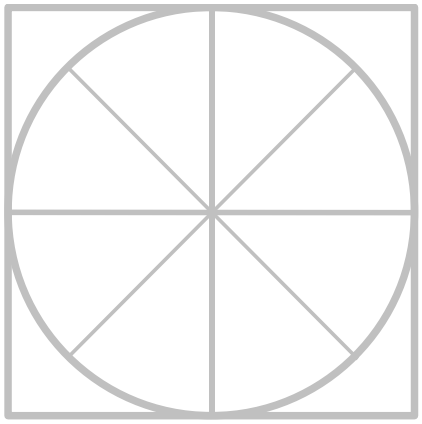
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Cloud Access Security Broker (CASB) - Market Quadrant 2018



An Analysis of the Market for CASB Solutions, Revealing Top Players, Trail Blazers, Specialists and Mature Players.

October 2018

TABLE OF CONTENTS

==========

==========

RADICATI MARKET QUADRANTS EXPLAINED

Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

1. ***Top Players*** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don't become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.

2. ***Trail Blazers*** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for "disrupting" the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

3. ***Specialists*** – This group is made up of two types of companies:

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.
    b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

4. ***Mature Players*** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered "movers and shakers" in this market as they once were.

    a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, they may choose to slow development on existing products.

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.
c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant. As a vendor continues to develop its product solutions adding features and functionality, it will move vertically along the "y" functionality axis.

The horizontal "x" strategic vision axis reflects a vendor's understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.

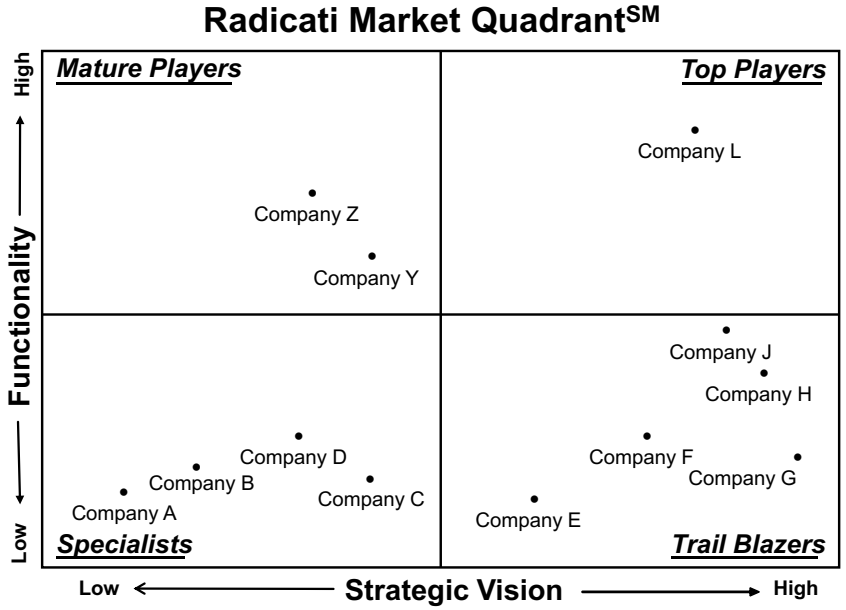


Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

We include vendors based on the number of customer inquiries we receive throughout the year. We normally try to cap the number of vendors we include to about 10-12 vendors. Sometimes, however, in highly crowded markets we need to include a larger number of vendors.

MARKET SEGMENTATION – CLOUD ACCESS SECURITY BROKER (CASB)

This edition of Radicati Market Quadrants[SM] covers the "**Cloud Access Security Broker**" segment of the Security Market, which is defined as follows:

- **Cloud Access Security Broker (CASB) –** are solutions that serve to monitor activity and enforce security policies between cloud users and cloud applications. CASB solutions give organizations visibility into authorized and non-authorized (i.e. Shadow IT) cloud applications, in order to monitor user activity, warn administrators about hazardous actions, enforce security compliance policies, and prevent malware. Some of the leading players in this market are *Bitglass, CipherCloud, Cisco, Forcepoint, McAfee, Microsoft, Netskope, Palo Alto Networks, Proofpoint,* and *Symantec.*

- CASB solutions are available as cloud services, on-premises appliances (physical or virtual), or hybrid solutions. While cloud-based CASB solutions are more prevalent, on-premises CASB solutions are still in demand by a number of regulated industries in order to meet compliance requirements.

- CASB solutions may operate in different modes, which include: Forward Proxy (all traffic is directed through a proxy, which requires signed certificates on all devices), Reverse Proxy (all traffic is backhauled through the corporate network, which doesn't require agent software to be downloaded on devices), or API inline mode (using the cloud application's API). Some solutions support "mixed mode" or "multi-mode", which use both proxy and API mode.

- CASB solutions monitor user activity across desktop and mobile devices, and typically offer tight integration with other solutions such as Data Loss Prevention (DLP), Threat Intelligence, Authentication and Singe Sign-on, Encryption, Web Security, Application Firewalls, User and Entity Behavior Analytics (UEBA), Email Providers, and more.

- The worldwide revenue for CASB solutions is expected to grow from $400 million in 2018, to over $1.0 billion by 2022.

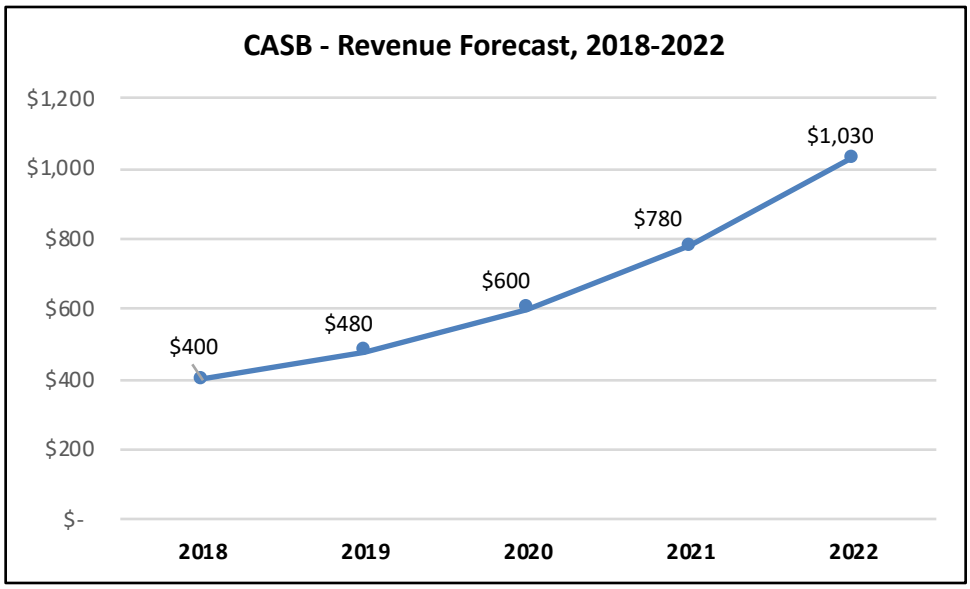


Figure 2: CASB Market Revenue Forecast, 2018 – 2022

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: *Functionality* and *Strategic Vision*.

Functionality is assessed based on the breadth and depth of features of each vendor's solution. All features and functionality do not necessarily have to be the vendor's own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor's strategic direction, which comprises: a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

Vendors in the *Cloud Access Security Broker (CASB)* space are evaluated according to the following key features and capabilities:

- ***Deployment Options*** – availability of a CASB solution in different form factors, such as cloud-based, on-premises appliance and/or virtual appliance, or hybrid.

- ***Operation Mode*** – CASB solutions may operate in three different modes: Forward Proxy (all traffic is directed through a proxy, which requires signed certificates on all devices), Reverse Proxy (all traffic is backhauled through the corporate network, which doesn't require agent software to be downloaded on devices), or API inline mode (using the cloud application's API). Some solutions support "mixed mode" or "multi-mode", which use both proxying and API mode.

- ***Cloud Application and Shadow IT*** – CASB solutions should provide detection and inventory of all sanctioned and unsanctioned (Shadow IT) applications in use.

- ***Cloud Malware detection*** – cloud malware can include spyware, viruses, worms, rootkits, and much more. Detection may be based on signature files, reputation filtering (proactive blocking of malware based on its behavior, and a subsequent assigned reputation score), and proprietary heuristics. CASB solutions should provide malware detection and isolation.

- ***Threat Intelligence Feeds*** – the CASB solution should integrate with existing Threat Intelligence feeds to gain information about new threats as well as distribute information about threats it has identified to other security entities, e.g. Endpoint security solutions, Web Security Gateways, Secure Email Gateways, and others.

- ***Authentication and Single Sign-on Integration*** – CASB solutions should control access to cloud applications by integrating with Single Sign On and multifactor user authentication. At a basic level, integration allows the CASB solution to control the onset of a user's cloud application session. However, deeper integration between CASB and multifactor authentication allows the CASB to also require additional rounds of authentication in mid-session if it suspects the user is engaging in risky activity. If the user completes the authentication successfully the action is allowed, while if they don't it is blocked. This ensures that legitimate actions are enabled while actions triggered by malware or a hacker are denied.

