Critical Capabilities for Content Collaboration Platforms

Published: 12 September 2017   **ID:** G00320955
Analyst(s): Karen A. Hobert, Monica Basso, Michael Woodbridge

Summary

The evolution of EFSS into content collaboration platforms creates new use cases. Application leaders can choose among these products to support use cases such as workforce productivity, extended collaboration, data infrastructure modernization, document governance and lightweight workflow.

Overview

Key Findings

The market evolution from enterprise file sync and sharing (EFSS) to services-led platform intensifies the content collaboration platform (CCP) role in digital workplace transformation, making a CCP choice more strategic and less tactical.

While inconsistent across the market, most CCPs offer basic content services such as document and metadata management, analytics, search, retention and lightweight workflow.

Assumptions that CCPs can substitute backup or high availability/disaster recovery (HA/DR) systems may expose organizations to significant risk in the event of an attack or data center disaster.

CCP platform APIs, native integrations and connectors enable the creation of highly tailored client solutions, even though adoption is still limited in the market.

Recommendations

For application leaders tasked with enabling digital transformation initiatives in their workplaces:

Develop strategies that leverage CCP capabilities and integration to deliver more seamless productivity and team collaboration experiences, by evaluating current content collaboration use cases and processes. This will align CCP deployments with digital transformation initiatives for workforce productivity and extended collaboration.

Use a CCP as an alternative to niche applications such as virtual data rooms (VDRs), and work with risk and data managers to evaluate compliance and data governance capabilities. This may expand value of the CCP to new workloads and use cases, particularly in regulated sectors such as legal and finance.

Conduct prototype tests and proofs of concept to fully assess the integration capabilities of a particular CCP. These will help to determine whether the CCP can support current and future requirements, particularly the user interfaces and usability requirements that underpin infrastructure modernization use cases.

Strategic Planning Assumption

By 2020, 80% of large and midsize organizations in mature regions will have deployed one or more content collaboration platform (CCP) products to implement a content productivity and collaboration strategy.

What You Need to Know

Application leaders are challenged with the objective of enabling digital workplace transformation. Business users' demands for rapid innovation, coupled with the shift to cloud and mobile use cases, are disruptive to traditional IT choices. Providing new and more agile ways to procure services and implement solutions includes rethinking approaches to the delivery of content services. Yet, the need for good governance, data management and regulatory compliance is still present.

A content collaboration platform (CCP) is a core enabling component of digital workplace transformation. Organizations consider CCPs a priority for enabling better productivity, external document sharing, team collaboration, internal/operational efficiencies, and data infrastructure modernization.

This market has moved beyond the traditional requirements for enterprise file synchronization and sharing (EFSS) and mobility, to support users' productivity and team collaboration — more complex use-case scenarios are developing around extended collaboration and lightweight content workflow. Customers' needs have moved beyond traditional EFSS use cases to ones that play a more strategic role in the use and sharing of unstructured content in the digital workplace; so much so that Gartner has renamed the market CCP. The extended list of critical capabilities shown in this research demonstrates these expanded digital workplace and user needs.

This report considers CCP products from 13 vendors that qualified for inclusion in the 2017 "Magic Quadrant for Content Collaboration Platforms." It assesses and scores products across nine critical capabilities, through the following five common use cases:

Workforce productivity — Enabling general-purpose, nonroutine working experiences on documents, from different locations and across multiple devices. It includes enhanced syncing and access capabilities. Content creation is often a key requirement for productivity.

Extended collaboration — Supporting file sharing between people or in a team, inside and outside of the organization, with support for commenting, versioning, notification, data protection, and rights management capabilities.

Infrastructure modernization — Rationalizing legacy data infrastructure, replacing file and FTP servers by moving content to the cloud. Key requirements include controls for data residency and backup/recovery automation.

Centralized content protection — Supplying a locked-down document collaboration environment with support for policy enforcement, data protection, audit trail, e-discovery, and data residency.

