IDC MarketScape

IDC MarketScape: Worldwide Cloud Security Gateways 2017 Vendor Assessment

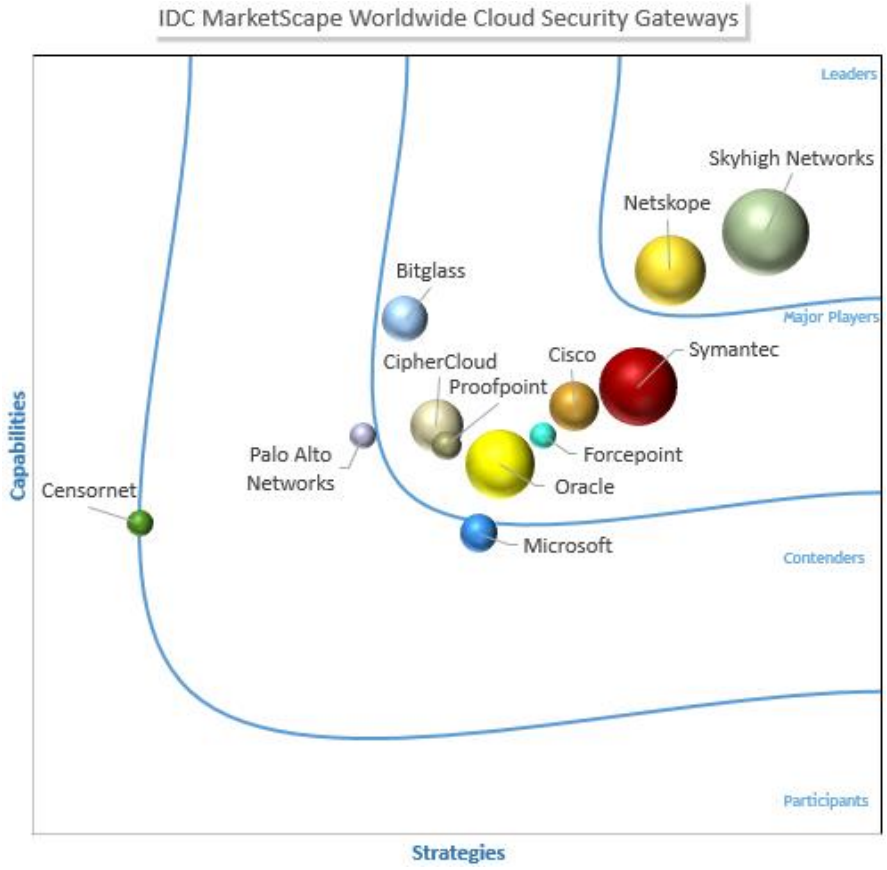
Pete Lindstrom
Tom Austin
Konstantin Rychkov

THIS IDC MARKETSCAPE EXCERPT FEATURES: FORCEPOINT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cloud Security Gateways Vendor Assessment



Source: IDC, 2017

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Cloud Security Gateways 2017 Vendor Assessment (Doc #US43093817). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The cloud is revolutionizing IT architectures and management. People (or more importantly, organizations) have clearly identified the cloud's great benefits — dynamic payloads on the technical side and flexible economic models on the business side — resulting in increased efficiency and effectiveness in the use of cloud technology. And there is no end in sight to the adoption of the new architectures.

But the value of the cloud isn't without its risks. The new architectures require a new look at security requirements. As enterprises lose control over the different architectural components of the cloud, more uncertainty is introduced into the environment. Organizations must rethink their security programs.

Cloud security gateways (CSGs), also known as cloud access security brokers (CASBs), are rapidly evolving to cloud security platforms in concert with the adoption of public SaaS solutions, most notably Office 365 and Google's suite of apps, as well as salesforce.com, Dropbox, and Box.com. CSG architectures now include both inline proxy-style options for applying policies to users interacting with apps and API connectors that can identify and protect leaks occurring in near real time as well as cloud-to-cloud activities. Given the robustness of CSG solutions and opportunities associated with aggregating data across multiple apps, CSGs are a fundamental requirement for any organization that leverages multiple public SaaS solutions.