- ***Encryption*** – integration with encryption allows confidential data to be automatically encrypted based on automatic DLP classification policies when users send data to a cloud account. Later, users who want to view or download that same file must pass a user authentication check to verify that they have permission to access the data. This encryption and authentication requirement should stay with the file even after it has been downloaded from a cloud account and sent on to another user (e.g. colleague, partner, customer, etc). In addition, the CASB solution keeps track of who has access to a particular file wherever it goes, and provides the ability to revoke access to it at any time.

- ***Web Security*** – CASB solutions should integrate with Secure Web Gateway solutions (either the vendor's own or third parties). This allows the CASB cloud application risk intelligence to dynamically feed the secure web gateway so organizations can automate control over shadow IT use of cloud applications. If the intelligence feed provides information on granular risk attributes associated with specific cloud applications organizations can create policy controls directly in their Secure Web Gateway solution to monitor, redirect, or block the use of cloud applications based on risk attributes. In addition, connecting Secure Web Gateway logs into the CASB solution helps ensure continual monitoring and risk analysis of what applications employees are using. The integration should be easy to manage through a backend administrative interface, which can also provide unified user authentication and traffic management.

- ***Application Firewalls*** – CASB solutions should integrate with application firewalls (either the vendor's own or third parties). This again ensures maximum cohesion across different points of data egress through a set of common compliance policies.

- ***Email Providers*** – CASB solutions should integrate with leading email solutions, such as Google G Suite and Microsoft Office 365.

- ***DLP*** – CASB solutions should integrate with Data Loss Prevention (DLP) solutions either from the same vendor or third party vendors. By integrating CASB with enterprise DLP, organizations can ensure that inspection of data residing in cloud applications is based on the same DLP policies in use throughout the enterprise. It allows organizations to easily apply the same policies to data in the cloud as for data at the endpoint, datacenter, or network.

- ***User and Entity Behavior Analytics (UEBA)*** – CASB solutions can integrate with UEBA solutions to track and detect any anomaly in user behavior based on machine learning techniques. This also helps organizations gain additional insight into how users may be accessing data across multiple devices.

- ***SIEM Integration*** – CASB solutions should be able to integrate with Security Information and Event Management (SIEM) solutions to collect log data from network firewalls and web proxies, as well as report cloud threats to the SIEM. This ensures tighter intelligence and more rapid intrusion detection across the organization. The CASB solution will typically provide a SIEM with cloud-related usage and threats in two ways: by sending events to a SIEM via a syslog feed, or by exposing an event API for the SIEM to query.

- ***GDPR support*** – a number of CASB solutions now support specific features and/or modules in support of European Union General Data Protection Regulation (GDPR) compliance requirements. This is important since GDPR mandates the disposition of user data according to specific privacy requirements. CASB solutions can offer libraries of pre-built identifiers that can be used to scan for names, phone numbers, addresses, national identity and driver's license numbers, health record information, bank account numbers, and more. CASB solutions can also include policy options that allow organizations to geofence personal information in order to meet GDPR's in-country data residency requirements.

- ***Administration*** – CASB solutions should offer an easy-to-use interface, that allows administrators to effectively design and disseminate policy controls in accordance with the organization's compliance needs.

In addition, for all vendors we consider the following aspects:

- *Pricing* – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a "good value".

- *Customer Support* – is customer support adequate and in line with customer needs and response requirements.

- *Professional Services* – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

Note*: On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*

MARKET QUADRANT – CASB

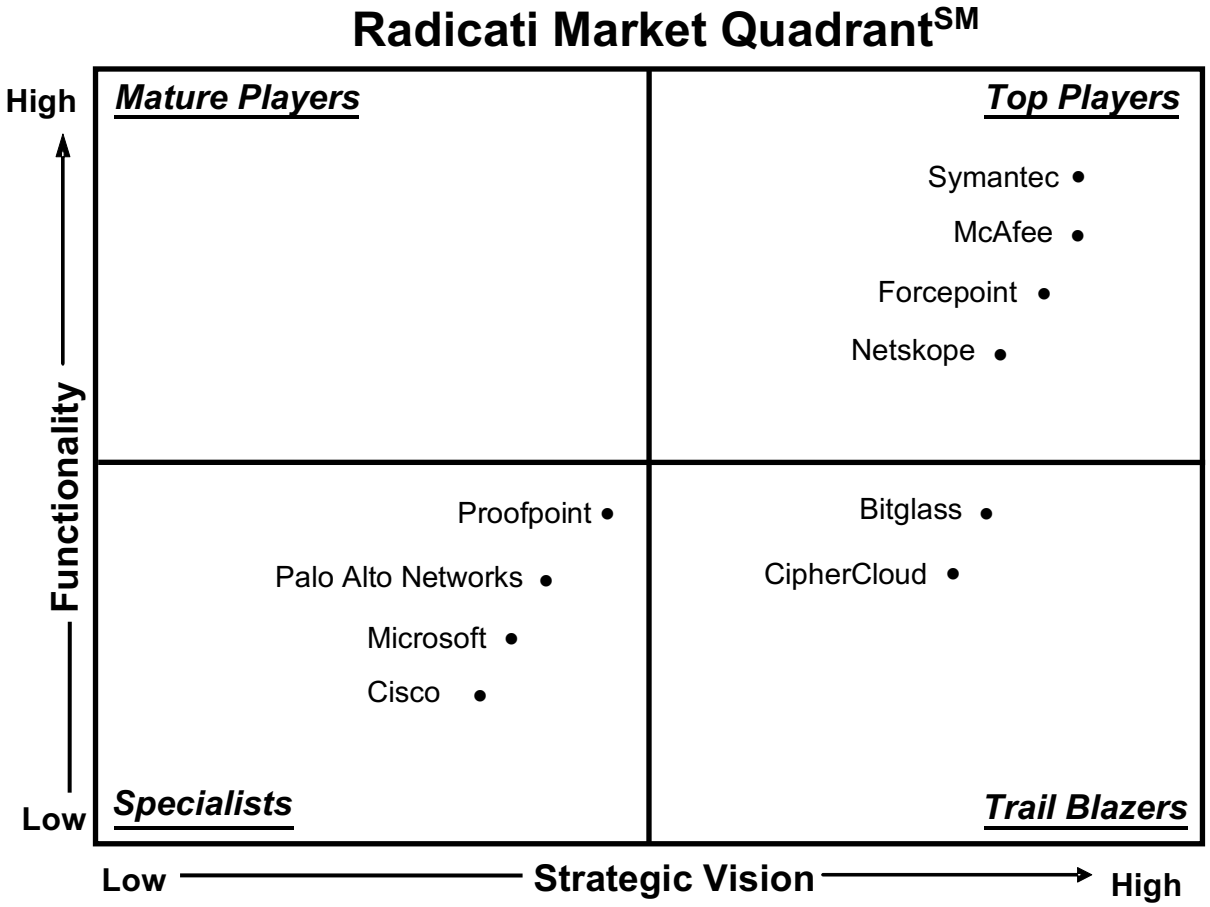


Figure 3: CASB Market Quadrant, 2018*

* Radicati Market Quadrant℠ is copyrighted October 2018 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the market are *Symantec, McAfee, Forcepoint,* and *Netskope.*
- The **Trail Blazers** quadrant includes *Bitglass,* and *CipherCloud*.
- The **Specialists** quadrant includes *Proofpoint, Palo Alto Networks, Microsoft,* and *Cisco*.
- There are no **Mature Players** in this market at this time.

CASB - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Symantec offers a wide range of security solutions for enterprises and consumers. Symantec operates one of the largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. In 2016, Symantec acquired BlueCoat, which included Elastica CloudSOC CASB. Symantec is publicly traded.

SOLUTIONS

The **Symantec CloudSOC** platform provides visibility into shadow IT, governance over sensitive data in cloud apps, and user and entity behavior analytics (UEBA) to protect against compromised accounts, cyber threats and malware, as well as granular monitoring of cloud app activity for incident investigation and response. CloudSOC is deployed as a cloud service, but also offers on-premises virtual appliances (called SpanVA) to help streamline information exchange to the service (e.g. by aggregating and anonymizing log data).

CloudSOC is a multimode solution, offering forward proxy, reverse proxy, and API modes of operation. It provides granular visibility into hundreds of cloud apps and services, and also monitors and controls custom apps. CloudSOC provides full support for major collaboration suites, such as Google G Suite and Microsoft Office 365.

The Symantec CloudSOC product comprises the following components:

- **Symantec CloudSOC Audit** – discovers and monitors both sanctioned and unsanctioned cloud services and mobile apps. It maintains a database of tens of thousands of cloud apps and services, including native mobile apps, for Shadow IT discovery. In addition, it calculates each app's customizable Business Readiness Ratings (BRR) based on over 120 security attributes, enabling organizations to make smart app choices through side-by-side cloud app comparisons. CloudSOC Audit automatically delivers cloud app intelligence to Symantec Secure Web Gateways, such as ProxySG and WSS, for Shadow IT visibility and control. Policies can be applied and enforced directly from the secure web gateway management console. In addition to ingesting proxy and firewall logfiles for Shadow IT discovery, CloudSOC can also ingest and analyze log files from Symantec Endpoint Manager to discover shadow IT on roaming devices outside of the network perimeter.

