized servers run a broad range of applications, there is a need for virtual appliances with a broad range of security functionality.
- In cloud environments, virtual security solutions may need to deal with a narrower set of applications and protocols (mostly web-based), but they will need to scale, and provide multi-tenancy features that allow providers to deliver services to many customers from one solution.
- The deployment of SDNs in data centers and NFV in large carrier networks will impact security investment, as an SDN/NFV environment is a logical place to deploy virtualized security solutions, and the ability to apply security policies logically (and not physically) is not a new topic at all; it's likely that in many data center environments security is already virtual, and when SDNs are more widely deployed, security shouldn't be a roadblock, rather, it's likely to be an extension of an existing security solution deployed over the SDN. On the NFV front, carriers will be more than happy to interface with elastic software-based security solutions that can be provisioned side-by-side with other virtualized network services, and a variety of security vendors (new and old) are already working on developing the necessary interfaces.

This all leads to a trend, over time, of centralizing security for virtualized environments of all types and building software solutions that that interact with the hypervisors, SDN controller APIs, and orchestration platforms.

REPORT AUTHOR

Jeff Wilson

Principal Analyst, Security

Infonetics Research

+1 408.583.3337 | jeff@infonetics.com

Twitter: @securityjeff

ABOUT INFONETICS RESEARCH

Infonetics Research is an international market research and consulting analyst firm serving the communications industry since 1990. A leader in defining and tracking emerging and established technologies in all world regions, Infonetics helps clients plan, strategize, and compete more effectively.

REPORT REPRINTS AND CUSTOM RESEARCH

To learn about distributing excerpts from Infonetics reports or custom research, please contact:

North America (West) and Asia Pacific
Larry Howard, Vice President, larry@infonetics.com, +1 408.583.3335

North America (East, Midwest, Texas), Latin America and EMEA
Scott Coyne, Senior Account Director, scott@infonetics.com, +1 408.583.3395

Greater China and Southeast Asia 大中华区及东南亚地区
Jeffrey Song, Market Analyst 市场分析师及客户经理 jeffrey@infonetics.com, +86 21.3919.8505