Lightweight workflow — Enabling automation of simple tasks related to document flows, involving document management and team collaboration capabilities.
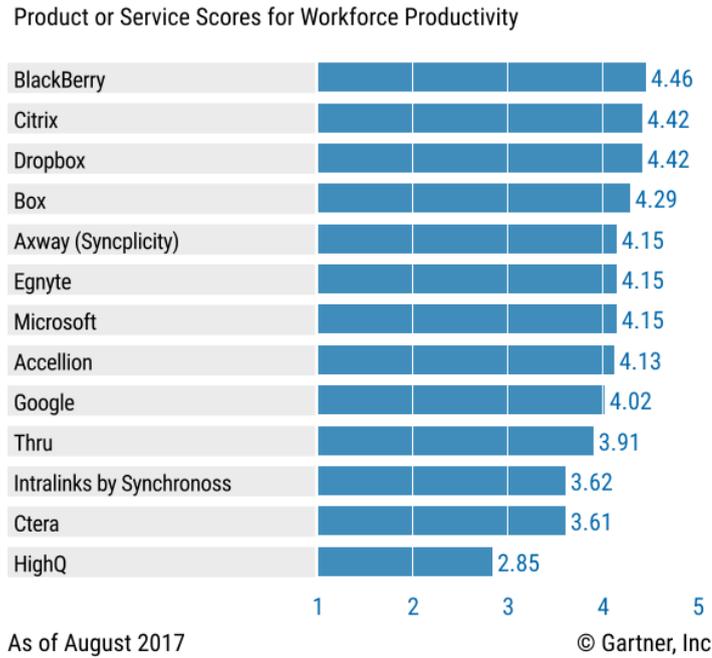
This report provides a set of interactive, customizable online charts, arranged by use case. Each use case shows Gartner's weighted rating of the critical capabilities and the ranked scoring of each of the 13 vendor products, showing how well each product meets those capabilities for a given use case. The relative weights of the critical capabilities can be adjusted to meet your own priorities.

This Critical Capabilities report is a companion to Gartner's "Magic Quadrant for Content Collaboration Platforms." Using the report will enable application leaders to identify the most appropriate CCP products, out of the Magic Quadrant selection, to match their own use cases and feature requirements.
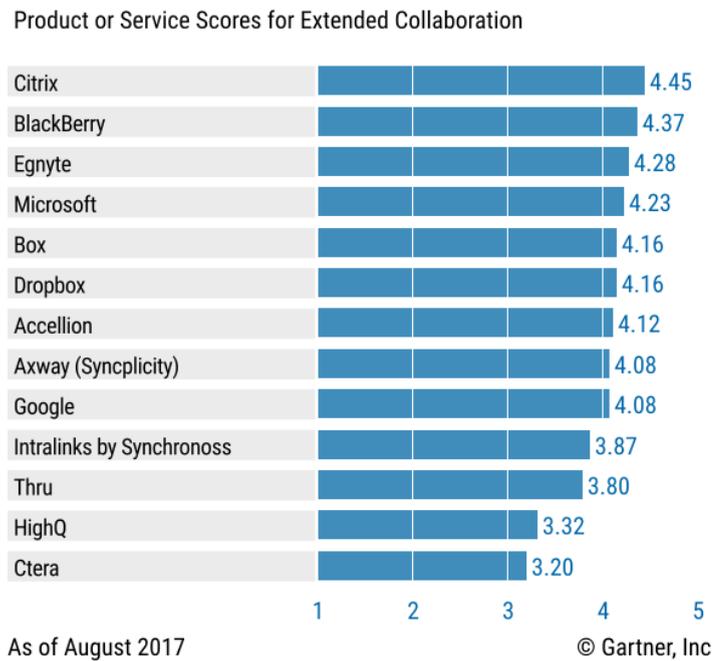
Analysis

Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for the Workforce Productivity Use Case

Product or Service Scores for Workforce Productivity
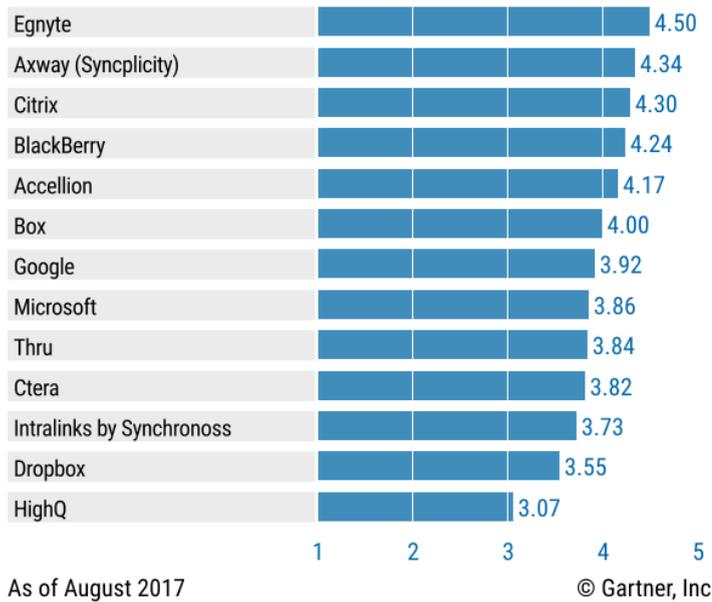
Vendor	Score
BlackBerry	4.46
Citrix	4.42
Dropbox	4.42
Box	4.29
Axway (Syncplicity)	4.15
Egnyte	4.15
Microsoft	4.15
Accellion	4.13
Google	4.02
Thru	3.91
Intralinks by Synchronoss	3.62
Ctera	3.61
HighQ	2.85