- **Symantec CloudSOC Security for SaaS** – monitors and controls the use of a wide range of sanctioned SaaS platforms through API interfaces. It relies on Securlets (i.e. API interfaces) to provide visibility and control for sanctioned apps, including for Microsoft Office 365, Google G Suite, Box, Dropbox, Salesforce and others. The Securlets for Box and Office 365 include Fast API functionality, which allows for faster identification and remediation of exposures and threats by reducing API polling overhead.

- **CloudSOC Security for IaaS** – monitors administrator activity, enforces policies to prevent misconfiguration, protects against compromised credentials and provides DLP and malware protection for storage. In addition, Cloud Workload Assurance (CWA), Symantec's cloud security posture management solution, assesses the compliance posture of cloud environments through out-of-the-box policies. CWA policies comprise automated checks which run on cloud resources and enable customers to prove compliance with PCI, HIPAA, CIS, and other compliance standards. It also provides detailed remediation guidance.

- **Symantec CloudSOC Gateway** – is an in-line security gateway that enables enterprises to continuously monitor and control the use of sanctioned and unsanctioned cloud apps in real-

time. It includes hundreds of standard Gatelets (i.e. gateway signatures) for the most popular cloud apps, as well as a custom Gatelet that enables customers to create Gatelets for any cloud app, including custom developed apps in AWS, Azure, or Google Cloud Platform. CloudSOC Gateway can operate as a forward proxy, or reverse proxy.

Symantec CloudSOC also leverages a number of key integrations with other Symantec solutions, which include:

- **CloudSOC and Symantec DLP** – leverages existing on-premises DLP policies and workflows to extend protection to content in cloud services, through a single management console for DLP. CloudSOC integrates with Symantec DLP via a RestAPI connection (rather than ICAP) which maximizes performance and allows for granular controls.

- **CloudSOC and Symantec Proxy integration** – is the integration of CloudSOC Audit with Symantec's web security solutions (i.e. ProxySG and WSS), which through a feed of tens of thousands of cloud apps and their risk attributes, enables Shadow IT visibility and policy control from the proxy management console.

- **CloudSOC and Symantec Encryption** – CloudSOC integrates with Symantec Information Centric Encryption (ICE) to deliver an end-to-end information rights management solution. It allows sensitive content to be automatically identified and encrypted as it is transferred to the cloud, and it remains encrypted as it is downloaded from the cloud to an endpoint. Users must authenticate themselves in order to access the content. At any point in time, the organization can revoke the data, essentially digitally shredding it.

- **CloudSOC and Symantec Advanced Threat Protection** – delivers file reputation intelligence, URL analysis, AV scanning, and sandboxing technologies to protect cloud accounts and transactions against malware.

- **CloudSOC and Symantec VIP** – enables Adaptive Authentication. When CloudSOC detects elevated risk in the network, based on a user's threat score, or an attempt to access sensitive content, or a variety of other customizable transactions, a real-time message is sent to VIP to trigger a multifactor authentication challenge to the end user. Organizations can craft these policies based on a variety of criteria, providing greater security in real-time vs. simple single sign-on (SSO) protection at the start of a session.

- **CloudSOC and Symantec Endpoint (SEP)** – enables CloudSOC Audit to ingest log files from SEP Manager to uncover Shadow IT for users and managed devices that are accessing the cloud from outside of the corporate network. SEP mobile integration provides CASB profile provisioning on mobile devices, such as iOS, which simplifies deployment.

In addition to these integrations with Symantec products, CloudSOC also integrates with third party solutions for DLP, encryption, authentication. CloudSOC also offers agents for popular SIEMs, such as HP ArcSight, IBM QRadar, and Splunk. The agents can also be customized to work with other SIEMs based on the log formats they consume.

Symantec CloudSOC offers compliance with FERPA, GLBA, HIPAA, PCI, PII, as well as industry-specific regulations.

Symantec CloudSOC SaaS Securlets, Gateway and Audit are licensed user/year. Whereas, IaaS Securlets for AWS, Azure, and other virtualization platforms, are licensed by volume (i.e. MBs) of data used.

STRENGTHS

- Symantec CloudSOC is a multimode solution, which includes API, as well as forward and reverse proxy modes of operation.

- Symantec CloudSOC provides coverage for a wide range of apps and cloud platforms, including full coverage of Google G Suite (i.e. including all services), and Microsoft (i.e. including all services).

- Symantec leverages integration of CloudSOC with its content-aware, enterprise DLP solution to deliver a common set of DLP policies and workflows that work across cloud apps as well as other network elements under DLP protection.

- CloudSOC uses the same anti-malware engines and reputation intelligence that come with Symantec Endpoint Protection, as well as its Advanced Threat Prevention (ATP) cloud sandboxing and URL reputation to detect and mitigate advanced threats such as ransomware.

- CloudSOC is fully integrated with UEBA functionality to protect users from account takeovers, data exfiltration, and data destruction.

- CloudSOC is tightly integrated with other solutions across Symantec's portfolio, such as Web Security, DLP, User Authentication, Information Rights Management, Advanced Malware Protection, and Endpoint Security. This delivers streamlined protection across an organization's entire security infrastructure.

WEAKNESSES

- While offering a rich set of functionality, Symantec CloudSOC requires an experienced IT team to properly deploy and maintain the solution in a way that best leverages its full capabilities.

- Symantec currently offers a wide breath of API support, but needs to continue adding new API connectors for support of additional popular cloud apps. The vendor has this on its roadmap.

- Symantec needs to leverage device security posture from SEP Mobile (from its Skycure acquisition) to provide additional cloud app controls in CASB. The vendor has this on its roadmap.

MCAFEE
2821 Mission College Blvd.
Santa Clara, CA 95054
www.mcafee.com

McAfee delivers security solutions and services for business organizations and consumers. The company provides security solutions, threat intelligence and services that protect endpoints, networks, servers, cloud and more. In 2017, McAfee acquired Skyhigh Networks an early developer of cloud security services and cloud access security broker (CASB) technology.

SOLUTIONS

McAfee Skyhigh Security Cloud is a CASB solution that can be deployed on-premises as a virtual appliance, in the cloud, or in hybrid mode. It addresses the security needs of SaaS (Software as a Service, PaaS (Platform as a Service), and IaaS (Infrastructure as a Service)

environments. McAfee Skyhigh Security Cloud can operate in a multi-mode deployment architecture, which includes:

- *API* – in this mode it establishes direct connections to cloud services using publicly available APIs from cloud providers. It also supports near-real time controls as data is uploaded, or real-time when shared via the Lightning Link API deployment mode.

- *Reverse Proxy* – McAfee Sky Gateway is an inline reverse proxy that supports several capabilities not available in API mode, such as encryption, access control, and real-time data loss prevention.

- *Forward Proxy* – McAfee Sky Gateway can be deployed in a forward proxy mode, which can be used to enforce inline controls across shadow or sanctioned cloud services.

- *Log collection* – in this mode, Skyhigh collects event logs generated by existing infrastructure such as firewalls and secure web gateways to provide visibility into shadow cloud usage.

McAfee Skyhigh Security Cloud delivers the following functionality:

- *Cloud application and shadow IT* – Skyhigh Security Cloud discovers all cloud services (sanctioned and shadow, including shadow IaaS) in use by employees both on and off-network, including thousands of cloud services uncategorized by firewalls and web proxies. The solution's usage analytics summarizes cloud usage in aggregate, at the department and user level with traffic patterns, access count, and usage trends over time.

- *Threat Intelligence Feeds* – Skyhigh Security Cloud integrates with McAfee's Global Threat Intelligence (GTI) and Advanced Threat Defense capabilities. McAfee Skyhigh Security Cloud receives and incorporates different intelligence feeds as part of applying security controls to cloud usage. These include: IP reputation (both source and destination), Attachment reputation (e.g. malware signatures), URL reputation (e.g. cloud phishing), User risk, and Darknet intelligence. It also integrates with third party industry solutions, including: Digital Element, Zscaler, CSID (Experian), Cyphort, and Cloud Cyber Incident Sharing Center (CloudCISC).

- *Authentication and Single Sign-on* – Skyhigh Security Cloud integrates with authentication providers via SAML to enforce step-up authentication, leveraging the authentication factors users are already familiar with. It also integrates with major IDaaS or Sign Sign-on providers that support the SAML standard, including Azure Active Directory, Centrify, Okta, OneLogin, and Ping Identity.

- *Encryption* – Skyhigh Security Cloud includes encryption at field level, object level, and file level.

- *Web Security* – Skyhigh Security Cloud integrates with web security solutions to support log collection and analysis as well as closed-loop policy enforcement, including McAfee Web Gateway, Palo Alto Networks, Check Point, Fortinet, Cisco, Zscaler.

- *Application Firewalls* – Skyhigh Security Cloud integrates with all major firewall solutions to support log collection and analysis as well as closed-loop policy enforcement, including McAfee, Palo Alto Networks, Check Point, Fortinet, Cisco, and McAfee.

- *Email Providers* – Skyhigh Security Cloud integrates with leading cloud email service providers such as Microsoft Office 365 and Google G Suite to provide security controls.

- *Data Loss Prevention* – Skyhigh Security Cloud provides data loss prevention (DLP) capabilities while also integrating with existing enterprise DLP solutions, such as McAfee DLP or Symantec DLP.

- *User and Entity Behavior Analytics (UEBA)* – Skyhigh Security Cloud provides its own UEBA functionality, to detect insider threats, priviledged user threats, compromised account threats, data exfiltration, ransomware, and cloud phishing.

