Market Share

Worldwide Cloud Security (Software-Defined Compute Workload Security and Firewall Fabric) Market Shares, 2018: Protecting Workloads in Hybrid and Multicloud

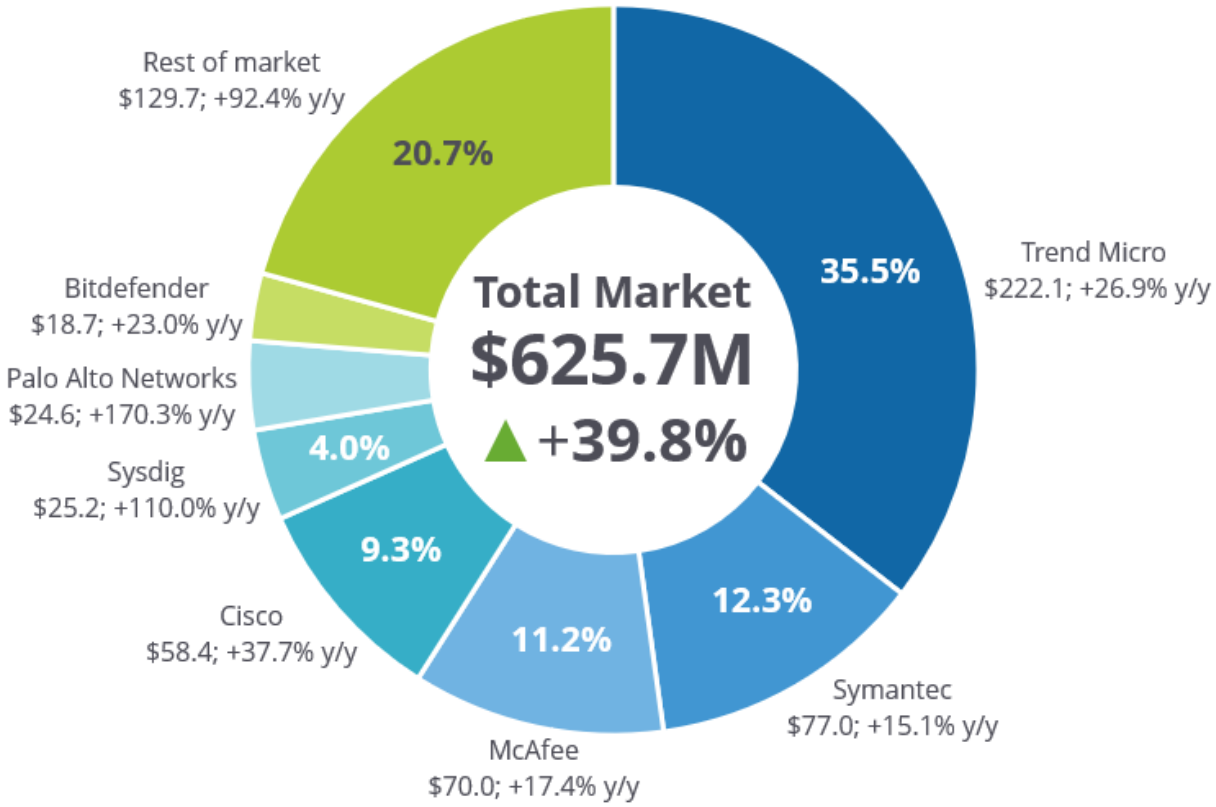
Frank Dickson

THIS IDC MARKET SHARE EXCERPT FEATURES: TREND MICRO

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Cloud Security (Software-Defined Compute Workload Security and Firewall Fabric) 2018 Share Snapshot



Note: 2018 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2019

November 2019, IDC #US45638919e

IN THIS EXCERPT

The content for this excerpt was taken directly from Worldwide Cloud Security (Software-Defined Compute Workload Security and Firewall Fabric) Market Shares, 2018: Protecting Workloads in Hybrid and Multicloud (Doc# US45638919). All or parts of the following sections are included in this excerpt: Executive Summary, Advice for Technology Suppliers, Market Share, Who Shaped the Year, Market Context, Methodology, Market Definition, and Related Research sections that relate specifically to Trend Micro, and any figures and or tables relevant to Trend Micro.