As of August 2017

© Gartner, Inc

Figure 2. Vendors' Product Scores for the Extended Collaboration Use Case

Product or Service Scores for Extended Collaboration

Vendor	Score
Citrix	4.45
BlackBerry	4.37
Egnyte	4.28
Microsoft	4.23
Box	4.16
Dropbox	4.16
Accellion	4.12
Axway (Syncplicity)	4.08
Google	4.08
Intralinks by Synchronoss	3.87
Thru	3.80
HighQ	3.32
Ctera	3.20

As of August 2017

© Gartner, Inc

Figure 3. Vendors' Product Scores for the Infrastructure Modernization Use Case

Product or Service Scores for Infrastructure Modernization

Vendor	Score
Egnyte	4.50
Axway (Syncplicity)	4.34
Citrix	4.30
BlackBerry	4.24
Accellion	4.17
Box	4.00
Google	3.92
Microsoft	3.86
Thru	3.84
Ctera	3.82
Intralinks by Synchronoss	3.73
Dropbox	3.55
HighQ	3.07

As of August 2017 © Gartner, Inc

Figure 4. Vendors' Product Scores for the Centralized Content Protection Use Case

Product or Service Scores for Centralized Content Protection

Vendor	Score
BlackBerry	4.45
Citrix	4.36
Egnyte	4.31
Box	4.28
Axway (Syncplicity)	4.27
Microsoft	4.22
Accellion	4.19
Dropbox	4.19
Thru	3.97
Google	3.95
Intralinks by Synchronoss	3.75
Ctera	3.54
HighQ	3.11

As of August 2017 © Gartner, Inc
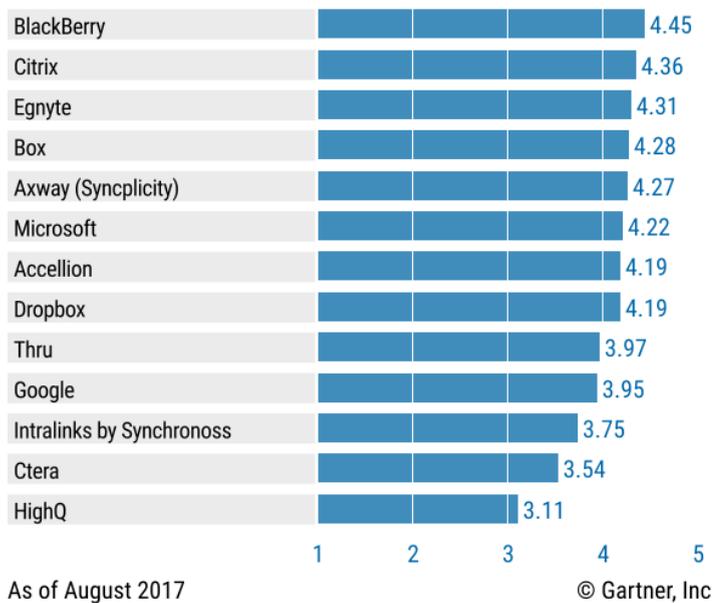
Figure 5. Vendors' Product Scores for the Lightweight Workflow Use Case

Product or Service Scores for Lightweight Workflow

Vendor	Score
Egnyte	4.44
BlackBerry	4.43
Box	4.37
Citrix	4.31
Axway (Syncplicity)	4.13
Dropbox	4.09
Microsoft	3.92
Google	3.91
Accellion	3.89
Thru	3.85
Intralinks by Synchronoss	3.83
Ctera	3.60
HighQ	2.90