Requirement notwithstanding, CSGs are not simply plug and play, and a few key decision points must be considered:

- What functional requirements such as data loss protection, user behavior analysis, and malicious threat detection are the most important to your cloud security program?
- Should an organization look for a CSG that complements and integrates with its existing security solutions or consider a pure-play solution focused on the cloud security challenges?
- Which architectural elements — proxy gateways, API connectors, and client agents — should be deployed, and should they be hosted on-premises or in the cloud?
- Should an organization incorporate encryption capabilities for structured and unstructured data into its CSG?
- How can organizations integrate with and rationalize existing security solutions within their security programs?

This IDC MarketScape identifies the strengths and challenges of the key players in the CSG product category. It provides insight into each solution's ability to perform the various functions described in the sections that follow as well as others that have been included by solution providers as differentiators.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

A cloud security gateway (CSG) leverages the functionality of traditional security controls and methods and applies them to the newer cloud architectures. CSGs have functions similar or analogous to a number of existing product categories, including next-gen firewalls (NGFW), secure web gateways, web app firewalls, and cloud encryption solutions. In addition, they provide key data loss protection and user behavior analysis capabilities for cloud environments.

CSGs operate either physically or logically inline between users and cloud applications, as well as between cloud-to-cloud communications. They monitor all of the activity during a session and apply dynamic policy enforcement that can shut a session down, apply surgical encryption or masking, identify malicious behavior, and perform other actions in both directions.

The inclusion criteria for this IDC MarketScape are as follows:

- The solution must offer an on-premises and/or cloud service focused on real-time management and monitoring of activity between end users and multiple public SaaS and/or IaaS environments intended to provide protection to the enterprise.
- The solution must have at least $10 million in worldwide organizational revenue in the previous 12 months, with at least $5 million in a CSG product/platform.
- The solution must have worldwide operations in the Americas, EMEA, and APAC.
- The solution must offer at least four of the following functions applied to enterprise users accessing multiple public SaaS/IaaS environments: identity insight, deep application insight, activity monitoring, content monitoring, policy enforcement, and encrypted communications.

More specifically, the cloud security platform has the following characteristics and functions:

- **Identity insight.** The user is a crucial endpoint in cloud-based architectures. CSGs do not typically store and manage users, but they must consume identity information to use for tracking and policy enforcement.
- **Deep application insight.** Following a trend started a few years ago, the CSG must understand multiple public cloud apps at a granular functional level, with or without published APIs.
- **Activity monitoring.** CSGs track the actions and transactions occurring among users and cloud applications to understand the typical and anomalous activities and provide an opportunity to take action for any activity deemed to be inappropriate.
- **Content monitoring.** In addition to tracking activity, CSGs track structured and unstructured content during its life cycle to identify sensitive locations and actions throughout the cloud environment.
- **Policy enforcement.** CSGs must be in a position to take action associated with activity and content monitoring. They must have an interface for developing policies about the resources in play and incorporate mechanisms for notifying, alerting, blocking, redirecting, and/or obfuscating (e.g., encrypting) sessions and content based on results.
- **Encrypted communications.** CSGs must be able to provide basic communication encryption along the entire path between users and applications/services.

In addition to these core functions, CSG solution providers are differentiating with a handful of different features that include more robust unsanctioned app discovery, application risk and control catalogs, app and/or user risk scoring, single sign-on (SSO), and data-at-rest encryption. These differentiators are discussed in context in the sections that follow.

ADVICE FOR TECHNOLOGY EXECUTIVES

Cloud security is at a turning point in enterprises as adoption levels have rapidly increased over the past few years. More and more higher-risk information is being stored and managed in public SaaS, PaaS, and IaaS environments.

CSGs are likely to become the key security solution for any organization that is heavily dependent on cloud environments, in particular, public SaaS solutions. Given the mass movement toward solutions like Office 365, salesforce.com, Dropbox, Box.com, and Google Apps, this means almost everyone. The more robust and complex the cloud environment, the more likely a CSG will be required for efficient and effective security management.