- *SIEM integration* – Skyhigh Security Cloud supports both syslog and API connections to SIEM solutions. Additionally, McAfee Skyhigh Security Cloud exposes an API that can be used by SIEM and other analytics tools for forensic investigations. Skyhigh Security Cloud also offers a Splunk App to simplify analyzing Skyhigh data within Splunk.

- *Administration* – Skyhigh Security Cloud provides, a single, intuitive management interface for security administrators to investigate policy violations, create a single policy or a set of policies, and seamlessly apply them to all users and cloud services, including IaaS services

and resources. McAfee Skyhigh Security Cloud also integrates with **McAfee's ePO (ePolicy Orchestrator)** administrative console, which can be used to can centrally set policies, manage incidents and workflows across all its solutions.

McAfee Skyhigh Security Cloud has achieved compliance certifications for FedRAMP, ISO 27001, SOC2, and others. It also adheres to data residency and privacy regulations such as EU GDPR, PCI-DSS, FISMA, GLBA, HIPAA-HITECH, PIPEDA, and others.

For sanctioned SaaS and Shadow, McAfee Skyhigh Security Cloud is priced per user. For sanctioned IaaS, McAfee Skyhigh Security Cloud is priced per IaaS account.

STRENGTHS

- McAfee Skyhigh Security Cloud supports a set of operational modes including API, Reverse Proxy, Forward Proxy, and Log Collection, which addresses the needs of complex cloud environments.

- McAfee Skyhigh Security Cloud can be deployed on-premises as a virtual appliance, in the cloud, or in hybrid mode. While most organizations will deploy a cloud approach, many organizations still require an on-premises virtual appliance approach to satisfy in-country or industry requirements, as well as co-location with custom applications.

- McAfee offers a full set of capabilities for cloud security, which include DLP, Collaboration Control, Access Control, Threat Protection, Malware Integration, Shadow Visibility, Configuration Audits, aimed at the needs of SaaS, PaaS, and IaaS environments.

- McAfee delivers out-of-the-box integration to third-party security solutions using open standards, including Identity platforms (IdP), next generation firewalls (NGFW), Secure web gateways (SWG), rights management (EDRM), SIEM, malware engines, HSM, DLP, and EMM/MDM solutions.

- McAfee Skyhigh Security Cloud can be centrally managed via the McAfee ePolicy Orchestrator, that also provides central management for all other McAfee solutions in an organization which allows for easier common policy management across all solutions.

- McAfee Skyhigh Security Cloud delivers one of the most impressive set of compliance certifications and adherence to leading data privacy regulations, with a clear understanding of different regional requirements.

WEAKNESSES

- McAfee could work to further simplify its licensing, packaging and pricing model for McAfee Skyhigh Security Cloud. The vendor is working to address this.

- McAfee Skyhigh Security Cloud needs to continue to accelerate its integration with the broader McAfee products portfolio, including the McAfee Web Gateway (MWG), and Cloud Workload Security (CWS).

- McAfee Skyhigh Security Cloud could move closer towards supporting full customer self-service onboarding.

- While attractively priced for the level of functionality it delivers, McAfee Skyhigh Security Cloud is priced somewhat at a premium compared to other solutions.

- While offering a rich set of functionality, McAfee Skyhigh Security Cloud will require an experienced IT administration team to properly install and maintain the solution in a way that fully leverages its capabilities.

FORCEPOINT
10900 Stonelake Blvd
3rd Floor
Austin, TX 78759
www.forcepoint.com

Forcepoint is a joint venture of Raytheon Company and Vista Equity Partners that was formed in 2015 out of a combination of Websense, Raytheon Cyber Products, and the Stonesoft and Sidewinder firewall assets it acquired from Intel Security in early 2016. In 2017, Forcepoint acquired the Skyfence CASB business from Imperva, as well as RedOwl, a vendor of user behavior and security analytics. Forcepoint offers DLP, web, data, and email content security,

cloud access security, next generation firewall, user behavior analysis, insider threat detection, and threat protection solutions to organizations of all sizes.

SOLUTIONS

Forcepoint CASB automatically discovers cloud application use, analyzes risks, and enforces appropriate controls for Software as a Service (SaaS) and custom applications. It is available as a cloud service, and is also available as an embedded module in Forcepoint's DLP and secure web gateway offerings. Forcepoint CASB supports all modes including forward proxy, reverse proxy, API mode or any combination. Forcepoint CASB supports detection and inventory of sanctioned and unsanctioned applications or Shadow IT. The reverse proxy support provides visibility into access and activities performed by un-managed devices (BYOD) using business applications. A risk dashboard within Forcepoint CASB gives adminstrators a view of the risk scores and risk factors associated with cloud applications that have been accessed by users.

Forcepoint CASB supports the following functionality:

- *Cloud malware detection* – integrated sandboxing is provided via Forcepoint's Advanced Malware Detection (AMD) module, which provides full stack emulation to detect all types of malware including sophisticated sandboxing-aware malware.

- *Threat Intelligence feeds* – Forcepoint CASB has both built-in Threat Intelligence provided by Forcepoint Labs, and integration with third party solutions, like Lastline.

- *Authentication and Single Sign-on* – Forcepoint CASB integrates with leading authentication and SSO solutions including Centrify, Ping, Okta, OneLogin, SecureAuth, Microsoft and others. It also ties in to SSO providers for reverse proxy to monitor activities performed by unmanaged devices (BYOD).

- *Encryption* – Forcepoint CASB serves as a broker between a customer's key store and a cloud app's Bring Your Own Key (BYOK) encryption functionality. This leverages the cloud app's native BYOK encryption functionality, while giving customers full control of their encryption keys. It can perform all key actions including periodic key rotations and provide full audit. Encryption broker works at both app and field level.

- *Web security* – Forcepoint CASB integrates with Forcepoint's Web Security solution. As a part of the integration the web security solution provides cloud application discovery and reporting. Adminstrators can see the risk level of accessed applications and the associated risk factors. Administrators can see which users have accessed a given high risk cloud application and then pivot to see which other high-risk cloud apps have been accessed by the same users.

- *Application firewalls* – Forcepoint CASB integrates with Forcepoint's next generation firewalls (NGFW), enabling traffic in enterprise networks to be seamlessly directed to the CASB without requiring manual redirection or client software. In addition, both Forcepoint CASB and Forcepoint NGFW, also integrate with Forcepoint Web Security Cloud to enable web content to be dynamically analyzed through the web gateway, while sanctioned application traffic is sent directly to the CASB.

- *DLP* – Forcepoint CASB provides native DLP functionality. It also integrates with Forcepoint's DLP solution. The DLP content analysis is performed within the CASB cloud service, using Forcepoint's DLP engine, which means that no files are sent back on-premises for DLP scanning. This considerably reduces DLP scanning latency, and allows Forcepoint DLP customers to apply their exising DLP policies to enterprise cloud applications. ICAP integration is also available, allowing DLP analysis to be performed by any DLP vendor supporting ICAP.

- *User and Entity Behavior Analytics (UEBA)* – Forcepoint CASB leverages both supervised and unsupervised machine learning algorithms to profile common user behavior (e.g. typical geo-location, devices used, pages and modules typically accessed, activity volumes, and more) and help detect behavior anomalies. Forcepoint CASB has built in risk adaptive protection, and when used in conjunction with Forcepoint Dynamic Data Protection (DDP) it can also provide risk adaptive data protection.

- *SIEM Integration* – Forcepoint CASB provides SIEM integration of all audited data (activities, alerts, shadow-IT, and more). Export can be set automatically using file connector or syslog messages. Forcepoint also provides a SIEM client allowing automatic & seamless retrieval of logs from the Forcepoint data center to the customer's site.

- *Administration* – Forcepoint CASB includes a single browser-based user interface which provides intuitive dashboards, reports and management/administration capabilities.

Forcepoint CASB offers adherence with leading compliance standards, including HIPAA, NIST, PCI DSS, and others.

STRENGTHS

- Forcepoint CASB supports all CASB operational modes including API, forward and reverse proxy.

- Forcepoint CASB leverages Forcepoint's full UEBA capabilities, to create risk profiles based on threat likelihood and business impact. It utilizes full context cloud behavior for analytics based on thousands of apps and activities to provide risk prioritized alerts for SOC and incident response teams.

- Forcepoint CASB integrates with Forcepoint DLP, which extends DLP functionality and dynamic data protection to cloud applications.

- Forcepoint CASB integrates with Forcepoint secure web gateway and next-generation firewall solutions for in-depth analysis of app data movement across all communication channels.

WEAKNESSES

- While Forcepoint CASB leverages threat intelligence provided by Forcepoint Labs and Lastline, it could benefit by adding more user data and risk feeds from other third party systems.

- While Forcepoint offers CASB and DLP capabilities, it does not yet offer the ability to set common policies across the two solutions. Forcepoint has this on its near-term roadmap.

- Forcepoint could strengthen its CASB solution, by further integrating it with its risk adaptive approach to security. The vendor has this on its roadmap.

- Forcepoint CASB would benefit from the addition of Information Rights Management (IRM) support for sensitive data.

- Forcepoint CASB is designed to work best in the context of a full Forcepoint deployment, consisting of Forcepoint DLP, Forcepoint NGFW, and Forcepoint web security.

