Market Share

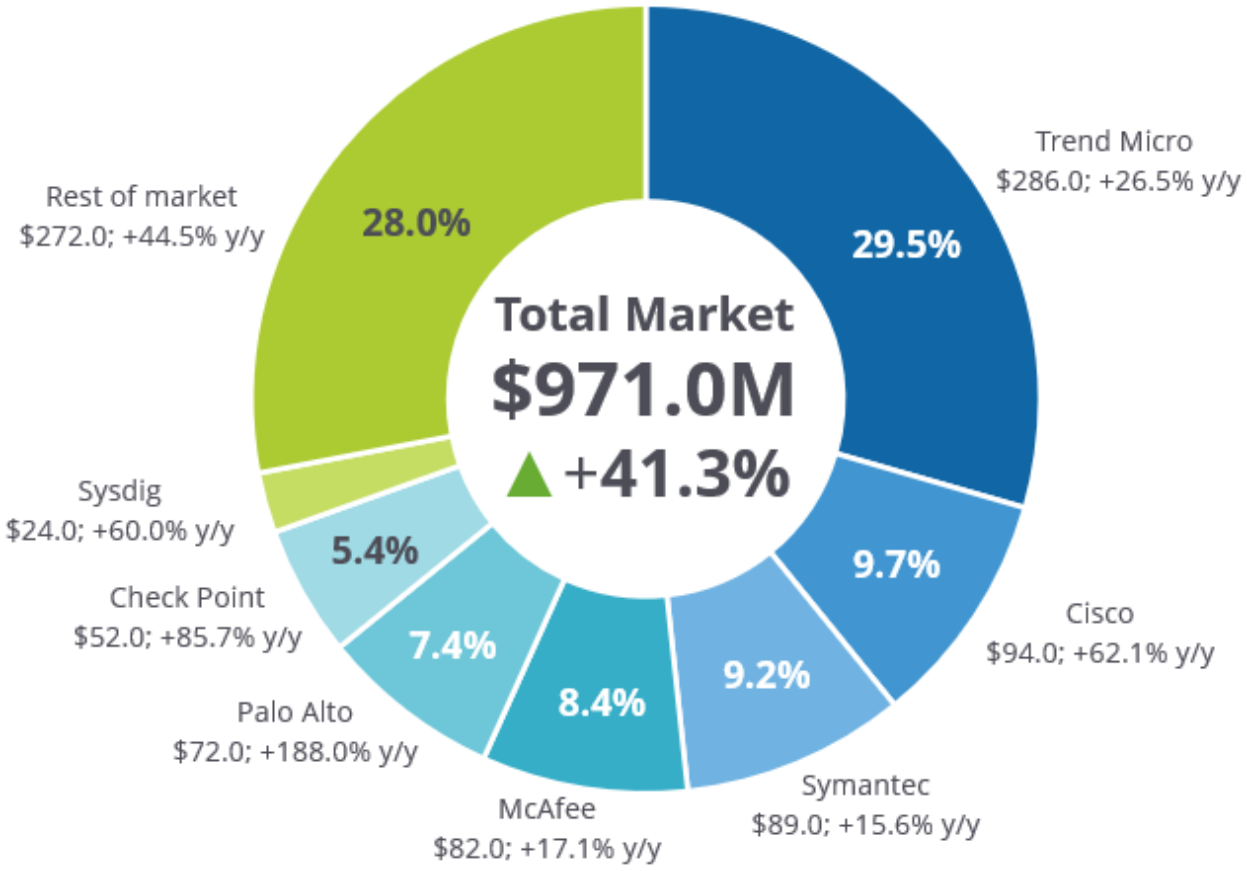
Worldwide Hybrid Cloud Workload Security Market Shares, 2019: Vendor Growth Comes in All Shapes and Sizes

Frank Dickson

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Hybrid Cloud Workload Security 2019 Share Snapshot



Note: 2019 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2020

June 2020, IDC #US46398420e

IN THIS EXCERPT

The content for this excerpt was taken directly from Worldwide Hybrid Cloud Workload Security Market Shares, 2019: Vendor Growth Comes in All Shapes and Sizes (Doc #US46398420). All or parts of the following sections are included in this excerpt: Executive Summary, Advice for Technology Suppliers, Market Share, Who Shaped the Year, and Market Context sections that relate specifically to Trend Micro, and any figures and or tables relevant to Trend Micro.

EXECUTIVE SUMMARY

Hybrid cloud workload security protects workloads in software-defined compute (SDC) environments, encompassing a number of compute abstraction technologies that are implemented at various layers of the system software stack. Hybrid cloud 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). Hybrid cloud workload security and firewall fabrics are components of an integrated set of offerings that span threat protection, vulnerability management, analytics, and data integrity for SDC environments.

Trend Micro is the dominant leader in SDC workload protection. The future of the market, though, has not yet been decided. Vendors such as VMware, Symantec, McAfee, Cisco, and Palo Alto Networks are making both organic and inorganic investments to grab share. Start-ups are strategically attacking newer cloud approaches such a Kubernetes, managed Kubernetes, and serverless. Although the new approaches are no more than "curiosity" of market share currently, the market will move there; "younger" start-ups such as Sysdig, Aqua, and Tigera will be waiting.

This IDC study presents the worldwide hybrid cloud workload security market shares for 2019.

"Hybrid cloud workload security solutions have evolved, providing more than malware detection, intrusion prevention, and vulnerability assessments. Although the kill chain is a wonderful threat assessment analysis framework, the human element is often the weak link. Software configuration assessments have become a differentiator for the leading providers." — Frank Dickson, program vice president, Security and Trust at IDC

ADVICE FOR TECHNOLOGY SUPPLIERS

Based on the results from an IDC survey on cloud security, conducted in late 2019, user preference for security solutions designed explicitly for cloud use is stronger than porting existing on-premises security solutions into cloud environments. Over 50% of survey respondents indicated that they chose security solutions designed for cloud usage when their organizations originally deployed workloads in the cloud. For organizations that subsequently changed their solution choice, again, over 50% chose security designed for the cloud solutions.