As of August 2017 © Gartner, Inc
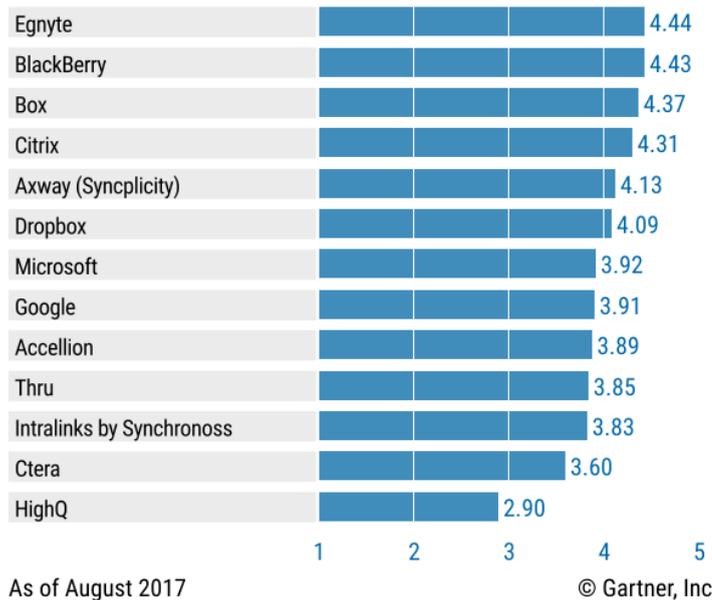
Vendors

Accellion

Accellion's CCP product, kiteworks, supports back-end and bidirectional integration, centralized security and management aimed at compliance across the file-sharing ecosystem. The user interface (UI) supports consistent experience across mobile, browser, email and desktop clients. A technical partnership with Microsoft has resulted in greater integration of kiteworks with Outlook, SharePoint, OneDrive for Business and Office 365 interfaces, improving usability and seamless user productivity experience.

The kiteworks architecture employs a multitier model that separates the web, application and data layers. The product can be deployed on-premises, as a private cloud (either on-premises or hosted via Azure or Amazon Web Services [AWS], including the Federal Risk and Authorization Management Program [FedRAMP] cloud instance), as a hybrid cloud (mixing on-premises and hosted), or as a public cloud. The hybrid model can combine the on-premises component with public and private cloud services. This architecture is conducive to bidirectional integration with enterprise applications and workflows.

The kiteworks' content platform has enterprise-grade RESTful APIs and software development kits (SDKs) for developers to build secure apps and custom integrations. A mobile container managed by IT administrators allows content to be kept securely on a mobile device, while restricting editing, forwarding and other users' actions.

Accellion is a good fit for organizations that prioritize on secure and centrally managed access to a variety of corporate data repositories; and that require customized apps (mobile, web or desktop) to support document-centric business workflows while ensuring data protection and compliance, particularly in regulated markets.

Axway (Syncplicity)

Axway Syncplicity offers a hybrid cloud content platform with user productivity and collaboration, prioritizing on data infrastructure modernization, security and data governance. In addition to Syncplicity for content collaboration, Axway also sells the Amplify platform, including managed file transfer (MFT), mobile application development (Appcelerator), and API management (from creation, management, governance, consumerization, and analytics). Combined, these products offer an extensive hybrid cloud content platform to address a range of scenarios for digital transformation, IT modernization, data governance and digital workplace.

Axway Syncplicity provides connectors to integrate with on-premises network-attached storage arrays, object storage APIs, and content repositories such as Microsoft SharePoint and OpenText Documentum. With DataHub, customers can migrate, copy and sync content from existing enterprise repositories to the Axway Syncplicity one. SyncDrive enables users to access files through their devices regardless of the folder or file sizes.

Axway Syncplicity can be deployed in public, hybrid or private cloud, or on-premises. A policy-driven storage model allows customers to store data in different locations. This hybrid architecture can be built mixing Axway Syncplicity public cloud storage in the U.S. and EU (based on AWS S3), private cloud storage and on-premises storage. In addition to content collaboration, the Axway Syncplicity platform can replace legacy storage, file shares and network drives.

Other capabilities include data governance with fine-grained group security and IT administrative policies. Axway Syncplicity offers advanced security features, including native digital rights management (DRM) with policies, customer key management and geofencing; and compliance certifications, such as for FedRAMP, FERPA, FISMA, HIPAA and ITAR.

A real-time document backup mechanism is enabled by a multifolder synchronization feature. Rich platform APIs enable customers to develop custom functionality. Axway Syncplicity is a good fit for large enterprises that want to enable productivity and team collaboration in flexible deployment options (on-premises, cloud or hybrid) without forcing the adoption of a public cloud model. This vendor is also a match for customers who prefer to modernize their existing data infrastructure through hybrid architecture that integrates with and manages corporate systems and new cloud services. It is a suitable choice for replacing or optimizing traditional storage with cloud options, and legacy FTP and backup services with modern synchronization and sharing mechanisms — all while meeting security and compliance requirements.