EXECUTIVE SUMMARY

Software-defined compute (SDC) encompasses a number of compute abstraction technologies that are implemented at various layers of the system software stack. SDC workload security solutions are not intended to protect the integrity of the SDC infrastructure (hypervisors, control plane/management, and orchestration) but to protect what runs on top of the SDC infrastructure (virtual machines [VMs] and containers). SDC workload security and firewall fabrics are components of an integrated set of offerings that span threat protection, vulnerability management, analytics, and data integrity for software-defined compute environments.

In 2009, Trend Micro bought Third Brigade, a provider of host intrusion prevention software (HIPS) and firewall software. Starting with 50 Third Brigade employees, Trend Micro has become the dominant leader in SDC workload security. Vendors such as Symantec, McAfee, Cisco, and Palo Alto Networks are making strong efforts to grab future share of the market from Trend Micro. "The rising tide" bodes well for all vendors.

This IDC study discusses worldwide cloud security market shares of software-defined compute workload security and firewall fabric for 2018.

"Trend Micro turned its 2009 acquisition of Third Brigade into a dominant position in software-defined compute workload security," according to Frank Dickson, program vice president, Cybersecurity Products at IDC. "However, the future is not yet written. Vendors such as Symantec, McAfee, Cisco, and Palo Alto Networks are making both organic and inorganic investments to grab future share of the market; the potential booty is plentiful."

ADVICE FOR TECHNOLOGY SUPPLIERS

Before providing advice, defining the market is important. The goal of this study is not to provide market share for all of software-defined compute security or even just "cloud" security, but to provide market shares for two "cloud" security categories: SDC workload security and firewall fabrics; a detailed explanation is forthcoming.

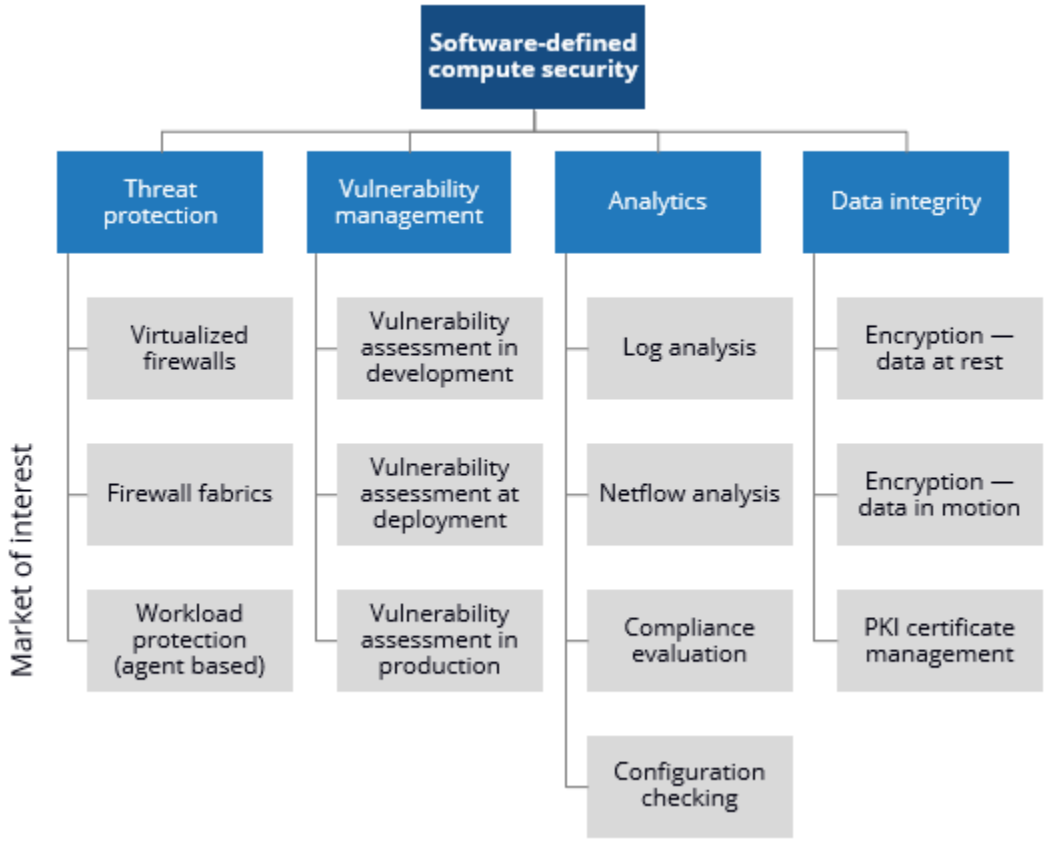
Software-defined compute encompasses a number of compute abstraction technologies that are implemented at various layers of the system software stack. SDC security solutions are not intended to protect the integrity of the SDC infrastructure (hypervisors, control plane/management, and orchestration) but to protect what runs on top of the SDC infrastructure (VMs and containers). SDC technologies are often used in the context of public or private clouds, but they can also be implemented in noncloud environments — particularly virtualized and/or containerized environments. Workload security solutions are designed to maintain the integrity of SDC servers, providing protection