Before providing advice, defining the market is important. We now refer to "hybrid cloud workload security" as "software-defined compute workload security." Why did we change the name? To be perfectly blunt, the old name was terrible. And although SDC workload security is incredibly accurate, it required time to explain and it sounded terrible in the press release. The "market" liked the hybrid cloud name, and IDC acquiesced to the will of the market.

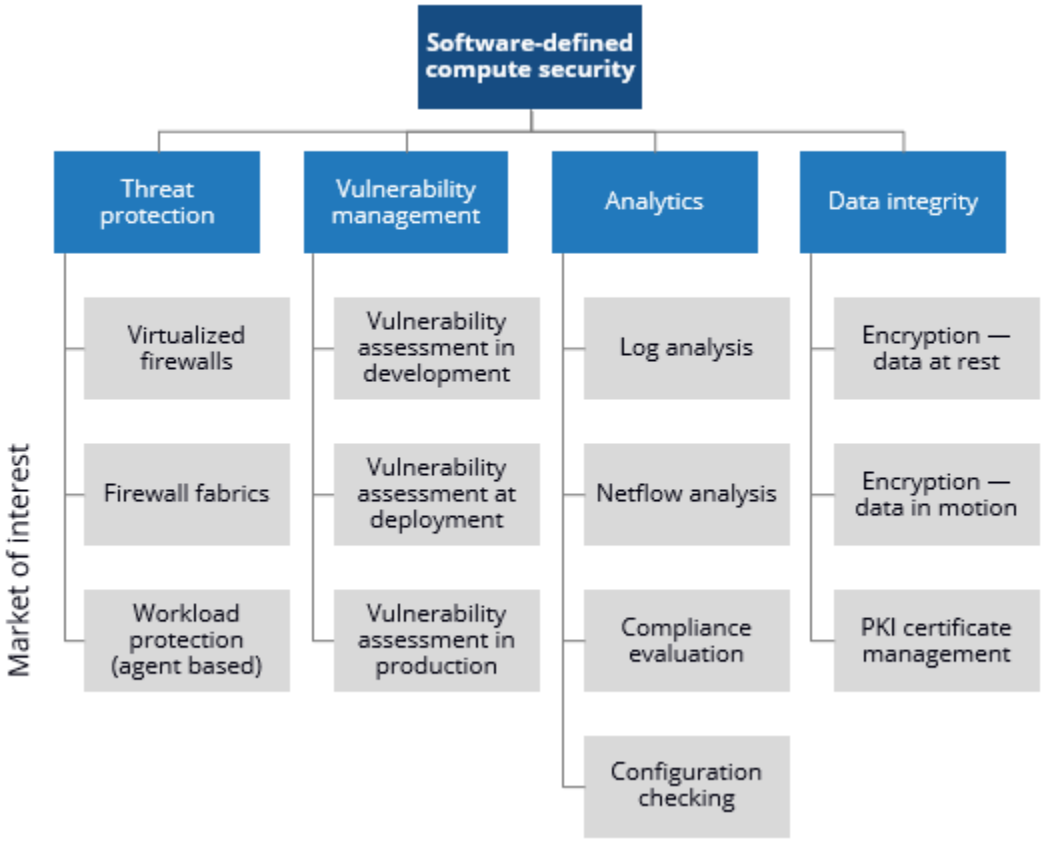
The goal of this study is not to provide market shares for all of SDC security or even just "cloud" security. This document provides market shares for two "cloud" security categories: workload security and firewall fabrics. The details of these categories are explained in the sections that follow.

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 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 that the system does not run malicious software that can compromise business applications and data on the servers. As with other endpoint security submarkets, SDC 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 SDC 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 (see Figure 2).

FIGURE 2

IDC's Cloud Security Framework



Source: IDC, 2020

Threat protection is accomplished by three primary approaches:

- **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 cloud (e.g., AWS Azure, KVM, and VMware). A virtualized firewall inspects packets and uses security policy rules to block unapproved communication into and out of a SDC environment or between VMs. Virtualized firewalls are excluded from the scope of this study.
- **Firewall fabrics,** under the strictest of definitions, could be included as part of virtualized firewalls. Firewall fabrics implement a mesh of firewalls around virtual machines or containers, controlling access to the VM or container based on IP, protocol, and/or instruction. Firewall fabrics typically implement security from outside of the VM or container (as they are not agent-centric protection) and often employ analytics to discover connections between the protected and the resources outside of the VM or container. Firewall fabrics are included in the scope of this study.

- **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 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 (HIPS), and application control. Firewall fabrics are included in the scope of this study.

MARKET SHARE

Trend Micro has become the dominant leader in hybrid cloud workload security, as it is literally three times the size of the number 2 player in the market (see Table 1).

The future of the market though has not yet been decided. An unusual mix of high-growth companies exist, looking to make inroads on Trend Micro's dominance. Sysdig and Aqua Security make a lot of sense because they are addressing a hot Kubernetes segment, and growth is easier for small, nimble, venture-backed start-ups. Palo Alto is showing strong growth – the product of acquisitions. Cisco is a bit atypical, driving organic revenue from a product suite that was originally targeting datacenters. And don't forget VMware. VMware clearly has aspirations in the market, as the acquisition of Carbon Black points to an increasing presence in the segment.

TABLE 1

Worldwide Hybrid Cloud Workload Security Revenue by Vendor, 2018 and 2019

	2018		2019		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2018–2019 Growth (%)
Trend Micro	226	32.9	286	29.5	26.5
Cisco	58	8.4	94	9.7	62.1
Symantec	77	11.2	89	9.2	15.6
McAfee	70	10.2	82	8.4	17.1
Palo Alto	25	3.6	72	7.4	188.0
Other	231	33.7	348	35.8	721
Total	687	100	971	100	41.3

Source: IDC, 2020

WHO SHAPED THE YEAR

Trend Micro

Trend Micro is the "800-pound gorilla" in this space, and its market leadership is not an accident. In 2009, Trend Micro bought Third Brigade, a provider of host-based intrusion-prevention and firewall software. Trend Micro 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.