BlackBerry

BlackBerry Workspaces focuses on enhanced secure mobile productivity and content collaboration. While it is available as a stand-alone product, more often, customers purchase it through a service bundle or on-premises deployment within the BlackBerry Enterprise Mobility Suite — Content Edition. Workspaces integrates with BlackBerry Unified Endpoint Manager and BlackBerry Dynamics, enabling secure content sharing between BlackBerry apps (e.g., Work), BlackBerry independent software vendor (ISV) partner apps and multiple custom enterprise apps.

BlackBerry Workspaces can be deployed on-premises, in a public cloud or in a private cloud, with multiple hybrid options through a virtual appliance, and integrated with corporate applications through APIs. Enhanced capabilities include digital rights management, secure viewers, document editing, file-level comments and annotations. In addition, BlackBerry Workspaces supports cross-platform collaboration and can be deployed on the BlackBerry Dynamics platform environment. A

full set of APIs and SDKs enable organizations and developers to integrate BlackBerry services into custom applications and workflows, and to build brand-new applications. Third-party apps can upload files, folder structures and permissions into a repository.

BlackBerry Workspaces is a good fit for midsize and large organizations in regulated or IPR-sensitive sectors. Those organizations typically want to enable mobile worker productivity and secure document collaboration for internal and extended teams that need to work with sensitive information in a protected and managed virtual workspace. BlackBerry is suitable for high-security use cases involving externalization and mobility.

Box

Box offers a cloud-based CCP, with file storage, synchronization and sharing at the core. Box aims to be the central content platform for any type of content, providing capabilities, controls and APIs to enable multiple use cases. Box is available in the public cloud only, and it is implemented in its own data centers in the U.S., or through local data centers of AWS, Microsoft Azure and IBM in other regions. Content can be stored in these regions, but customer metadata is always stored in the U.S. data center.

Box supports user productivity and collaboration across any device — integrating with Microsoft Office 365 and Google G Suite. Enhanced capabilities for content streaming, real-time editing, machine learning and analytics are also available. Box provides rich security, compliance and administrative capabilities, such as cloud data protection and governance capabilities, including encryption key management of customers' content stored in the cloud (Box KeySafe) and flexible content geolocation technology (Box Zones) for storage. Box is developing, in conjunction with IBM, a content workflow automation environment. Extensive APIs for content, metadata and collaboration function access, and an SDK environment, enable application integration, UI customization and custom solution development.

Box is a good fit for public-cloud-friendly organizations prioritizing digital workplace transformation and business process automation strategies. It is a viable option for stand-alone use cases, particularly when external-facing collaboration scenarios are involved.

Citrix

ShareFile is Citrix's CCP product, with a value proposition that is focused on user productivity, collaboration, infrastructure modernization, security, compliance and integration. ShareFile supports hybrid architectures with over 60% of its deployments being implemented in this way. Citrix extends its collaboration and productivity features to a range of other repositories including file shares, on-premises content services platforms (CSPs) and other cloud services. Connectors to these services are either native to ShareFile or provided by third parties.

ShareFile is well-integrated with other Citrix products, particularly:

    XenDesktop (desktop virtualization) and XenApp (app virtualization) for virtual clients and end-user computing

    Podio for social collaboration and project management

    NetScaler for mobile and web application delivery control

ShareFile is a good fit for a broad spectrum of collaboration and productivity-based end-user scenarios, and its focus on security and compliance make it a good consideration for regulated industries. Citrix is often seen in shortlists for VDR requirements.

Ctera

Ctera's CCP offering is based on an underlying product known as the Ctera Enterprise File Services Platform. It provides enterprise cloud file management capabilities with an emphasis on security and data protection. This software component provides secure remote file sharing, collaboration and storage management features, such as integrated backup, utilizing either a dedicated cloud storage service (hosted in Microsoft Azure or AWS) or on-premises data centers.

Ctera can be deployed completely on-premises, in hybrid architectures and also as public cloud through its hosted SaaS version (recently launched). Ctera addresses the challenges of data infrastructure modernization, including protection of corporate boundaries and data migration.

Ctera's solution is also available as a white-label option to be branded and customized according to customers' needs. A focus on file system modernization rather than purely synchronization and share has led Ctera to develop and provide a range of services to assist clients in the migration of their datasets to cloud-based solutions. This includes the ability to map existing file system access control levels to the new cloud-based storage.

Ctera is a good fit for organizations with highly distributed users and offices, and priorities on data privacy or data sovereignty. These organizations are looking to modernize their file storage infrastructure by moving to the cloud while maintaining security and data protection, but also pursuing greater degrees of collaboration.