NETSKOPE

270 3rd St.
Los Altos, CA 94022
www.netskope.com

Netskope, founded in 2012, develops cloud access security broker (CASB) solutions that provide full visibility into cloud activities, data protection and advanced threat protection. Netskope is based in Silicon Valley, with offices worldwide. The company is privately and held.

SOLUTIONS

Netskope Security Cloud relies on patented Cloud XD technology to deliver CASB functionality to help detect shadow IT, track and control data movement, and provide advanced threat protection. The solution is available in all deployment options, cloud, on-premises, or as a hybrid deployment.

Netskope offers multiple deployment modes, which can be used in parallel, as follows:

- *Risk Insights* – offers collection of logs from firewalls or web proxies either directly to Netskope's cloud, or via an on-premises Log Parser.

- *API Protection* – allows to connect directly to sanctioned cloud applications via APIs to audit, or detect all policy violations and actions before or after they occur.

- *Proxy-Chaining* – allows configuration of an on-premises perimeter proxy to steer explicit application to the Netskope platform for real-time contextual access control, policy control, data protection and governance.

- *Netskope Virtual Appliance* – can be configured in various operational modes to include ICAP DLP client, KMIP Client, Explicit Proxy or in DNS integration mode to allow traffic going to SaaS apps to be steered through the virtual appliance to Netskope in the cloud.

- *Netskope Dataplane On-Premise* – allows processing to be done directly on-premises, rather than forwarding traffic to the Netskope Cloud infrastructure. The management and reporting remain in the cloud.

- *Netskope Client* – users deploying the Netskope client will have their designated SaaS traffic steered through Netskope.

- *Netskope Reverse Proxy* – provides support for managed and unmanaged users access to sanctioned SaaS services through browser sessions.

- *Netskope Mobile Profile* – allows Netskope to deploy a profile or integrate with existing MDM solutions to steer traffic SaaS app to Netskope.

- *SAML integration* – can be used to apply granular policies over unmanaged endpoints.

Netskope's product offering includes:

- **Netskope for SaaS** – provides security and compliance for SaaS apps like Office 365, Box, Slack, and ServiceNow through continuous, real-time visibility and control of activities and data insight into the security posture of all deployed SaaS apps.

- **Netskope for IaaS** – provides comprehensive security and compliance for IaaS environments like AWS, Azure, and Google Cloud Platform by providing continuous, real-time visibility and control of activities and data insight into the security posture of IaaS resources.

- **Netskope for Web** – provides secure web gateway category-based URL filtering and threat detection as a cloud-based service.

All three services are managed from the Netskope Security Cloud, which provides visibility, analytics, data protection, threat protection, and more. Within the three services, Netskope offers the following options:

- *Netskope Risk Insights (Available across SaaS, IaaS, and Web)* – identifies all SaaS, IaaS, and Web use in an organization. It enables contextual understanding of cloud service and website usage, including information on users, activities, devices, location, and more. It

enables direct querying from the dashboard for dynamic cloud and web usage reports. It also provides unlimited access to the Netskope Cloud Confidence Index (CCI), a Netskope cloud app auditing tool, which helps assess the enterprise-readiness of each cloud service based more than 40 objective criteria.

- *Netskope API Protection (Available across SaaS and IaaS)* – relies on APIs from vendors like Box, G Suite, Office 365, and Slack to get visibility into usage and data already resident in the service. It inventories and classifies content, content owners, and collaborators as well as provides content sharing status. Additionally, it enables the download of files for review, and performs a variety of actions such as restricting access, revoke sharing, encrypting content, quarantining content, and placing content on legal hold.

- *Netskope Data Loss Prevention (Available across SaaS, IaaS, and Web)* – offers advanced DLP functionality. Key capabilities include more than 3,000 data identifiers, support for more than 1,000 file types, custom regular expressions, proximity analysis, fingerprinting, exact match, optical character recognition (OCR), and more. Netskope DLP detects violations across all cloud services and web traffic with an architecture capable of covering users whether they are on premises, remote, using a web browser, using a mobile app, or a sync client. It can also discover sensitive data at rest in cloud services and in motion to and from cloud services and websites.

- *Netskope Encryption (Available across SaaS, IaaS, and Web)* – provides advanced encryption, tokenization and key management technology to protect both structured and unstructured data, and can also use advanced DLP to selectively encrypt sensitive content. It operates automatically, transparent to end users, seamlessly encrypting and decrypting data behind the scenes. Netskope relies on advanced technology, including NIST-approved AES-256 encryption and a FIPS 140-2 level 3 certified key management service with a hardware security module and can integrate with an on-premises, KMIP-compliant key management system to keep encryption keys under control.

- *Netskope Threat Protection (Available across SaaS, IaaS, and Web)* – backed by Netskope Threat Research Labs, Netskope's threat prevention team, it delivers pre-execution, heuristic analysis and dynamic, sandbox analysis to detect and prevent zero-day threats. Netskope Threat Protection also provides ransomware detection and remediation capabilities, which protect cloud storage services from propagating ransomware. Unauthorized encryption due to ransomware is detected in sanctioned cloud services, such as Microsoft Office 365. Upon

detecting ransomware, Netskope provides an integrated workflow that uses cloud storage service versioning capabilities to restore affected files from earlier versions.

Netskope offers compliance with leading data residency and privacy regulations, including HIPAA, GDPR, GLBA, and PCI DSS.

STRENGTHS

- Netskope is available in all deployment options, cloud, on-premises, or as a hybrid deployment. This makes it attractive for customers with different deployment requirements.

- Netskope offers strong support for Shadow IT and provides an in-depth view of data movement across all cloud and web traffic sources, including web browsers, mobile apps, and sync clients.

- Netskope provides advanced DLP and encryption functionality across SaaS, IaaS, and web to protect data integrity. It also provides end-to-end incident management capabilities and automated workflows, to protect sensitive data in transit to the cloud or already resident in sanctioned cloud services.

- Netskope goes beyond CASB functionality by also providing advanced threat protection across SaaS, IaaS, and web, to deliver cloud-native security service with multi-layered threat detection and remediation capabilities.

- Netskope provides a single cloud-based management platform, for unified analytics and policy enforcement.

- Netskope provides visibility and control over native mobile applications (in addition to the control provided when users are accessing the cloud through a browser) this provides a greater level of control over mobile data exfiltration.

WEAKNESSES

- Netskope's support for API-based cloud applications is not as extensive as that provided by other CASB vendors.

- While Netskope supports a rich set of modes of operation (e.g. API, proxy, etc.), deploying all options correctly will require careful configuration planning and a capable IT staff.

- While delivering very high functionality, Netskope solutions are priced somewhat at a premium compared to other solutions.

TRAIL BLAZERS

BITGLASS

675 Campbell Technology Parkway
Suite #225
Campbell, CA 95008
www.bitglass.com

Bitglass, founded in 2013, develops cloud access security broker (CASB) solutions to deliver zero-day, agentless, data and threat protection for applications and devices. Bitglass is based in Silicon Valley, with offices worldwide. The company is privately held.

SOLUTIONS

Bitglass Next-Gen CASB provides agent-less zero-day data protection, threat protection, identity management, and visibility across managed and unmanaged apps (i.e. Shadow IT). It supports managed apps, such as Microsoft Office 365 and AWS, as well as unmanaged apps, such as personal Dropbox and social media. Unmanaged apps are automatically detected and can easily be sanctioned from an administrative console. Bitglass can be deployed in three ways: on-premises; in the customer's private cloud; or on Bitglass's globally hosted, multitenant SaaS offering delivered via AWS. The majority of customers leverage the multitenant SaaS deployment, which is available in major AWS regions globally, guaranteeing high performance for employees anywhere.

Bitglass supports a multimode architecture which includes *API integration*, as well as proxies to protect data in transit in real time as follows:

- *Forward proxies* – for managed devices.

- *Reverse proxies* – for unmanaged devices
- *ActiveSync proxies* – for mobile devices.

Bitglass Next-Gen CASB delivers the following functionality:

- *Cloud application and shadow IT* – automatic discovery and classification of hundreds of thousands of unsanctioned cloud applications via its shadow IT discovery product, which uses machine learning to categorize applications. Bitglass offers the ability to block shadow IT apps, coach users away from them, turn them read only to prevent data leakage, or sanction and protect through a variety of other capabilities such as data loss prevention.

- *Threat Intelligence Feeds* – Bitglass subscribes to several threat intelligence feeds, Information Sharing Analysis Centers (ISACs), and industry consortiums in order to integrate collective intelligence from the global security community.

- *Authentication and Single Sign-on* – Bitglass can act as an identity provider for single sign-on for cloud applications, as well as integrate with any single sign-on solution utilizing SAML 2.0, such as Okta, Ping, OneLogin, and others.

- *Encryption* – Bitglass delivers searchable SaaS encryption at the file and field level. It holds a patent on searchable, full-strength encryption for cloud data-at-rest. Bitglass uses FIPS compliant AES-256 crypto by default, but can work with any encryption algorithm as desired.

- *Web Security* – the Biglass agentless reverse proxy does not interfere with existing web security solutions.

- *Application Firewalls* – Bitglass interoperates with any firewall including Cisco, Juniper, Palo Alto Networks, Fortinet, Checkpoint, and others.