Trend Micro has not rested on its position but rather continues to invest. Trend Micro acquired Immunio in November 2017, and it's being integrated into the Trend Micro portfolio. Immunio brings 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 (including web and serverless applications), there is no slowdown to the development and release cycles.

In 2019, Trend Micro acquired Cloud Conformity, a cloud security posture management provider. Increasingly, the threat to cloud instances is less about vulnerabilities and more about configuration errors. Cloud Conformity, an AWS Technology Partner of the Year for 2019, augments Trend Micro's offering with cloud infrastructure misconfiguration protection.

Trend Micro entered into a strategic partnership with Snyk, which looks to help organizations provide security for open source software. The partnership looks to address the challenge that open source vulnerabilities create for developers, stemming from code-reuse, public repositories, and open source.

At the end of 2019, Trend Micro launched Cloud One, its integrated cloud security services (SaaS) platform that addresses customers' security challenges around datacenter servers and virtual machines, IaaS workloads, containers and containers services, cloud security posture management, cloud file and object storage services, and serverless.

Last, Trend Micro strengthened its offerings for non-AWS environments, announcing enhancements to its Deep Security product designed to extend protection to virtual machines on the Google Cloud Platform (GCP), Kubernetes platform protection, and container image scanning integration with the Google Kubernetes Engine (GKE). Trend Micro created a GCP Connector that enables automated discovery, visibility, and protection of GCP virtual machine instances. It should also be noted that Trend Micro was honored as the 2019 Google Cloud Technology Partner of the Year for Security.

MARKET CONTEXT

The cloud providers continue their rapid innovation pace. For example, AWS re:Invent was held December 2-6, 2019, in Las Vegas. AWS launched a potpourri of new features and services. The most significant of which are:

- Graviton2 — a more powerful ARM-based processor
- AWS Wavelength — 5G cloud computing and storage services that minimized the latency associated with mobile networks
- AWS Local Zones — a new type of AWS infrastructure deployment that places compute, storage, database, and other select services close to customers, which is essentially a creative implementation of Outpost

- Amazon Fraud Detector — a managed service that identifies fraudulent online activities such as online payment fraud and the creation of fake accounts
- Contact Lens for Amazon Connect — a contact center service that can recognize people's emotions on phone calls

Rolled out in 2018, Oracle's Generation 2 cloud was designed to run traditional on-premises enterprise software in addition to net-new cloud-native applications. One key point is that no customer code and data are ever commingled with cloud control code on the same computer. With this approach, Oracle can't see customer data, and users can't access the cloud control code. This is part of OCI's security-first design and effectively eliminates the need for transparency or the ability of clients to understand what the cloud provider might be doing with their private information. Customers can also choose to run applications on dedicated virtual machine (bare metal) hosts, ensuring that no VMs from any other tenancy (customer) will run on that host.

Oracle further announced intentions to offer a category of services it calls Maximum Security Zones early in 2020. A Maximum Security Zone is a dedicated deployment environment that ensures that any resources running in it will run on the highest level of isolation and will meet best practices for security. This will help customers avoid configurational mistakes and associated vulnerabilities to attack. IDC notes that this is the first vendor to change what is called the shared responsibility model where cloud providers secure the hardware and software of the cloud itself, while the customer is responsible for the security of their assets within the cloud. Maximum Security Zones seem to fit the model of an autonomous enterprise.

Another key design point and a big reason for OCI's high-performance capabilities entails implementing "off box" network virtualization. The innovation here is isolating network and IO controls from the server instance, reducing performance impact and enforcing a zero-trust model that allows cloud administrators to manage infrastructure without access to customer data or configuration. Dedicated hardware is performing all the networking tasks, allowing the application hypervisor to focus on the workloads. Several vendors have shared the performance gains they've seen moving to OCI. Cisco Tetration previously moved from AWS to OCI and saw a 60x performance increase. McAfee chose OCI to host its McAfee SIEM cloud service, measuring 16x the rate of ingested events compared with an on-premises deployment.

Oracle is aggressively investing to build out its physical infrastructure and aims to match other vendors in the number of cloud regions available around the world by the end of 2020. The target is to have 36 operational regions where each region has multiple failover domains. Back in 2017, the company had three (U.S. East, U.S. West, and Europe West). IDC understands that vendor philosophies differ. OCI capabilities will not directly match AWS, in terms of the construction of networks, buildings, datacenters, servers, and so forth, but it will likely offer enough security technology to address the needs of a substantial market segment dominated by PaaS deployments of Oracle Cloud Applications.

Significant Market Developments

AWS

In *IDC FutureScape: Worldwide Security and Trust 2020 Predictions* (IDC #US45582219, October 2019), IDC predicted that "innovation, opportunity, and market demand collide to place hyperscale cloud providers directly and permanently in the security business; by 2025, 9% of their revenue will be attributed to security." IDC's experience at AWS re:Invent reaffirms our belief in the prediction.

New offerings were plentiful and value added. Amazon Detective, AWS' first productization of the Sqrrl IP, offers strong threat hunting and incident response tools for AWS accounts. Certainly, the trajectory of the offering will continue to be positive as it continues to be enriched.

Amazon Detective (Sqrrl)

In late 2017, AWS announced Amazon GuardDuty, a fully managed intelligent threat detection service that helps customers protect their AWS accounts and workloads by continuously monitoring account activity for malicious or unauthorized behavior. With 25 new finding types added since the launch, Amazon GuardDuty now includes 54 definitions of suspicious or unexpected behaviors it automatically detects.