features that include antimalware, desktop firewall, host intrusion detection, application control, and integrity monitoring. These products accomplish their goals by ensuring the system does not run malicious software that can compromise business applications and data on the servers. As with other endpoint security submarkets, software-defined compute workload security and firewall fabric solutions are mutually exclusive categories distinct from physical server or antimalware offerings. Workload security solutions provide protection to three categories of SDC compute environments:

- Virtual machine software, also known today as hypervisor software, uses low-level capabilities offered by certain hardware environments or installs a complete hardware emulation layer using software to support multiple operating environments and the related stacks of applications, application development and deployment software, and system infrastructure software. This segmentation is often referred to as server virtualization or partitioning. Representative solutions include Citrix XenServer, IBM (PowerVM), Microsoft Hyper-V (included with Windows Server), Oracle VM for x86, Oracle VM for SPARC, Oracle Solaris Kernel Zones, and VMware vSphere.
- Containers are an operating system (OS) segmentation technology, similar in concept to hypervisors except they abstract an OS instead of server hardware. Containers rely on segmenting away parts of the operating system. Optionally, various OS user space tools and libraries may also be included. Representative solutions include Canonical (LXD), CoreOS rkt, CoreOS Tectonic, Docker CE, Docker EE (portions thereof), Microsoft Windows Containers (as part of Windows Server), Oracle Solaris Native Zones, VMware's Integrated Containers, Photon Platform, and Kubernetes open source container orchestration software.
- Cloud system software represents a tightly bundled combination of server abstraction and orchestration software and node-level controller software, often sold as part of a larger cloud infrastructure platform solution. The compute resource layer represents a combination of virtual machine, container engine, and/or operating system and orchestration software running on a physical server, which is designated as a cloud compute node. The controller software virtualizes groups of compute nodes into a single logical compute resource. Cloud system software also exposes APIs that simplify the scheduling and control of VMs, containers, and bare metal servers running on the node and maintains a database of resource state and policies.
- Providing software-defined compute security is not executed by a single technology or offering but by an integrated set of offerings that span threat protection, vulnerability management, analytics, and data integrity. Figure 2 provides IDC's cloud security framework.

FIGURE 2

IDC's Cloud Security Framework, 2019



Source: IDC, 2019

Threat protection is accomplished by three primary approaches:

- **Virtualized firewalls:** Virtualized firewall products are created to filter network traffic through packet filtering, stateful inspection, and/or proxy. Some firewalls may include virtual private networking capabilities along with other security features including UTM functionality such as IPS, antimalware, URL filtering, and application layer controls. Virtualized firewall "appliances" are built with a specialized operating system and provide network traffic filtering and monitoring for virtualized environments, including public and private clouds (e.g., Amazon Web Services [AWS] Azure, kernel-based virtual machine [KVM], and VMware). A virtualized firewall inspects packets and uses security policy rules to block unapproved communication into and out of a software-defined compute environment or between VMs. Virtualized firewalls are not included in the scope of this document.
- **Firewall fabrics:** Firewall fabrics, under the strictest of definitions, could be included as part of virtualized firewalls. Firewall fabrics implement a mesh of firewalls around virtualized machines or containers, controlling access to the VM or container based on IP, protocol, and/or instruction. Firewall fabric solutions typically implement security from outside of the VM

or container (not agent-centric protection) and often employ analytics to discover connections between the protected workload and resources outside of the VM or container. Firewall fabrics are included in the scope of this document.