- *Email Providers* – Bitglass Next-Gen CASB can secure Microsoft Office 365, Google G Suite, and other email solutions, by authenticating users, scanning file attachments for threats, enforcing download DLP, and more.

- *Data Loss Prevention* – a native DLP engine supports all regex patterns, keyword matching, exact data matching, file metadata property matching, and advanced patterns. The Bitglass

DLP engine can ingest data classification metadata (e.g. Titus or Boldon James data classification tags in Office docs) and use it in policy decisions.

- *User and Entity Behavior Analytics (UEBA)* – Bitglass supports aggregation and baselining of user activities in order to detect deviations from standard behaviors and flag anomalies. Administrators can determine what kind of automated response they wish to deploy (e.g. suspicious user location can trigger multi-factor authentication).

- *SIEM integration* – Proxy logs generated by Bitglass Next-Gen CASB can be easily used by log aggregation devices, such as SIEMs or UBA/UEBA.

- *Administration* – Bitglass Next-Gen CASB logs every transaction across all cloud applications protected by the platform, to provide dynamic dashboards, reports, and alerts. Admins can consume the collected data on the Bitglass administrative console, or integrate with SIEMs or other SOC tools via the REST API.

Bitglass provides a prebuilt DLP pattern for GDPR compliance. It also adheres to leading data residency and privacy regulations, such as HIPAA, FedRAMP, FISMA, FERPA, and others.

STRENGTHS

- Bitglass can be deployed on-premises, in customer private cloud environments, or through its own multitenant SaaS offering delivered on AWS. This makes it attractive for customers with different deployment requirements.

- Bitglass Next-Gen CASB offers agentless deployments on any device, and can secure any app or workload, including SaaS apps, custom apps, and IaaS platforms.

- Bitglass is a multimode CASB solution that uses a combination of forward proxies, reverse proxies, ActiveSync proxies, and API integrations with cloud apps.

- Bitglass' Zero-day Shadow IT Discovery tool uses machine learning to automatically identify and evaluate new apps that employees access. This is a departure from labor-intensive processes of manually identifying and classifying new apps.

WEAKNESSES

- Bitglass does not have its own threat intelligence network, and instead it relies on third party threat intelligence feeds, ISACs, and industry consortiums in order to integrate collective intelligence into its solution.

- Bitglass does not integrate with web security gateways to share or gather threat detection information.

- The Bitglass administrative user interface could be improved, to ease activity visibility and streamline policy creation and distribution. The vendor is working to address this in the near term timeframe.

- Bitglass' incident management functionality could be improved so that, if a security incident occurs, it is easier to triage and assign events and remediation tasks to different administrators. The vendor is working to address this.

CIPHERCLOUD

2581 Junction Ave.
Suite #200
San Jose, CA 95134
www.ciphercloud.com

CipherCloud, founded in 2010, provides end-to-end protection for data resident in the cloud. Its cloud access security broker (CASB) solution delivers comprehensive visibility, data security, threat protection, and compliance for cloud-based assets. The company is privately held.

SOLUTIONS

The CipherCloud **CASB+** platform provides cloud security for users and data and enables complete control over user access, their activities and data access. CASB+ functionality includes visibility, end-to-end data protection, advanced threat protection, and compliance controls and support. CipherCloud CASB+ is available as a cloud service, on-premises, or as a hybrid deployment. Cloud hosted components can also integrate with enterprise systems to deliver a

richer, seamless security solution. CipherCloud CASB+ supports all three operation modes: forward proxy, reverse proxy and API mode. Cloud instances can be on-boarded in multi-mode manner, such as reverse proxy and APIs connected at the same time.

The CipherCloud **CASB+** platform provides the following functionality:

- *Cloud Application and Shadow IT* – CASB+ integrates with enterprise edge devices and next generation firewalls to detect cloud activity and provide an inventory of sanctioned and unsanctioned clouds. Categorization, risk rating and interactive analytics are also provided. The solution aggregates and correlates the raw activity using a rich knowledge base, provides risk scores and allows blocking of risky/undesirable cloud activity. Unwanted cloud activity can be also be suppressed as needed.

- *Cloud malware detection* – CipherCloud provides malware detection and isolation through the OEM integration of the BitDefender AV/AM engine. Ransomware detection and isolation are also included.

- *Threat Intelligence feeds* – CipherCloud leverages threat intelligence feeds from Juniper Networks Sky ATP. It also supports security feeds for malware signatures through BitDefender.

- *Authentication and Single Sign-on* – CASB+ integrates with Active Directory, ADFS, Ping Identity, Okta, SiteMinder, OneLogin, and others. Compatibility with SAML 2.0, ensure that any SSO federation can be used. In addition, role-based access control can be driven by the group information in the authentication system, such as Active Directory groups.

- *Encryption* – CASB+ provides encryption capabilities, at the field-level, file attachments and downloaded content.

- *Web Security* – cloud activity can be streamed or sent from a web security solution such as Palo Alto Networks next generation firewall, Forcepoint or Symantec. CASB+ proxies are also capable of chaining internet access. Unsanctioned clouds can be controlled by generating configurations compatible with web security solutions.

- *Application Firewalls* – CASB+ integrates with several application firewalls, such as F5.

- *DLP* – CASB+ provides a built-in DLP engine. Policies can be layered, prioritized, activated/deactivated and run on data (in motion or historical), as well as user activity. It also integrates with third party DLP solutions using ICAP-based integration. Remediation actions include quarantine, encrypt, delete, alert the user, remove public links, remove collaboration, and more.

- *User and Entity Behavior Analytics (UEBA)* – CASB+ provides UEBA functionality out of the box. User activity is gathered using inline activity capture and API-based queries. Easy-to-use, interactive analytics make it easy to visualize the behavioral patterns at a high-level and then drill down to specifics for details or forensics. Unusual activity or anomalies across clouds is also determined using machine learning algorithms.

- *SIEM integration* – CASB+ provides a turn-key integration with any SIEM, based on the JSON format. By using the CipherCloud SIEM agent, which can be installed within customer's network, the customer's SIEM can receive activity from CipherCloud CASB+ without requiring additional firewall rules for inbound traffic.

- *Administration* – CASB+ provides a unified management console which offers visibility, control, compliance and protection controls in a single pane of glass. Multiple clouds can be easily on-boarded in several protection modes. All the users, clouds and resources can be viewed in this user interface.

CipherCloud CASB+ supports compliance with HIPAA, GDPR, PCI, PII, and others.

STRENGTHS

- CipherCloud CASB+ is available in all deployment options, cloud, on-premises, or as a hybrid deployment. This makes it attractive for customers with different deployment requirements.

- CipherCloud provides end-to-end encryption and full tokenization support for all leading applications, such as SAP, Salesforce, ServiceNow, Google Drive, Box, Dropbox, Office 365 and others.

- Native device management can completely control devices that handle sensitive encrypted data and track all movement of files, as well as provide real-time revocation features.

- CipherCloud CASB+ provides UEBA functionality out of the box.

- CipherCloud CASB+ is attractively priced and highly affordable even for smaller organizations.

WEAKNESSES

- CipherCloud does not have its own antimalware technology or threat intelligence network, relying instead on a partnership with BitDefender for AV/AM and third party threat intelligence feeds.

- CipherCloud DLP policy definitions are rather basic.

- CipherCloud is still best known for its encryption technology, but needs to build great awareness for its CASB solution.

SPECIALISTS

PROOFPOINT

892 Ross Drive
Sunnyvale, CA 94089
www.proofpoint.com

Proofpoint is a next-generation cybersecurity company protecting people, data, and brands from advanced threats and compliance risks. The company delivers solutions for email and cloud app security, data loss prevention, privacy protection, email encryption, eDiscovery, and email archiving. Proofpoint is publicly traded.

SOLUTIONS

Proofpoint protects cloud applications and data through a family of solutions which includes:

TAP SaaS Defense – offers threat monitoring for Microsoft Office 365 and Google G Suite. It provides detection and isolation of malicious files (for data in motion), as well as forensics. It also helps identify at-risk users and offers account compromise detection for Microsoft Office 365.

Cloud Account Defense (CAD) – protects organizations from Microsoft Office 365 account compromise. It allows organizations to detect, investigate and defend against unauthorized access to sensitive data and accounts. It provides detection and isolation of malicious files (for data at rest and in motion), as well as forensics. It also provides account compromise detection, forensics, and response actions. CAD supports policy-based login control and geo-fencing, as well as integration with SIEM solutions.

Cloud App Security Broker (CASB) – is Proofpoint's CASB solution which protects against account compromise, malicious files, data loss and compliance risks in cloud apps, such as Microsoft Office 365, Google's G Suite, Box, Salesforce and more. It is a cloud-based solution which supports all operation modes (i.e. API, and Proxy). It supports the following functionality:

- *Cloud Application and Shadow IT* – Proofpoint CASB discovers cloud services by retrieving and processing logs from firewalls and web proxies. It catalogs thousands of applications and categorizes these services into 20+ categories. The risk scoring is customizable based on customer requirements. The product also discovers and assigns a severity score to third-party apps and scripts based on permission level, vendor trust, application trust and other insights curated via threat research. Proofpoint CASB can generate alerts and notify admins based on app severity, type, and category. In addition, it can revoke third party apps manually or automatically via policies.