Amazon Detective essentially picks up where Amazon GuardDuty leaves off. Based on the intellectual property gained from the acquisition of Sqrrl in 2017, Amazon Detective provides tools to investigate threats and issues with AWS accounts. It helps security teams deeply investigate single instance findings by providing a time-based analysis of user and resource activities presented in a visual behavior graph model.

Amazon Detective leverages three sources of data collection:

- Virtual private cloud (VPC) flow logs
- AWS CloudTrail
- Amazon GuardDuty Findings (which admittedly are derived from VPC flow logs and AWS Cloud Trail)

AWS is addressing the challenges associated with threat detection in the cloud, including the low signal-to-noise ratio, complexity of the environments, lack of experienced talent, and cost to deploy and maintain a sophisticated threat detection platform. Amazon Detective creates a time-services graph of resource behavior, including up to a year's worth of environmental data, enriched with analytical summaries and user or resource activity baselines. To aid navigation, SoC analysts can move directly from Amazon GuardDuty to Amazon Detective, preventing console pivoting.

There are three primary uses cases to be addressed:

- **Finding/alert triage –** Accelerate triage, and avoid unnecessary escalations.
- **Incident investigation –** Improve context- and surface-correlated behavior.
- **Threat hunting –** Simplify data collection, aggregation, and pivoting.

AWS sets Amazon Detective pricing to maximize solution adoption. The goal for the 50th percentile customer is $1/GB of log data ingested per month while maintaining historical access for a year. The AWS quote is to "make it a no brainer to turn it on and keep it on across all accounts and regions." There will be a 30-day free trial for all, per account/region, with automatic backfill of processing for two weeks of data for immediate value. Final pricing will likely be tiered based on the amount (in gigabytes) ingested per account/region/month:

- First 1,000GB/month, $2.00 per GB
- Next 4,000GB/month, $1.00 per GB
- Next 5,000GB/month, $0.50 per GB
- Over 10,000GB/month, $0.25 per GB

Amazon Detective had 15 development customers running private beta trials since June 2019. A broader, general preview was announced and made available December 3, 2019, and general availability is projected for 1Q20. Several partner integrations are projected to be available at launch, including threat detection platforms, SIEM, and managed services.

Areas for future investment include expanding availability into all regions and supporting additional data sources. DNS information seems to be the most obvious (so obvious that it is surprising that DNS information is not included at launch), followed by S3 bucket data – especially given the richness of the AWS IAM offering. IDC believes that AWS CloudTrail data events (data plane operations) are another likely data source to be supported.

IAM Access Analyzer

As we look at the IaaS shared responsibility model (of the cloud versus in the cloud), providers such as AWS are realizing that the real challenge of the model involves the responsibility of the customer. In 2018, AWS launched a feature that looked at which S3 buckets were open to the internet and notified administrators. In theory, such a service should not have been necessary, as S3 buckets are closed by default. A person with administrative access must consciously expose the bucket contents to the internet; yet the problem existed.

AWS IAM Access Analyzer is essentially the next generation of the S3 bucket inspection feature. AWS IAM Access Analyzer lives between the use-case extremes of one resource being totally open to the internet and the other perfectly limited to an internal team dedicated to a specific project. Several methods exist to access an S3 bucket, and a number of individuals external to a project team, or even external to an organization, will have an infrequent need to review bucket contents (such as professional services support or compliance administrators). IAM Access Analyzer continuously reviews permissions granted for Amazon S3 buckets – as well as AWS KMS keys, AWS IAM roles, SQS queues, and AWS Lambda functions – in accordance with defined usage policies. The function looks to quickly analyze and transparently provide information for both security and compliance use cases. In addition, AWS IAM Access Analyzer provides automated reasoning, making it possible to provide comprehensive results about cross-account or external access.

Please note that IAM Access Analyzer is different from the previously introduced Amazon IAM Access Advisor, which provides insights such as information on service last accessed. Think of Access Advisor as a historical summarization of access information, a version of an IAM "flight data recorder," while Access Analyzer reports who could do what rather than who actually did what.

We would like to note that IAM Access Analyzer and IAM Access Advisor are not truly two different products – they are two different features available to customers in the IAM console. In addition, Access Analyzer results are visible in Security Hub. Access Analyzer results for S3 buckets are visible in the S3 console as well.

AWS Single Sign-On

AWS Single Sign-On (SSO) provides authorization and access based on identities that live within AWS SSO's identity store or easily connect to existing identity sources, including Microsoft Active Directory and Azure Active Directory (Azure AD). When thinking of the offering, it is best to divorce oneself of the definition that one may use in describing an offering from a company such as Ping Identity. Ping Identity single sign-on enables users to access all applications, whether hosted or on premises, with a single authentication event.

AWS Single Sign-On is different, as it serves a different use case. AWS Single Sign-On prioritizes access to resources and applications in AWS; however, it does also offer a catalog of integrations with third-party SaaS apps. AWS Single Sign-On leverages identities in Azure AD, eliminating the need for another identity store, as Azure AD identities are synchronized into AWS IAM. As a result, fine-grained access to AWS resources is provisioned based on a single authentication event from Azure AD. In addition, Azure AD maintains a single source of truth for compliance reporting.

CloudTrail Insights

On November 21, 2019, AWS announced CloudTrail Insights, a feature that identifies unusual operational activity in AWS accounts such as spikes in resource provisioning, bursts of AWS identity and access management actions, or gaps in periodic maintenance activity. Essentially, the feature is anomaly detection, analyzing AWS CloudTrail events to establish a baseline for normal behavior and then raise issues by generating CloudTrail Insights events when it detects unusual patterns. Abnormal activity is delivered as an event through dashboard views in the AWS CloudTrail console. The events can also be sent to Amazon CloudWatch Logs, allowing for integration with existing event management and workflow systems.