Accordingly, technology executives should consider the following:

- **Determine the level of complexity expected for cloud security over the next three years.** All of these solutions satisfy basic needs for cloud security, but enterprises that expect to have a complex cloud architecture at all layers (SaaS, PaaS, and IaaS) with public and custom apps should lean toward solutions that are dedicated to supporting these new cloud architectures.
- **Begin with what you have.** The previous bullet point notwithstanding, CSGs have a broad set of capabilities that overlap significantly with existing traditional products. It is likely that your existing solutions incorporate some of the CSG functionality already. In some cases, the capabilities may be included in licenses unbeknownst to tech executives.
- **Look to your existing strategic security vendors.** When evaluating CSG solutions, ensure your existing strategic security vendors are included. They likely have products and clear road maps to incorporate CSGs into broader security programs.
- **Evaluate your encryption strategy.** Whether to incorporate key management and encryption of structured and unstructured data is a "hot button" issue for many solution providers in this space. IDC recommends performing a separate evaluation in this area, however, for those organizations with basic requirements, such as encrypted file transfer, where CSG capabilities may make sense. Solutions vary significantly in their approach in this regard.
- **Custom app support may be the differentiator.** It is extremely difficult to evaluate support for custom applications among these CSGs, primarily because it is extremely uncommon. To the extent your organization is committed to custom apps that will require security, you will find a handful of players that have strong capabilities here, but will need to decide for yourself which one specifically fits the bill.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of the vendor's strengths and challenges.

Forcepoint

Forcepoint is positioned as a Major Player in this IDC MarketScape.

Forcepoint acquired Skyfence from Imperva in February 2017. The first product of Skyfence was made generally available in January 2014. With this acquisition, Skyfence – Forcepoint CASB – inherits the resources of 50 offices in 45 countries operating 27 datacenters and 2,500 channel partners.

Forcepoint CASB has worldwide presence with 41 datacenter locations (15 in NA, 10 in APAC, and 16 in EMEA) that comprise of Forcepoint locations as well as AWS datacenters. It provides for various proxy and API connector architecture options both in the cloud and on-premises.

Forcepoint CASB supports API monitoring for five popular SaaS apps as well as a number of less popular ones, and two PaaS/IaaS environments. It also provides granular access control support for more than 70 other cloud apps.

Along with standard protection for UBA and DLP, Forcepoint CASB provides device control to apply policy controls for both trusted and untrusted devices. It also plans to provide encryption capabilities to integrate with bring-your-own-key functionality in the near term.

Forcepoint CASB has a governance solution for on-demand assessment of applications and configurations and an audit and protection solution for real-time monitoring and blocking. They can be purchased alone or together in a security suite.

Strengths

Forcepoint CASB has a significant number of datacenter locations around the world. The Forcepoint acquisition is intended to provide more integration with a broader portfolio of security products. The ability of Forcepoint CASB to integrate custom apps may be useful to enterprises.

Challenges

Forcepoint's cloud security gateway solution is not well known to the market. Forcepoint only recently acquired Skyfence from Imperva and questions remain about the opportunity for success with integration and strategy.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

The cloud security platform market incorporates inline proxy gateways and API connectors to discover, monitor, and protect the use of cloud security applications by organizations. In particular, these solutions typically offer the following functionalities:

- **Identity insight.** The user is a crucial endpoint in cloud-based architectures. CSGs do not typically store and manage users, but they must consume identity information to use for tracking and policy enforcement.
- **Deep application insight.** Following a trend started a few years ago, the CSG must understand multiple public cloud apps at a granular functional level, with or without published APIs.
- **Activity monitoring.** CSGs track the actions and transactions occurring between users and cloud applications to understand the typical and anomalous activities and provide an opportunity to take action for any activity deemed to be inappropriate.
- **Content monitoring.** In addition to tracking activity, CSGs track the life cycle of structured and unstructured content during its life cycle to identify sensitive locations and actions throughout the cloud environment.
- **Policy enforcement.** CSGs must be in a position to take action associated with activity and content monitoring. They must have an interface for developing policies about the resources in play and incorporate mechanisms for notifying, alerting, blocking, redirecting, and/or obfuscating (e.g., encrypting) based on results.
- **Encrypted communications.** CSGs must be able to provide basic communication encryption along the entire path between users and applications/services.

LEARN MORE

Related Research

- *Worldwide Software as a Service and Cloud Software Forecast, 2017-2021* (IDC #US42014217, July 2017)
- *Worldwide Software as a Service and Cloud Software Market Shares, 2016: The Year of Multicloud* (IDC #US42884217, July 2017)
- *Worldwide IT Security Products Forecast, 2017-2020: Comprehensive Security Products Forecast Review* (IDC #US42374417, March 2017)

Synopsis

This IDC study evaluates the major players in the cloud security platform market and identifies their strengths and challenges.

"Every organization that uses cloud applications needs a cloud security platform to protect its data," said Pete Lindstrom, VP of Security Strategies.

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