- *Malware detection* – is provided through Proofpoint's advanced threat detection platform. It helps detect and isolate malicious files with malware or phishing URLs using a blend of hash checking and sandboxing technologies.

- *Threat intelligence feeds* – Proofpoint leverages its own threat intelligence as well as third party feeds. To detect account compromise, it combines contextual data (e.g. user device) and user behavior analytics with emerging threat intel (e.g. IP reputation check).

- *Authentication and Single Sign-on* – Proofpoint CASB supports SAML and can integrate with OKTA, OneLogin, Ping, ADFS, and others. It supports step-up authentication based on multiple risk vectors (e.g. network, device, user behavior, and more).

- *Encryption* – file level encryption is available via proxy.

- *Web Security* – Proofpoint supports standard web traffic log formats (CEF, KVP, LEEF, etc.), which can be exported from most proxy/web gateway products. Custom log formats are also supported.

- *DLP* – Proofpoint CASB integrates Proofpoint's own DLP technology and extends DLP capabilities from inbound/outbound email and on-premises data repositories to cloud apps including cloud storage, internal email and mailboxes. Flexible custom rules allow organizations to build their own DLP policies to control how your data is sent, shared and downloaded. Proofpoint DLP offers built-in classifiers for compliance with PCI, PII, HIPAA, GDPR, and others.

- *UEBA* – Proofpoint combines contextual data (e.g. user device, location, login time) and user behavior analytics (anomalies based on rarity, volume and velocity) with rich global threats intel for access control.

- *Administration* – is provided through an easy-to-use console with drill-down dashboard and reporting capabilities as well as fine-grained forensics details. Forensics provide visibility into at-risk users and account compromise.

STRENGTHS

- Proofpoint CASB offers a people-centric security architecture, which focuses on protecting users of sanctioned apps against email and cloud native threats, as well as data loss.

- Proofpoint provides advanced malware detection and isolation based on its own technology and threat intelligence.

- Proofpoint CASB provides compromised account detection, forensics and response actions.

- Proofpoint cloud security solutions provide strong threat correlation across email and cloud applications.

- Proofpoint cloud security solutions benefit from unified DLP detection across email, cloud apps and on-premises data repositories.

- Proofpoint CASB provides discovery, risk scoring and automated control of third-party add-on apps.

- Proofpoint CASB is attractively priced, compared to many competing solutions.

WEAKNESSES

- Proofpoint CASB could broaden its range of application coverage with the inclusion of more SaaS and IaaS APIs.

- Shadow IT discovery could be improved and expanded.

- Proofpoint currently provides only file level encryption. The vendor is working to add field-level encryption.

- Proofpoint solutions are best known in North America. The company is investing to improve its international presence.

PALO ALTO NETWORKS

3000 Tannery Way,
Santa Clara, CA 95054
www.paloaltonetworks.com

Palo Alto Networks, founded in 2005, is well known for its next-generation firewall solutions. The company covers a wide range of network security functions, including advanced threat protection, firewall, IDS/IPS, and URL filtering. The company recently acquired RedLock, a provider of AI-driven security analytics which provides visibility, threat detection and rapid response across public cloud environments. Palo Alto Networks is publicly traded.

SOLUTIONS

Palo Alto Networks provides CASB capabilities through its **Security Operating Platform**, which supports safe adoption of cloud applications by automating threat identification and prevention across cloud, network, servers, and endpoints with data-driven approach and advanced analytics. Palo Alto Network's CASB offering provides inline capabilities delivered as cloud services, virtualized appliances or hardware appliances. It also offers API-based capabilities as a cloud service.

CASB functionality is delivered through two solutions:

- **GlobalProtect Cloud Service** – offers inline CASB functionality, which supports forward and reverse proxy modes. The solution allows users to connect to the closest enforcement location seamlessly, where they are protected with a consistent set of SaaS security policies. GlobalProtect Cloud Service also provides: complete visibility of cloud application usage, granular function-level application control, secure SaaS access for managed and unmanaged devices, control to SaaS application based on risk attributes. It also leverages threat intelligence feeds from Palo Alto Network's WildFire platform to prevent known and unknown threats.

- **Aperture** – is as a multi-tenanted cloud service which supports API mode to analyze data in sanctioned software-as-a-service (SaaS) applications and performs policy-driven risk analysis to automatically remediate risks. Aperture's key capabilities include: data classification (based on pre-defined data patterns and machine learning), risk discovery, DLP and compliance enablement, user anomaly and activity monitoring, prevention of malware (including zero-day malware), and control of third party apps available through SaaS marketplaces.

Palo Alto Networks CASB solutions support the following functionality:

- *Cloud Application and Shadow IT* – is provided through continuous monitoring and reporting to obtain a complete risk assessment of sanctioned and unsanctioned SaaS apps. Detailed reporting identifies apps by category, sessions, bytes transferred, and more. The monitoring capability is further extended by the API mode via Aperture that provides deeper context into sanctioned SaaS app activity for users who are on-premises or off-premises.

- *Malware detection* – is provided through Palo Alto Networks Threat Intelligence Cloud, WildFire, a global distributed sensor system focused on identifying and preventing unknown threats.

- *Threat Intelligence feeds* – is based on WildFire threat feeds as well as third party threat feeds.

- *Authentication and Single Sign-on* – Palo Alto Networks supports Okta, Ping, Onelogin, Centrify, Duo or and other solutions that support SAML 2.0.

- *DLP* – Aperture delivers cloud-based inline DLP capabilities through integration with Palo Alto Network's next generation firewalls or the GlobalProtect Cloud Service. It supports pre-defined data patterns, regular expressions and machine learning based data classification. DLP can be enforced for data in motion and data at rest.

- *UEBA* – Palo Alto Networks offers two analytics capabilities for SaaS applications: Magnifier Behavioral Analytics, a cloud-based app which identifies targeted attacks, malicious insiders and compromised endpoints, and Aperture natively provides heuristic-based user behavior monitoring and alerting.

- *SIEM integration* – Palo Alto Networks Integrates with third-party SIEM vendors such as Splunk, QRadar and others. It also integrates with other CASB vendors (e.g. Netskope, McAfee, and others) and other security solutions by forwarding any logging events via syslog and API.

- *Administration* – the GlobalProtect Cloud Service inline CASB solution, has a centralized management interface across all sites, branches and headquarters. The API-based Aperture solution has an administrative interface is delivered directly from the cloud.

STRENGTHS

- Palo Alto Networks offers a platform approach to CASB, which builds on existing next generation firewall investments and provides protection for on-premises and cloud applications.

- Palo Alto Networks delivers strong threat intelligence through its WildFire platform, which is integrated in the pricing of the Aperture CASB solution.

- Palo Alto Networks offers advanced DLP with Machine Learning, which improves ease of use and helps to reduce false positive and false negatives.

- Palo Alto Network's Aperture is attractively priced for customers of all sizes.

WEAKNESSES

- Palo Alto Networks does not provide technology to encrypt and tokenize data in SaaS applications. The vendor is addressing this requirement through upcoming rights management features, mainly through integration with Microsoft Azure Information Protection (AIP).

- Palo Alto Networks currently provides separate, overlapping behavioral analytics functionality through Aperture and the Magnifier Behavioral Analytics engine. The vendor is working to harmonize this in future releases.

- Palo Alto Networks currently offers SaaS visibility from two different consoles – GlobalProtect Cloud Service for inline CASB, and Aperture for API-based CASB. The vendor is working to provide consolidated reporting through its Palo Alto Networks reporting service.

- Palo Alto Networks offers a rich set of capabilities through its GlobalProtect Cloud Service and Aperture CASB solutions, however integrating the two correctly in a way that addresses all CASB requirements can be somewhat complex, and requires careful planning.

MICROSOFT

1 Microsoft Way
Redmond, WA 98052
www.microsoft.com

Microsoft provides a broad range of products and services for businesses and consumers, with an extensive portfolio of solutions for office productivity, messaging, collaboration, and more.

SOLUTIONS

Microsoft Cloud App Security (MCAS) is based on the 2015 acquisition of Adallom, an early developer of cloud-based identity and data protection security. MCAS is available as part of Microsoft's Enterprise + Security (EMS) suite, which allows it to integrate with other key identity and security solutions including Azure Active Directory, Microsoft Advanced Threat Analytics, Microsoft Intune and Azure Information Protection. It also integrates deeply with Office 365 for better email security management. MCAS is an API based CASB solution, but can be complemented with **Conditional Access Control** which delivers a reverse proxy that integrates with Azure AD conditional access. By integrating natively with Azure AD, it can support any app configured with SAML single sign-on in Azure AD, including: AWS, Box, Dropbox, G Suite, Salesforce, Slack, and many more.

MCAS delivers the following functionality:

- *Data retention and compliance* – helps organizations control cloud applications, through tools that help uncover shadow IT, assess risks, enforce policies and investigate activities, auditing capabilities, and granular controls over sensitive data. It ties into Microsoft's extensive compliance with a wide set of national, regional and industry-specific requirements concerning the collection and use of data.

- *Cloud Discovery* – uses traffic logs to dynamically discover and analyze the cloud apps in use within an organization.