Dropbox

Dropbox is the best-known provider of cloud file storage and sharing services, with the largest user base for consumer services. Dropbox delivers Dropbox Business, an enterprise-secure content platform for collaboration. Dropbox Business is a full CCP service offering to support individual workers and teams, both inside and outside of the organization. Available as a public cloud service only, Dropbox Business includes storage, file synchronization, sharing, productivity, collaboration, central IT management, and security features. Teams can collaborate in real time with Dropbox Paper, which brings context and conversations to all types of content, from tasks and tables to code, videos and files.

For large-scale deployments, Dropbox provides advanced security and administration features to give the needed visibility and control to manage a collaboration solution companywide. Management features include separation of personal and business data in two connected accounts, and remote wiping of business data from users' devices. The Dropbox Enterprise plan is available for larger organizations that require additional security management and control features.

Dropbox runs a dedicated storage infrastructure for service performance and reliability. Its infrastructure footprint has 10 regional accelerators with 14 points of presence in the U.S., Europe and Asia, granting customers faster data access across the globe. Regional data location is available for EMEA via Dropbox's AWS-based European infrastructure in Germany. The Dropbox platform includes extensive APIs, enabling custom integrations with business applications, content repositories and other clouds, supporting business processes and document workflows. A large developer and partner ecosystem has built thousands of app integrations on top of the Dropbox platform.

Dropbox Business is a good fit for organizations aiming to enable modern file productivity with external parties. Dropbox Business helps organizations to pursue broad user acceptance, particularly when users are familiar with the Dropbox service as a personal tool and accustomed to working with it.

Egnyte

Egnyte Connect is a CCP targeted at supporting digital workplace initiatives, including content collaboration and data infrastructure modernization use cases. The product provides federation capabilities through a single interface to integrate enterprise content from line-of-business applications and other content repositories. It also provides data migration, archiving and centralized management.

Egnyte is available for hybrid scenarios where its functions are enabled for on-premises storage and data repositories or other cloud repositories. Egnyte Connect Desktop provides an integrated experience to users in one app, presenting files from multiple sources, and access to an entire file system in the cloud regardless of hard disk space (Egnyte Drive). It also supports pure cloud deployment.

Egnyte has data centers in the U.S. and Europe. In addition, Egnyte Protect extends this orchestration layer to provide content security and data governance to remote content sources such as Microsoft SharePoint or Windows File Servers. Egnyte's CCP offers APIs at both the user interaction layer and the infrastructure layer supporting both user-centric and IT-centric use cases.

Egnyte is a good fit for organizations that are struggling to get control of the ever-increasing number of content repositories in an organization. Its focus on collaboration and governance, not just for its native repository but also remote sources, is a differentiating aspect of its offering. Organizations for which security, privacy and geographical data residency are important should consider Egnyte, as these areas are of considerable strategic focus for the vendor. In addition, organizations with distributed workforces and remote offices should consider Egnyte for its smart governance of storing and sharing files, and access to files depending on user profile.

Google

Google Drive is a public cloud CCP offering available as a stand-alone product or bundled in G Suite. Google Drive is the central content repository for all productivity, collaboration and communications apps in the suite, including Google Docs, Google Sheets and Google Slides for collaborative document creation. The browser-based G Suite applications introduce a brand-new content creation style for collaborative cloud document creation, authoring and collaboration.

Google Drive integrates with Gmail, Calendar, Docs and other productivity applications. Advanced security includes external sharing controls, audits and alerts on document status changes, information rights management (IRM), data loss prevention (DLP), search (Google Cloud Search), e-discovery (Google Vault), and compliance certifications.

Google has a global infrastructure for fast access to data that can store and serve large files (up to five terabytes) at high speed. New features, such as Drive File Stream, can operate as a network drive without limits on device storage space . Google's worldwide customer support organization, enhanced by distribution partners, grants presence in many countries. Technical specialists, as well as a network of authorized resellers, support customers of all sizes. Small businesses are served through online self-service channels. The CCP platform APIs and SDK enable developers to integrate Google Drive with existing or new business applications. Thousands of apps are available in the Google Marketplace for integration with Google Drive — for example, DocuSign, HelloFax and Jive Software. Google also provides the AppBridge product for enterprise migrations.

Google Drive is a good fit for organizations with a distributed and mobile workforce aiming to enable agile content productivity, team collaboration and collaborative document creation (with Google Docs). Google Drive is attractive for organizations that are prioritizing users' preferences and value for money. It is appropriate for organizations without regional storage constraints and not requiring deep integration with Microsoft Office or other third-party business applications.

HighQ

HighQ Collaborate is a cloud collaboration platform for individual productivity and team collaboration centered on secure file sharing and document management that includes project management tools. Collaborate provides personal and team workspaces to sync and share personal work files or shared folders, accessible through a web interface, native desktop applications and mobile apps. Through a main dashboard, users get an aggregated overview of recent activities, tasks and messages per projects.