- **Workload protection:** Workload protection products provision security using or leveraging an endpoint agent or client as a core or fundamental component. If a solution does not include a client or an agent, the solution would be included within firewall fabrics or possibly another functional market such as network or cybersecurity AIRO. Protections may include antivirus, virtualized firewall, host intrusion prevention software, and application control. Firewall fabrics are included in the scope of this document.

MARKET SHARE

In 2009, Trend Micro bought Third Brigade, a provider of host intrusion prevention software and firewall software. Trend Micro's CEO Eva Chen defined a strategy to evolve Third Brigade's software to meet the security needs of customers operating in cloud environments and datacenters with virtualized systems... and that Trend Micro did. Starting with 50 employees in 2009, Trend Micro has become the dominant leader in SDC workload protection.

The future of the market though has not yet been decided. Vendors such as Symantec, McAfee, Cisco, and Palo Alto Networks are making both organic and inorganic investments to grab share. Currently, the future rewards are promising. As grabbling even fractions of a percentage of market share in traditional endpoint security takes significant effort and investment, addressing "greenfield" cloud opportunities has a special appeal. In addition, start-ups are strategically attacking newer cloud approaches such as Kubernetes, managed Kubernetes, and serverless. Although the new approaches are no more than "curiosity" of market share currently, the market will move there; "younger" upstarts like Sysdig, Aqua, Tigera, and Protego Labs will be waiting (see Table 1).

TABLE 1

Worldwide Cloud Security (Software-Defined Compute Workload Security and Firewall Fabric) Revenue by Vendor, 2017 and 2018

	Revenue ($M)		Share (%)		
	2017	2018	2017	2018	2017–2018 Growth (%)
Trend Micro	175.0	222.1	39.1	35.5	26.9
Symantec	66.9	77.0	14.9	12.3	15.1
McAfee	59.6	70.0	13.3	11.2	17.4
Cisco	42.4	58.4	9.5	9.3	37.7
Sysdig	12.0	25.2	2.7	4.0	110.0
Other	91.7	173	20.5	27.7	88
Total	447.6	625.7	100.0	100.0	39.8

Source: IDC, 2019

WHO SHAPED THE YEAR

Trend Micro

Trend Micro acquired Immunio in November of 2017. The Immunio acquisition is being integrated into the Trend Micro portfolio. Immunio provides real-time application security, providing automatic detection and protection against application security vulnerabilities based on the actions executed by code. Instead of analyzing the code in its static form or using pattern matching on inputs to the code, the Immunio approach analyzes the operations that the code executes, such as operating system calls or database calls.

Immunio can identify anomalous operations using various techniques that may be indicative of malicious activity and actual vulnerabilities. This approach can result in reduced false negatives and positives. Perhaps more importantly, by embedding the application security into the running application, there is no slowdown to the development and release cycles.

MARKET CONTEXT

Infrastructure as a service (IaaS) will remain the second-largest IT cloud services category – with strong growth in cloud storage (31.5% CAGR) and cloud compute/server services (31.4% CAGR).

Both IaaS categories will be driven by the growth of PaaS and SaaS services that will continue to require underlying IaaS capacity.

In the past three years, IDC has predicted that the public cloud would be going everywhere — that a new "distributed cloud" model, supporting on-premise and edge ("hybrid") deployment, as well as multivendor ("multicloud") support, of public cloud software stacks would emerge. In the past year, with the announcement of such distributed cloud platforms by virtually all major cloud platform players, we have a much clearer view of just how quickly that will happen.

IDC believes that the next big wave of cloud adoption will be fueled by enterprises adopting the cloud across distributed locations and that the ability to support "hybrid" and "multicloud" — that is, distributed cloud — deployments will be a must-have for cloud service providers. These are becoming "the stacks that matter" — for the next decade — and likely beyond. Suppliers that provide "on-premise" and/or edge products or services to enterprises must make sure their offerings are built on, connected to, or somehow provide value within the context of a public cloud service providers' portfolio of technologies and services.