- *Sanctioning and un-sanctioning apps* – it helps organizations sanction or un-sanction apps through the use of a Cloud app catalog. Microsoft provides an extensive catalog of over 16,000 cloud apps that are ranked and scored based on industry standards. Organizations can further refine this based on regulatory certifications, industry standards, and best practices.

- *App connectors* – use APIs from cloud application providers to integrate MCAS with other cloud apps, and extend control and protection over those apps. It can also enforce policies, detect threats, and provide governance for resolving issues.

- *Conditional Access App Control protection* – uses a reverse proxy architecture to gain real-time visibility and control over access to and activities performed in the cloud. It helps avoid

data leaks by blocking risky downloads, set rules to automatically encrypt cloud data, gain visibility of unprotected endpoints, and control access from risky IP addresses.

- *Policy control* – help organizations define user behavior in the cloud. Policies can be set to detect risky behavior, violations, or suspicious data points and activities. Policies can also be used to integrate remediation processes for more comprehensive risk mitigation.

MCAS support a wide range of certifications, including: EU-U.S. Privacy Shield, HIPAA/HITECH, ISO/IEC 27001, SOC 1, SOC 2 Type 2 Reports, UK G-Cloud, and others.

MCAS is available for purchase as a standalone subscription, or as a part of the Microsoft Mobility + Security E5 plan.

STRENGTHS

- MCAS is a great solution for organizations that are deploying a Microsoft services infrastructure including Azure Active Directory, Office 365, Microsoft Advanced Threat Analytics, Microsoft Intune, Azure Information Protection, and more, as it integrates fully with these solutions to deliver a unified approach to cloud security and policy management.

- MCAS has access to a large catalog of sanctioned applications, which customers can further refine to best meet their needs.

- MCAS allows policy control to be integrated with remediation processes to enable, faster more secure risk mitigation.

- Microsoft has been investing heavily to all aspects of security, threat protection, compliance and identity management, and is now delivering an impressive portfolio of solutions.

WEAKNESSES

- MCAS works best in a fully deployed Microsoft security environment, which may not be suitable for organizations with heterogeneous environments not based primarily on Microsoft solutions.

- While MCAS benefits from a complete security ecosystem comprising multiple Microsoft technologies (e.g. Azure Active Directory, Microsoft Advanced Threat Analytics, Microsoft Intune, Azure Information Protection, and more) integrating all these components correctly and maintaining them fully integrated throughout Microsoft's continuous upgrade cycle can be daunting for many organizations.

- To get the full benefits of MCAS, organizations will need to deploy the Microsoft Mobility + Security E5 plan, which is the more expensive Microsoft enterprise security plan.

- Microsoft customers we spoke to, often indicated that Microsoft's customer support organization is not sufficiently knowledgeable about security issues.

CISCO

170 West Tasman Dr.
San Jose, CA 95134
www.cisco.com

Cisco is a leading vendor of Internet communication and security technology. In 2016, Cisco acquired CASB technology firm, CloudLock. In August 2018, Cisco announced the acquisition of Duo Security, a provider of unified access security and multi-factor authentication. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), which is made up of leading threat researchers.

SOLUTIONS

Cisco Cloudlock is a cloud-based API-only CASB solution. Since its acquisition in 2016, Cisco has been integrating Cloudlock with its broader security portfolio, which includes Cisco AMP for Endpoints, AMP for Networks (NGFW), email and web security, and OpenDNS. Cloudlock helps secure customer SaaS applications, such as Google Drive, Salesforce, and Box, as well as the applications that customers build, such as IaaS and PaaS platforms. Cloudlock is designed as a collection of RESTful, API-based microservices which makes it easy to extend to integrate customer applications on any platform. Cisco is in the process of integrating trusted identity awareness technology from its Duo Security acquisition with its Cloudlock CASB solution.

The Cloudlock cybersecurity platform consists of four key components:

- *Data Security & Compliance* – protects organizations against data breaches in cloud environments and apps through a configurable Cloud Data Loss Prevention (DLP) engine, which features out-of-the-box policies and a wide range of automated, policy-driven response actions such as encryption and quarantine, and end-user notifications.

- *Threat Protection* – defends against account compromises with cross-platform User and Entity Behavior Analytics (UEBA) for SaaS, IaaS, PaaS, and IDaaS environments. It integrates with IDaaS tools, such as Okta, and connects to log management, SIEM, ticketing systems and more. It uses machine learning to detect anomalies in account usage, as well as identifying actions outside of whitelisted countries or across unusual distances.

- *Application Discovery & Control* – the Cisco Cloudlock Apps Firewall addresses Shadow IT by discovering and controlling malicious cloud apps connected to corporate environments. It provides a large crowd-sourced security solution to help identify individual app risk, as well as relies on Cisco's Community Trust Rating to understand which new apps are risky or not, educate users on risky apps, and removing high-risk apps from the environment.

- *Integration and Orchestration* – the Cisco Cloudlock Cybersecurity Orchestrator is an API-driven solution that aggregates data feeds across existing IT infrastructure to enrich security intelligence and harmonize data protection across on-premises and cloud environments for improved insight and control.

Cloudlock has achieved security qualifications for FedRAMP, SSAE16 – SOC 2 Type 2 Certified, SOC 3 Certified, TRUSTe, Cloud Security Alliance Security, Trust & Assurance Registry (STAR).

Cisco prices Cloud Security based on the number of applications, and the number of users. Cloudlock is available as part of two licensing scenarios: a security package that includes Cisco Cloudlock and Cisco Umbrella (including DNS and Selective Proxy Layer Security, roaming client protection, and Cisco Advanced Malware Protection – AMP); or as part of Cisco's Security Enterprise License Agreement (Security ELA), where it is packaged with a number of other Cisco Security solutions, such as email security, NGFW and Cisco Stealthwatch for network security.

STRENGTHS

- Cisco Cloudlock is part of a Cisco security broad security portfolio, which encompasses threat intelligence, endpoint security, network firewall security, email and web security, and more.

- Cisco Cloudlock is easy to deploy and get up and running quickly even in fairly complex cloud environments.

- Cisco Cloudlock supports all applications on Salesforce's AppExchange, applications on Okta and OneLogin marketplaces.

- Cisco's developer API allows customers to easily extend it to their own custom applications running in cloud or on-premises.

WEAKNESSES

- Cisco Cloudlock is an API-only CASB solution and as such may not be appropriate for customers needing broader insight and access into non-API based applications.

- The Cisco Cloudlock shadow IT discovery and control functionality relies mostly on crowdsourced application information and Cisco's own Community Trust Rating database which may not provide as extensive visibility into risky applications as solutions available from competing vendors.

- Cisco Cloudlock lacks ICAP integration with on-premises DLP solutions.

- Cisco Cloudlock is not available as a standalone solution but comes packaged as part of a broader suite of Cisco services, which may or may not fit the needs of customers deploying heterogeneous security infrastructures.

- While Cisco acquired Cloudlock in 2016, the vendor has been somewhat slow to innovate on its initial purchase beyond integration with the existing Cisco security portfolio, despite growing market demand for feature-rich CASB solutions.

THE RADICATI GROUP, INC.
http://www.radicati.com

The Radicati Group, Inc. is a leading Market Research Firm specializing in emerging IT technologies. The company provides detailed market size, installed base and forecast information on a worldwide basis, as well as detailed country breakouts, in all areas of:

- **Email**
- **Security**
- **Instant Messaging**
- **Unified Communications**
- **Identity Management**
- **Web Technologies**

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim. The Radicati Group, Inc. was founded in 1993.

Consulting Services:

The Radicati Group, Inc. provides the following Consulting Services:

- Management Consulting
- Whitepapers
- Strategic Business Planning
- Product Selection Advice
- TCO/ROI Analysis

  Multi-Client Studies

To learn more about our reports and services, please visit our website at www.radicati.com.

MARKET RESEARCH PUBLICATIONS

The Radicati Group, Inc. develops in-depth market analysis studies covering market size, installed base, industry trends and competition. Current and upcoming publications include:

Currently Released:

Title	Released	Price*
Microsoft SharePoint Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Corporate Web Security Market, 2018-2022	Jun. 2018	$3,000.00
Email Market, 2018-2022	Jun. 2018	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Cloud Business Email Market, 2018-2022	Jun. 2018	$3,000.00
Information Archiving Market, 2018-2022	Mar. 2018	$3,000.00
Unified Endpoint Management Market, 2018-2022	Mar. 2018	$3,000.00
Advanced Threat Protection Market, 2018-2022	Mar. 2018	$3,000.00
Email Statistics Report, 2018-2022	Mar. 2018	$3,000.00
Social Networking Statistics Report, 2018-2022	Feb. 2018	$3,000.00
Instant Messaging Statistics Report, 2018-2022	Feb. 2018	$3,000.00
Mobile Statistics Report, 2018-2022	Jan. 2018	$3,000.00

*** Discounted by $500 if purchased by credit card.**

Upcoming Publications:

Title	To Be Released	Price*
Endpoint Security Market, 2018-2022	Nov. 2018	$3,000.00
Secure Email Gateway Market, 2018-2022	Nov. 2018	$3,000.00
Enterprise Data Loss Prevention Market, 2018-2022	Nov. 2018	$3,000.00
Cloud Access Security Broker Market, 2018-2022	Nov. 2018	$3,000.00

*** Discounted by $500 if purchased by credit card.**

All Radicati Group reports are available online at http://www.radicati.com**.**