CloudTrail Insights is not necessarily a security tool, as events may not necessarily be malicious. The unusual activity identified includes:

- Unexpected spikes in resources provisioned
- Burst of IAM management actions
- Gaps in periodic maintenance activity

Other Features of Note

A number of other noteworthy services were previously or recently launched that IDC views as relevant for security:

- **Amazon CodeGuru,** an automated developer tool, reviews source code — so that it runs efficiently, represents good hygiene, and adheres to AWS best practices — while giving specific recommendations to fix or improve code. The service will work with code storage service GitHub.
- **AWS Nitro Enclaves** creates isolated compute environments to protect and securely process highly sensitive data. It uses the same Nitro Hypervisor technology that provides CPU and memory isolation for EC2 instances. A preview for AWS Nitro Enclaves is expected to begin in 2020.
- **Amazon S3 Access Points** provides highly granular, least privileged access to data within an S3 bucket. Access points are unique hostnames that customers create to enforce distinct permissions and network controls for any request made through the access point. Customers with shared data sets, including data lakes, media archives, and user-generated content, can scale access for applications by creating individualized access points with names and permissions customized for each application.
- **Access Analyzer for Amazon S3** is a feature that monitors access policies, ensuring that the policies provide only the intended access to S3 resources. It also evaluates bucket access policies and enables discovery and remediation of buckets with potentially unintended access.
- **AWS Key Management Service (KMS)** supports asymmetric cryptography.
- **Post-quantum TLS** is now supported in AWS KMS.

Google

GCP and Chronicle

Chronicle, the cybersecurity venture formed within Alphabet's X subsidiary, joined Google Cloud to provide nearly unlimited and instantaneous capabilities to discover malware infections occurring anywhere — in the cloud or on premises — and to help Google Cloud Platform clients discover any present and past exposures. Chronicle was officially launched at RSA 2018 but had been operating for years as a "moonshot factory" project leveraging the compute and storage capabilities of Google infrastructure and the antivirus/malware megadatabase VirusTotal, which was acquired by Alphabet in 2012. The combination of GCP and Chronicle simplifies cybersecurity threat detection and monotonous forensics research processes to provide faster time-to-consumable insights for enterprise security organizations.

The combination of these two Alphabet subsidiaries provides GCP customers with a single source for a broadening array of security technologies and Chronicle with a ready route to market. Chronicle rolled out Backstory as its second new revenue-producing offering at RSA 2019, adding to its free and paid VirusTotal solutions and Uppercase services. The decision to combine the two organizations was driven by a realization that both product's long-term trajectories would eventually lead to development overlap, and it is better to join forces now than try to reconcile future technology differences.

What Chronicle brings to the table is a simplified approach to writing investigation flows and tooling. Backstory continuously reevaluates years of security telemetry data — but not packets — including DNS resolutions, DHCP, endpoint detection and response (EDR), and NetFlows at petabyte scale for every subscriber. The investment in specific and expensive security team training is minimized as there are no cryptic query languages to learn and develop into custom capabilities — expertise that might walk out the door when someone gets a better job offer.

What GCP brings to the table, something Chronicle has leveraged through Google's infrastructure since inception, is subsecond latency (250ms for any query) searching through years of data that most on-premises resources would struggle to plan, acquire, and maintain for more than 90 days. It also provides the affordable long-term storage capabilities with a pricing model based on the number of users rather than total capacity, making it easy to predict and budget future costs.

As a bonus, VirusTotal is Chronicle's malware database (corpus), acquired from a Spanish organization in 2012 that aggregates information from 70 different virus scanners to present 2 billion current malware samples growing by about 2 million new observations every day. Chronicle employees collect these instances and observe their operations in a sandbox environment, feeding any resulting observations into Backstory as new indicators of compromise (IoCs). Any change in URL status — safe versus compromised — would automatically trigger a new evaluation of any host or endpoint that's ever communicated with the newly defined rogue resource.

The security story for GCP continues to grow stronger. At Next '19, Google Cloud moved multiple offerings (Security Command Center, VPC Service Controls, and Access Transparency) to a generally available status after lengthy alpha and beta program releases. Absent among these were technologies to perform threat hunting and forensic investigations, and now the Chronicle offerings fill that gap.

A key focus, cited by new CEO Thomas Kurian, is investing in a broader field and go-to-market reach to grow Google Cloud into a larger cloud service provider. The new combination helps Chronicle avoid

the challenges of building out its own sales force as well as the struggle to expand into international markets, as most of its pipeline was built from domestic opportunities. GCP exists across the globe, bringing immediate visibility to the unique capabilities of the Chronicle offerings.

Other synergies will no doubt emerge, based on the partner ecosystem that GCP has built with complementary technology suppliers that have recognized the value of building out new capabilities on the platform. Instantaneous search and perpetual telemetry data storage could help partners better understand how to enhance their offerings to address what still exists as an asymmetric battle against the cybersecurity defenders.

GCP and Palo Alto Networks

Palo Alto Networks announced the availability of Cortex XSOAR, another platform that is symbolic of what is possible with cybersecurity vendors that have broad product portfolios. Palo Alto Networks successfully articulated the concept of a platform fabric connecting together network insights, endpoint insights, threat intelligence, and orchestration and automation. The XSOAR announcement was centered on the ability for customers to integrate external threat intelligence into Palo Alto Networks' existing Cortex platform to uncover additional threats and work the new telemetry into a workflow.

The integration of XSOAR with Google Chronicle adds another dimension to the platform trend: cross-platform integration. It is conceptually promising, not only in terms of the value that security teams could gain but also in the integration of products from multiple vendors. Integration can work but not as well as the integration of products from a single vendor (i.e., the single platform approach). Nevertheless, cross-platform integration is moving forward.