Security remains a concern. In preliminary data from IDC's 2019 *Industry CloudPath Survey* of almost 2,000 enterprise respondents, nearly 50% of enterprises evaluating public clouds and nearly 40% of those evaluating private clouds indicated concerns about security in the cloud. In both the cases, this was the area of greatest concern. This is not new: Concerns about security in the cloud have been a steady result in all our annual cloud user surveys since 2009. What is new is this: In the same IDC's 2019 *Industry CloudPath Survey,* about 45% of respondents cited security capabilities available from cloud service providers as a top benefit of moving to the cloud. For IT executives, security was the top benefit; for line-of-business executives, security was number 2, right behind business agility. As we noted in our previous whole cloud forecast, our assumption is that security (and related issues of privacy and trust) will continue to give pause to enterprises moving systems and data to the cloud, but that pause will get shorter and shorter over time as the incentives to move to the cloud — including stronger security services — get more and more compelling (see *Worldwide Whole Cloud Forecast, 2019–2023,* IDC #US45101619, June 2019).

The ecosystem of tech companies supporting cloud environments will rapidly expand as the variety of cloud services and third-party professional and managed services around the cloud services marketplace focused on enabling traditional enterprise workloads on public clouds has been expanding dramatically over the past several years. At AWS re:Invent 2018, AWS indicated that its partner network expanded by over 35,000 companies in the past two years, which IDC estimates brings the total partner count to over 65,000 companies. We estimate that Google Cloud's partner ecosystem has expanded at least 30% to over 20,000 companies. Our forecast assumes continuing expansion of these cloud services and professional and managed services in the public and hybrid cloud arenas.

Lock-in to proprietary cloud services — which embeds complexity — remains a concern for many enterprises. On the flip side of this concern is the excitement enterprise developers have about many of the new and unique cloud services that providers have introduced over the past several years (see Public Clouds Will Increasingly Be the Primary Route to Access IT Innovation in the "Drivers" section of *Worldwide Whole Cloud Forecast, 2019–2023,* IDC #US45101619, June 2019). Developers (and their organizations) are excited by new capabilities, but a significant percentage — about 30% in IDC's

preliminary 2019 *Industry CloudPath Survey* – are reluctant to become too dependent on single-source services.

We've noted in the past several years that a growing number of major cloud services providers are showing a greater embrace of open source models. As previously mentioned, several major cloud platform players have begun introducing multicloud offerings – ones that run on competitors' clouds. And, of course, there is a fast-growing community of third-party cloud services providers and professional or managed services players focused on helping enterprises interconnect to/from proprietary cloud services. Our assumption is that, over the forecast period, there will be an increase in all these approaches, allaying – albeit not eliminating – lock-in concerns.

Significant Market Developments

The major developments driving demand and market share leadership in the public IT cloud services market include:

- **Digital transformation/innovation as a business priority:** A strategic focus on digital innovation and transformation to remain competitive in their own industries will be a key driver of cloud growth. In 2023, enterprises worldwide will spend more than $2 trillion on technology products and related services to implement digital transformation initiatives, more than double the 2018 spending, reflecting a CAGR of 17.1%. Most of these initiatives (and resulting digital innovations) will require cloud technologies and solutions to power them, making digital transformation the number 1 driver of cloud spending for the foreseeable future.
- **Cloud as the number 1 source for tech innovation:** The major cloud platforms – and their expanding solution ecosystems – are becoming the "launchpad" for virtually all tech innovation. This steady drumbeat of tech innovation is coming from the major public cloud suppliers, making it virtually impossible for enterprises (and developers) seeking advantage through IT not to embrace the public cloud.
- **Enterprise software vendors' journeys to the cloud:** The accelerating migration of enterprise application providers to the SaaS model is bringing their customer bases along with them to the public cloud.
- **Expanding professional and managed services ecosystems:** The expansion of cloud-related managed services and professional services offered by both traditional players and a new generation of competitors is providing enterprises with a rich variety of support services that allow them to more quickly and easily assess, adopt, integrate, and manage cloud services within their overall IT portfolio.
- **Intensifying competition among cloud providers:** Increasing, intense competition among the major cloud service platform players – including Amazon Web Services, Google Cloud, IBM, Microsoft, Oracle, salesforce.com, SAP, and Alibaba – has continued to generally drive down pricing, raise support quality, and stimulate a tech innovation "arms race" that has greatly benefitted tech ecosystem partners, enterprises, and consumers.
- **Industry-specialized cloud platforms:** The embrace of the cloud (and the API-based platform model) as a foundation for digital innovation in virtually every industry has led to the emergence of a growing number of "industry cloud platforms." (The verticalized cloud services/solutions springing from these platforms will be a major driver of growth for the cloud market as a whole during the forecast period.)
- **Distributed cloud (hybrid cloud/multicloud):** As mentioned previously (see the "Drivers" section of *Worldwide Whole Cloud Forecast, 2019-2023,* IDC #US45101619, June 2019), the adoption of a new wave of distributed cloud offerings (hybrid cloud/multicloud) will open new use cases