HighQ provides one integrated CCP offering for users and teams, embedding core file sharing and document productivity tools. It includes project management and process automation tools; virtual deal rooms; and social interaction and communication features such as wikis, blogs, calendars, activity streams, profiles, messaging and structured data list management.

HighQ implements a private cloud architecture based on its own data centers (located in the U.K., the U.S., Germany, Australia and the United Arab Emirates) hosting its platform. In Asia/Pacific, it can set up a new location hosted by another service provider. For each customer, it deploys a dedicated copy of the application as single tenancy. HighQ provides hybrid file storage, allowing customers to store their files on-premises, but its offering is not fully on-premises.

HighQ addresses concerns of regulated organizations and offers data protection capabilities such as data geolocation, data sovereignty and regional isolation of data centers, through a choice of six existing data center locations or new dedicated ones. It also provides private cloud implementation with hybrid storage, encryption key management and single tenancy for compliance requirements.

HighQ is a good fit for regulated organizations, particularly in the legal and financial sectors, aiming to enable team collaboration and project management among employees and external parties.

Intralinks by Synchronoss

Intralinks' CCP offering is Intralinks VIA, for enterprise-secure content sharing and collaboration with external-facing business processes and sensitive data. Intralinks also traditionally offers Intralinks' Virtual Data Room Edition for specialized use cases, such as VDRs, loan syndication, merger and acquisition (M&A) transactions, private equity fundraising, and clinical trials.

With the acquisition (Synchronoss acquired Intralinks early in 2017), Intralinks products go to market within two different offerings:

Synchronoss Enterprise for sales to all enterprises

Intralinks for Strategic Financials, a VDR offering to support sensitive M&A and transactional activities

Intralinks VIA can be implemented in a private cloud — three colocated facilities hold the data and account for the processing. Intralinks has regional data centers and can locally host customers' files with processing and controls. A hybrid architecture is not available. Recent development has focused on a mobile-first approach, delivering a common and adaptive experience across devices.

The Intralinks VIA platform offers workspace capabilities for projects and teams, and enables content collaboration, teamwork and project management. Simple rule-based or multitask workflows are supported. Intralinks has also introduced analytics and visualizations for content insight. Industry solutions for financial services and life sciences, as well as connectors to content management (e.g., OpenText Documentum, Microsoft SharePoint and IBM FileNet), expand Intralinks' services for business processing. A single platform for content sharing and management, based on a common identity/access model, enables content access across applications, data protection and governance, and compliance reporting.

Intralinks VIA is a good fit for organizations that want a private cloud deployment with data protection, security and regulatory compliance, and that require sharing sensitive data and external collaboration. Large enterprises already using Intralinks' specialized applications (such as those for the financial services, legal and life science sectors) can benefit from Intralinks' content platform and enable horizontal CCP use cases by means of Intralinks VIA.

Microsoft

Microsoft OneDrive for Business (ODB) is a CCP product available as a stand-alone cloud service, as an extension to Microsoft SharePoint Server or in Microsoft Office 365. ODB is a critical engine in Microsoft's integrated Office platform. It offers file synchronization and sharing capabilities that can be coupled with Microsoft's Office and productivity products to create seamless user experiences across Microsoft applications, especially when working with enterprise content in SharePoint. Office 365 also expands the OneDrive experience with digital business workloads via the Flow connectors and other advanced collaboration and productivity features.

ODB can be deployed in several ways: in a public cloud either as stand-alone, or most commonly as part of an Office 365 subscription bundle; in a hybrid capacity through redirection via SharePoint 2016 using an app launcher; and on-premises, in SharePoint 2013 and SharePoint 2016 deployments. ODB is the unified sync client for Office 365, enabling integrated Office and file-centric experiences on desktops, browsers and mobile devices. ODB includes support for numerous file viewer types such as non-Office files, 3D and DICOM images, and video streaming.

Microsoft runs a global support operation and cloud data centers. A new administration console for centralized ODB management can be enhanced with Microsoft's identity-centric Enterprise Mobility + Security (EMS) — as well as other mobile device management suites such as VMware AirWatch and MobileIron — for mobile device and application management. Recent enhancements — including the OneDrive mobile app, Files On-Demand, OneDrive desktop sync client, customer key management and the introduction of connectors through the Flow integration — enhance UX in the Office 365 productivity platform.

Microsoft is a good fit for companies that have prioritized investment in Microsoft Office productivity and collaboration suites, content server platforms (such as SharePoint Server), SharePoint Online, and Office 365. It fits well with organizations that aim to leverage an integrated, cloud-based platform to enable digital workplace scenarios.