GCP and Tanium

GCP cross-platform integration is not limited to Palo Alto Networks. Last year, an integration with Tanium was announced. Tanium's platform provides a unifying view of endpoints, containers, and cloud architectures, and it powers scalable remediation. GCP adds cloud-scale security analytics fed by telemetry from Tanium-supported IT environments and customer log sources (e.g., firewall, netflow, and proxy) to speed the detection and investigation of security incidents. As incident verdicts are reached, Tanium-powered remediation cycles back in. For Tanium, cross-platform integration with GCP immediately augments Tanium's threat detection and response capabilities without requiring Tanium to develop the security analytics means, which would likely be a multiyear endeavor. In addition, GCP's per-user pricing, rather than volume of ingested data, and lengthy data storage period may also prove to be disruptively economical for joint Google-Tanium customers, relative to other security analytics systems.

Microsoft

Support for Any Device, Cloud, or Application

The strongest security theme at Microsoft Ignite was support for any device, cloud, or application, whether it comes from Microsoft or a competitor. Cloud analytics looks to support AWS, GCP, or other competitive clouds in the same manner in which Microsoft supports the Azure Cloud. Microsoft seems to be embracing the reality of a multicloud/multivendor future. In addition, security support for devices of other OS types such iOS, Mac, and Linux continues. For example, EDR support for Mac was announced at Ignite. Full support for Linux (endpoint protection platform and EDR) is coming soon. The recent rebranding of Windows Defender to Microsoft Defender is illustrative of the change in focus.

Security Built In

The theme of "built in instead of bolted on" has been a theme in security for quite a while. The theme has elevated within the security industry overall as many of the big security acquisitions of late have been by non-security companies. Ignoring the private equity acquisitions, Broadcom-Symantec, VMware-Carbon Black, and BlackBerry-Cylance are indicative of the trend. Microsoft has been on the path for some time.

The built-in approach was a consistent theme at Ignite. Microsoft announced new capabilities to find misconfigurations and threats for containers and SQL in IaaS while providing vulnerability assessment for virtual machines. Azure Security Center also provides integration with security alerts from partners and fixes for remediation. For example, Qualys was announced as a partner for vulnerability assessments.

Integrations

One might argue that integration is a subtopic of the built-in theme. "Integration" is a term that we throw around in security in a rather cavalier fashion. However, anyone that has tried to actually implement SAML or "integrate" applications using a poorly designed API knows that all integrations are not created equal. Three months of professional services with unstable results do not make a plug-and-play.

Microsoft had plug-and-play integrations on display. For example, Azure Sentinel is getting new connectors to help security analysts collect data from a variety of sources, including Zscaler, Barracuda, and Citrix, along with new hunting queries and machine learning-based detections to assist analysts in prioritizing important events.

Integration was also on display as Microsoft builds its Microsoft Threat Protection suite, essentially its xDR story. It is introducing new layers of cross-product knowledge and capabilities and providing coordinated protection. Microsoft 365 Security Center covers four traditionally siloed environments: identity (Azure Active Directory, Azure ATP, and Microsoft Cloud App Security), endpoint (Microsoft Defender ATP), email and collaboration (Office 365 ATP), and applications (Microsoft Cloud App Security). Microsoft 365 Security Center does not have a separate fee. If you purchase the components, "you just get it."

Essentially, the goal of Microsoft 365 Security Center is to orchestrate incident management, investigations, threat hunting, and threat analysts across products, providing automated protection and remediation playbooks. Note that Microsoft 365 Security Center is a fully integrated Microsoft-only portal; integrations with other security providers would need surface through Azure Sentinel.

Share Responsibility Model

A clear change in the approach to the Shared Responsibility Model was consistent in many presentations at Ignite. The common approach to the model in the industry has historically been to delineate what is the responsibility of the cloud provider (IaaS) and what is the responsibility of the tenant. It is congruent with Walt Whitman's quote: "Good fences make good neighbors."

Microsoft's approach acknowledges that the issue in cloud security is the user side of the shared responsibility model, and it's aggressively looking to provide tools to help harden the environment and facilitate security measure deployment. Essentially, users need help. To quote a Microsoft executive, "Security measures should be auto-provisioned and enabled by a checkbox, or it is not getting deployed."

Protection at the Data Layer

Microsoft had two big announcements surrounding data security: First, insider risk management in Microsoft 365 identifies and remediates threats by leveraging the Microsoft Graph and integrating third-party signals, such as HR systems, to identify hidden patterns indicative of malicious or careless insiders. Second, Microsoft's information protection and governance provide the ability to view data classifications categorized by sensitive information types or associated with industry regulations. Machine learning uses existing data such as customer records, HR data, and contracts to train classifiers.

IBM

IBM introduced new hybrid, multicloud, security capabilities — the likes of which a few other companies have the resources and perspective to develop. IBM wants to establish and standardize a new security data format that's capable of allowing packets, logs, and plain old files to all be searched in one place as part of one mono cybersecurity query — bully. The fundamental value proposition offered here is the reduction in operational complexity driven by data incompatibilities and silos, but the interesting twist is the ability to search without moving any of the underlying data in the process.

Will it work? Yes, most likely. IBM is pretty good at these codeveloped efforts laying the commercial foundation (contributed code) for a proposed industry standard. This one is an OASIS-contributed JSON format searchable with the technology named STIX-Shifter. IBM Cloud Pak for Security uses the structured threat information expression (STIX) patterning technology to simultaneously align all three fundamental security data source types (network, file, and log), allowing security teams to create complex queries and analytics that span both cloud and on-premises domains.

It's a pretty neat trick, but how many security teams really need it? It stands to reason that there will be some discoverable patterns in the past activities, but IDC believes that IBM Cloud Pak usage will be somewhat limited to mature security programs in highly regulated environments. Those are the prospects that can further justify new threat-hunting tools. That said, establishing an OASIS standard for security data interchange is a very good thing, so kudos to IBM and other STIX-Shifter adapter developers in the Open Cybersecurity Alliance (OCA). The day will likely come when security products store data identically, and that will be a big win for all those SoC analysts and forensics researchers.