to the cloud. "Local cloud" offerings — ones that are compatible with, and connected to, the major public cloud platforms (e.g., AWS Outposts, Google Cloud Anthos, IBM Cloud Private, Microsoft Azure Stack) — are poised to become widely deployed in the on-premise datacenters and distributed/edge locations. IDC estimates that, by 2023, at least 25% of public cloud deployments will be running in third-party, on-premise, and edge locations. This will open up a new wave of cloud-powered digital innovation use cases in locations like retail stores, branch offices, factories, other remote facilities, and edge locations.

- **New cloud-centric "power positions" to emerge for the tech supplier world:** The growth of cloud services as the core delivery, consumption, and business model in the tech industry (and beyond) has disrupted the traditional "power positions" in the tech industry. As noted at IDC Directions 2019, five new "competitive neighborhoods" are emerging that represent the new, sustainable power positions for tech suppliers. Technology product and service providers are assessing their competitive positioning for the new marketplace, determining which of these neighborhoods provide the best and most sustainable position and looking at this emerging industry structure to inform which other tech players they should form alliances with. The five "neighborhoods" we've identified are:
  - **Cloud megaplatforms:** These are the big global providers of horizontal/foundational cloud-based IT services, including AWS, Alibaba, Google, IBM, Microsoft, and Oracle. The strategy here is straightforward: It's all about rapid innovation, massive scale, and extending all the way out to customers' datacenters and edge locations. It's also about consolidation: We see room for about three or four big global players.
  - **App-centric platforms:** Competitors here, including Adobe, Intuit, Microsoft, Oracle, salesforce.com, and SAP, are focused on providing platforms that support higher-level business solutions, services, and processes (and usually ride on top of one or more cloud megaplatforms). Competition here is still in the early stages and expanding. The key strategies include becoming megaplatform agnostic to expand reach, building out a true platform and developer ecosystem to expand innovation and value on their platforms, and expanding into increasingly verticalized offerings and platforms.
  - **Industry platforms:** These are essentially industry-focused app-centric platforms, focused on delivering an ecosystem of data, services, and solutions to customers within a single industry or among connected industries. When IDC started covering industry platforms several years ago, we tracked about 60 players; today we track over 400 — this community is growing rapidly. Most players are not traditional tech companies but leaders within an industry, such as Citi, General Motors, Illumina, John Deere, and Walmart. But traditional tech suppliers — especially those competing in the app-centric platform neighborhood — are also entering (or considering entering) the industry platform world. The goal in this neighborhood is to attract data and developers: becoming the "digital innovation crossroads" within an industry.
  - **Multicloud integration and management platforms:** This "neighborhood" is about vendors creating, in effect, "platforms" that help enterprises integrate and manage across multiple clouds. Right now, this neighborhood is in a primordial state, consisting of a "soup" of diverse players up and down the stack, many of which are not yet platform based: network connectivity players, managed service providers, global and regional systems integrators, distributors and VARs, and more. There are three key strategies here: enhancing "platform" capabilities by migrating as much intellectual property into code as possible (making it deliverable as cloud services), racing to expand partnerships with key players across *other* neighborhoods, and pursuing M&A (and partnerships) within *this* neighborhood, linking players up and down the integration and management stack. We

expect to see some leaders emerge that consolidate a portfolio across these diverse integration and management capabilities.

- **Cloud-centric infrastructure and connectivity:** Of course, every "platform" requires real hardware/infrastructure to power it and connectivity services to link to and from it. Thus there is a significant opportunity for infrastructure and network services providers — Cisco, Dell EMC, Ericsson, Hewlett Packard Enterprise, Intel, NetApp, NVIDIA, and others (including ODMs) on the infrastructure side, as well as network services companies like AT&T, BT, China Mobile, NTT, SoftBank, and Verizon. The key strategy for both communities is simple: Increase product and market focus on the distinct needs of the four emerging competitive neighborhoods already mentioned.