IBM is contributing a cybersecurity defense technology in the form of a new data hunter. This tool is designed to help people protect themselves from really cryptic and hidden stuff. IBM Cloud Pak for Security allows security teams to build research cases using a common query tool to investigate all available data.

VMware

On August 22, 2019, VMware announced its intention to acquire endpoint security company Carbon Black for $2.1 billion. VMware also announced its acquisition of the app development vendor Pivotal Software for $2.7 billion. Both acquisitions are expected to close during VMware's FY 2H20, from August 1, 2019, to January 31, 2020. While Pivotal Software is a logical addition to VMware's business, nurtured and raised within the Dell EMC family, the Carbon Black acquisition is more of a surprise. With this surprise, questions arise regarding what impact this acquisition will have on the balance of power in endpoint protection and in the overall security market and how VMware's platform will change for its partners and clients.

The Carbon Black acquisition is VMware's latest, and not expected to be the last, step in lifting and shifting enterprises from today's operationally complex sprawl of security point products, vendors, and

administrative consoles to VMware's vision of intrinsic security. Emerging from a product partnership between CB Defense and VMware AppDefense for more than two years, Carbon Black will join the growing VMware portfolio of security products and platforms. It includes the previously noted AppDefense (a datacenter workload security product), Workspace ONE (a unified endpoint management [UEM] platform), NSX (a networking and security virtualization platform), and Secure State (a multicloud security product). This move also has the potential to exert additional force on industry consolidation and convergence in endpoint device management and security, both as a function within IT organizations and from a unified product toolset and centralized intelligence platform.

Taking a historical view on VMware's acquisition strategy, IDC sees consistency in its action plan. Since 2014, the company has acquired mobility, application management, and network optimization vendors to optimize the application delivery and monitoring. Interestingly, SD-WAN from VeloCloud Networks is now part of the network and security product family at VMware.

In the first thread of 2018 acquisitions, VMware acquired Kubernetes ecosystem builder Heptio, the mobility and workload transferability group at CloudVelox, and the service assurance team from Dell. All three are aimed at application developer-orientated offerings. For VMware, this was part of a strategic move to ensure usability and attractiveness of its platform across industries in transformational projects.

The second thread of 2018 acquisitions began in the spring when VMware acquired three security management companies focused on applications, cloud, and data management/protection: CloudCoreo, E8 Security, and Bracket Computing. This was VMware's first stab in enhancing the security capabilities of its VM platform in a nonorganic fashion.

2019 was a year of acquisition sprees for VMware, with a total of nine companies acquired or announced to be acquired through August:

- For developers: Pivotal and Bitnami
- For NetOps, infrastructure, and delivery teams: AetherPal, Avi Networks, Bitfusion.io, and Uhana
- For security and SecOps teams: Veriflow for network security and predictive analytics, Intrinsic for application security, and Carbon Black for mobility, cloud, and endpoint protection

With these acquisitions, VMware is strengthening its position to:

- Build flexible infrastructure capable of ingesting and managing workloads from anywhere.
- Ensure that development and delivery teams can continue to use their existing tooling.
- Secure application development and data.
- Orchestrate delivery and service mechanisms for large-scale rollouts.
- Build protection into runtime.

Although absent of VMware's organic research and development, in IDC's opinion, this is a good baseline for the main catalysts of VMware's acquisition of Carbon Black, which are as follows:

- VMware saw sales of CB Defense through its platform and realized benefits further emphasized by the use case of Carbon Black plus Workspace ONE. It was VMware COO Sanjay Poonen who pointed out that many Workspace ONE customers are also Carbon Black customers.
- Increasing market demand for in-built "by design" security, especially for virtualization and platform offerings, was one of left few strategic options for VMware. Its choice was not organic.

- VMware was busy building its DevOps offering and mobility capabilities, while Carbon Black brings a logical finishing part of the complete platform that is productive and secure.

As mentioned previously, VMware and Carbon Black have been codeveloping the AppDefense layer into a datacenter offering. Carbon Black is complementary, protecting the application layer above the kernel and virtualized back end. Given that the normal infrastructure runs VM instances for isolation and container clusters for productivity and flexibility, Carbon Black with VMware AppDefense formed an end-to-end virtualization protection layer with a potentially lower footprint than any nonnative option in the market. VMware CEO Patrick Gelsinger highlighted that VMware's goal is to collapse the sprawling numbers of agents/use cases into one underlying agent on the client side as part of the outlook for solutions integration.

Regarding the immediate market opportunities with the acquisition of Carbon Black, VMware called out the single-vendor approach to endpoint management (Workspace ONE) and endpoint security (Carbon Black). In addition to continuing the integration with AppDefense, other cross-product integrations are in the planning stages, such as embedding Carbon Black's cloud-native security analytics capabilities (i.e., the Predictive Security Cloud [PSC] platform) into NSX in support of advanced network threat analytics. With the Carbon Black acquisition as a step in its intrinsic security vision, additional product expansions are planned. Outlined during the VMworld keynote presentation (on August 26, 2019), product expansions include antivirus, device control, rogue device detection, app defense, vulnerability management, auditing and remediation, compliance reporting, and managed detection.

A formidable and foundational element that VMware already has in place is its products that power virtualization and erect segmentation in datacenters, devices, and apps as well as the networking among them. With VMware virtualization in corporate datacenters, public clouds, end-user devices, and edge computing environments (e.g., the upcoming AWS Outposts), VMware establishes a unifying platform from which to holistically inject security monitoring and control. Moreover, as its virtualization technology and partnerships with hardware manufacturers have advanced, VMware gathers determinants of trust of host environments (e.g., secure boot), which are beneficial in making context-based access decisions (i.e., who can access what under which set of circumstances).

IDC views Carbon Black's cloud-native security analytics engine as a strong strategic fit to VMware. The benefits for VMware customers are twofold. The first is enhanced security monitoring as more is seen, particularly in endpoints where the Carbon Black's lightweight agent resides. The second is in augmenting VMware's response capabilities. Faced with an ever-changing IT landscape and applications, clarity on the parameters that define good/acceptable behaviors is elusive. With the combination of Carbon Black's endpoint visibility and PSC, VMware is positioned to provide its customers heightened identification capabilities into abnormal and malicious behaviors and their contributing factors and improved confidence in responding appropriately. Circling back to the VMware virtualization platform, it is a ready-to-use platform to apply responses (e.g., block and quarantine) automatically, consistently, and dynamically.

The comprehensive monitoring capabilities of Carbon Black as a cloud security platform also pair well with VMware's presence in enterprise mobility management (EMM) and unified endpoint management (or the merging of PC and smartphone configuration/management). And the combination of Carbon Black endpoint security and Workspace ONE UEM puts VMware in the rarefied ranks of vendors with both endpoint security and endpoint management tools. Microsoft is among these vendors, as is BlackBerry (from its 2019 acquisition of Cylance) and, to a lesser extent, Symantec with its Symantec Endpoint Protection and Symantec Endpoint Management products (formerly Altiris, which is a PC-only management solution without EMM capabilities). Beyond marrying endpoint management and

endpoint security, the integration of Workspace ONE and Carbon Black also has potential for increased endpoint security situational awareness and actionable risk scoring via the Workspace ONE Intelligence platform — a software add-on to the UEM suite. This add-on, available at the launch of Workspace ONE Intelligence, aggregates overall device health and risk data on all devices under management (from PC to mobile and some IoT endpoints). Carbon Black endpoint security and cloud threat intelligence capabilities help create a more comprehensive threat feedback/remediation loop throughout an entire VMware-based infrastructure.

Enterprises are clearly on a trajectory to unify and converge PC and mobile management. According to IDC's 2019 *Enterprise Workspace and Mobility Decision Maker Survey,* nearly three quarters of enterprises said that they expect a majority of their PCs and mobiles to be managed through a single UEM platform in the next five years. Less clear is the future for unified security management. While EMM/UEM covers some mobile/PC endpoint security functions, it is far short of full-featured endpoint security solution. Within many large enterprises, teams that manage PCs and phones are still largely separated. As such, integration of endpoint security and endpoint management is likely further off. However, the value of having an entire management/security infrastructure delivered by a single vendor — if not by a single pane of glass — will be appealing to enterprises overall.

An unproven aspect of Carbon Black PSC is its scalability and adaptability. Can it match the size and diversity of VMware's customer environments, and how quickly can it come up to speed? The product integration with VMware AppDefense and CB Defense and Carbon Black supporting deployments exceeding 350,000 endpoints likely gave VMware the answer that it could. Also, as a cloud-native adopter since its inception and its quick but pragmatic embrace of resource-conserving/development-efficient serverless functions, Carbon Black presented VMware with additional reassurances that PSC is a future-built foundation. Nevertheless, the post-acquisition period will provide a more definitive answer on how broadly and quickly VMware integrates PSC into its security fabric.

While VMware has set out an ambitious plan of new security products and capabilities for its intrinsic security vision, there are glaring insufficiencies relative to enterprise needs. In its current described form, VMware's intrinsic security provides visibility, control, and response of the virtualized infrastructure and around application boundaries. For example, security within the application, data protection and privacy, and identity and access management are only covered sparsely and/or indirectly. Pertaining to application security, VMware Secure State delivers security via detection and response, not security via prevention. As enterprises embrace DevSecOps practices, interoperability between Secure State and their DevSecOps tools would be a valuable addition. Runtime detections cycling back to secure software development is a complementary use case of interoperability. In IAM, VMware Identity Manager (now renamed Workspace ONE Access) is a start but is not a market leading solution. Allowing enterprises to seamlessly extend their existing IAM solutions into VMware's virtualized footprint is worthwhile. The same applies to data loss protection (DLP) and key management. Reuse of existing solutions is an option that enterprises expect.

The challenge ahead for VMware is in demonstrating to skeptical decision makers that the highly tangible business value is present with its intrinsic security vision. This challenge is not unique to VMware, as other companies espousing a platform approach face the same challenge. To VMware's credit, it has crossed this type of bridge before in convincing enterprises of the financial and strategic value of virtualization. In security, however, the yardsticks are not as quantifiable and static. The yardstick for measuring "better" security against an evolving mix of cyber adversaries is prone to subjectivity. Even so, other demonstrations may be possible, such as gains in operational efficiencies.

And perhaps, VMware's road map focus on auditing and compliance reporting will serve as a tangible means in demonstrating better security.

The potential synergies and market implications of this acquisition should not be underestimated. Secure virtualization, advanced security analytics, threat intelligence, runtime protection of applications across the VMware suite, and access to a broader install base of the Dell family will contribute to market turbulence. When Carbon Black technology is fully integrated into the VMware platform, space for third-party security providers to offer added value will shrink.

There's also the rare survey respondent that tells IDC it only engages with one cloud vendor for all required IT services — those who do work for born-in-the-cloud businesses that never made a significant investment in legacy IT systems including Microsoft Windows–based solutions. The rest of us make do with what we have, and the value of a cross-platform and cross-cloud data searching tool grows proportionally with the number of providers engaged. Managed security service providers should especially appreciate these developments.

For IBM, this is a smart play but may not be the biggest near-term revenue producer. A new security-oriented universal data storage format (STIX 2) will take years to become absorbed by a majority of vendors, but it's an evolution that needs to happen. Five years from now, spending on these search tool and data integration projects could dramatically increase if they can crush or thwart a new popular attack technique.

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, and 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:

- **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's demand-side research.** This includes annual interviews with business users of software solutions 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 the 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

Hybrid cloud workload security solutions protect software-defined compute (SDC) 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 (virtual machines [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 that 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 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 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

- *AWS re:Invent 2019 - Extending the Erector Set for Cloud Security* (IDC #IcUS45740719, December 2019)
- *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