METHODOLOGY

The purpose of this section is to provide an overview of the methodology employed by IDC's software analysts for collecting, analyzing, and reporting revenue data for the categories defined by the software taxonomy.

IDC's industry analysts have been measuring and forecasting IT markets for more than 40 years. IDC's software industry analysts have been delivering analysis and prognostications for commercial software markets for more than 25 years.

The market forecast and analysis methodology incorporates information from five different but interrelated sources, as follows:

- **Reported and observed trends and financial activity.** This includes reported revenue data for public companies.
- **IDC's software vendor interviews and surveys.** IDC interviews and/or surveys significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.
- **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area model on more than 1,000 worldwide vendors.
- **IDC demand-side research.** This includes interviews with business users of software solutions annually and provides a fifth perspective for assessing competitive performance and market dynamics. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in IDC's software studies and pivot tables represents our best estimates based on the previously mentioned data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps.

Note: All numbers in this document may not be exact due to rounding.

MARKET DEFINITION

Software-defined compute (SDC) workload security solutions protect software-defined compute solutions, which encompass a number of compute abstraction technologies that are implemented at various layers of the system software stack. SDC workload security solutions are not intended to protect the integrity of the SDC infrastructure (hypervisors, control plane/management, and orchestration) but to protect what runs on top of the SDC infrastructure (VMs and containers). SDC technologies are often used in the context of public or private clouds but can also be implemented in noncloud environments, particularly virtualized and/or containerized environments. Workload security solutions are designed to maintain the integrity of SDC servers, providing protection features that include antimalware, desktop firewall, host intrusion detection, application control, and integrity monitoring. These products accomplish their goals by ensuring the system does not run malicious software that can compromise business applications and data on the servers. Like the other endpoint security submarkets, software-defined compute workload security solution is a mutually exclusive category with no overlap with other categories such as physical server or antimalware and suites. Workload security solutions provide protection to three categories of SDC compute environments:

- Virtual machine software, also known today as hypervisor software, uses low-level capabilities offered by certain hardware environments or installs a complete hardware emulation layer using software to support multiple operating environments and the related stacks of applications, application development and deployment software, and system infrastructure software. This segmentation is often referred to as server virtualization or partitioning. Representative solutions include Citrix XenServer, IBM (PowerVM), Microsoft Hyper-V (included with Windows Server), Oracle VM for x86, Oracle VM for SPARC, Oracle Solaris Kernel Zones, and VMware vSphere.
- Containers are an operating system (OS) segmentation technology, similar in concept to hypervisors except they abstract an OS instead of server hardware. Containers rely on segmenting away parts of the operating system. Each application is presented with a pristine virtual copy of the OS, and the application is made to believe that it is the only application installed and running on that OS. An application and its immediate dependencies are packaged into a container file. Optionally, various OS user space tools and libraries may also be included. Representative solutions include Canonical (LXD), CoreOS rkt, CoreOS Tectonic, Docker CE, Docker EE (portions thereof), Microsoft Windows Containers (as part of Windows Server), Oracle Solaris Native Zones, VMware's Integrated Containers, Photon Platform, and Kubernetes open source container orchestration software.
- Cloud system software represents a tightly bundled combination of server abstraction and orchestration software and node-level controller software, often sold as part of a larger cloud infrastructure platform solution. The compute resource layer represents a combination of virtual machine, container engine, and/or operating system and orchestration software running on a physical server, which is designated as a cloud compute node. The controller software virtualizes groups of compute nodes into a single logical compute resource. Cloud system software also exposes APIs that simplify the scheduling and control of VMs, containers, and bare metal servers running on the node and maintains a database of resource state and policies.

RELATED RESEARCH

- *Internet Defense in PaaS and IaaS: DDoS and WAF Insights from IDC's Cloud Survey North America* (IDC #US45471919, September 2019)
- *Virtual Firewalls and Segmentation in PaaS and IaaS: Insights from IDC's Cloud Survey North America* (IDC #US45449719, August 2019)
- *IDC's Worldwide Software Taxonomy, 2018: Update* (IDC #US44835319, February 2019)
- *An Organization's IaaS/PaaS Workload Security Evolution: Insights from IDC's Cloud Survey North America* (IDC #US44591819, January 2019)
- *Market Analysis Perspective: Worldwide Managed Security Services Providers, 2018* (IDC #US44316818, September 2018)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com