Thru

Thru's CCP solution is based on a service-oriented architecture and extensive APIs for building integration with multiple repositories. It can be deployed in public or private clouds, private or hybrid clouds, or on-premises. In hybrid configurations, data files can reside in a third-party cloud. Thru has global data centers, cloud route optimization and Optiband, a bandwidth management technology that customers can take advantage of for poor connections (e.g., satellite), WAN acceleration and back-end regional syncing optimization of large file transfers.

Thru focuses on security, workflows, mobile UI, integration with repositories, and content management with metadata. It prioritizes on secure file-sharing needs for businesses with remote offices and cruise lines operating on high-latency networks like satellite connections.

Thru provides plug-ins to productivity and business applications such as Microsoft Office 365. A new product, Optiflow, automates file sharing and workflows, expanding content orchestration capabilities for file movement between repositories, in support of business process applications. This adds support for more traditional content management, retention and records use cases.

Thru is a good fit for midsize and large organizations aiming to improve collaboration through secure exchange of large files among departments, customers and partners using any device and from any location. It also is a good fit for enterprises aiming to support file exchange across multiple applications (such as CRM, ECM and ERP), and for those needing to send large files to geographically distributed locations with high-latency downloads and uploads.

Context

In 2017, Gartner renamed the enterprise file synchronization and sharing (EFSS) market to the content collaboration platform (CCP) market. This name change aligns the market name with the significant evolution of capabilities and use cases of the market's products in the last few years (see "Magic Quadrant for Content Collaboration Platforms"). This evolution has seen offerings expand well beyond core file synchronization and sharing functions to deliver content-driven collaboration among individuals and teams, lightweight content management and file-centric workflows.

The evolution of the CCP market is ongoing, bringing continued transformation of product capabilities, such as the following:

Market consolidation through the acquisitions of Intralinks by Synchronoss and Syncplicity by Axway adds new installed bases and introduces new growth opportunities for both. In the case of Syncplicity, the Axway acquisition expands the platform offerings and indicates the critical nature of CCP functionality in infrastructure and data management systems such as MFT.

Competition from other markets, including productivity and collaboration systems, is driving further evolution of CCP products and capabilities. The addition of file syncing capabilities in CSPs, MFT middleware application software, workstream and cloud document collaboration services (e.g., Slack, Quip) and, most significantly, the cloud office hegemonies of Microsoft Office 365 and Google G Suite continue to raise the table stakes for differentiation and added value in CCPs.

Organizations continue to make CCP investments a strategic priority to enhance content experience and autonomy for users while being able to maintain oversight of usage for data protection and infrastructure modernization. Consumerized user experiences, external document collaboration, cloud content storage, centralized oversight and governance are leading reasons as to why customers look to CCPs as critical digital workplace systems.

Application leaders should use this report to focus in on the CCP product offerings that have the right capabilities to support their use cases.

The ratings in this report are derived independently each year and depend on comparative ratings between vendors. Each year's ratings should be assessed on their own. Fluctuations in scores between years for an individual vendor do not necessarily reflect year-over-year improvements or downgrades.

Product/Service Class Definition

CCPs (which used to be called EFSS) are services-led platforms (including repositories, clients and APIs) that enable users to share and collaborate on unstructured content across multiple devices. CCPs facilitate the syncing and sharing of files among individuals, teams and groups, inside and outside of the organization.

CCPs also provide centralized protection, document management and lightweight workflow over the content across multiple repositories and workloads. Core functionalities include:

Mobile access to content repositories

File synchronization across devices and cloud repositories

File sharing with people and applications inside or outside the organization

Files search and retrieval across multiple file repositories

CCPs originate from the EFSS "destination" offerings that were covered in the "Magic Quadrant for Enterprise File Synchronization and Sharing." As such, they are expected to be stand-alone products with file sync and share as the core capability, enhanced by collaboration and content management functions.

Critical Capabilities Definitions

Mobility

User support for access to enterprise content and storage via mobile devices such as smartphones, tablets and laptops. Native mobile applications and hybrid or web apps in mobile browsers enable content access, manipulation and sharing.

This capability supports remote and mobilized usage across different devices and locations. It includes common mobile and computing operating systems, secure information transfer over common communications networks (cellular, Wi-Fi or other), and adaptive clients or apps that support intuitive interfaces for users. IT administrator features such as device protection and remote wiping are critical for mobility. Additional capabilities for mobile device management, mobile device features such as native mobile alerting or messaging, camera access and containerization are offered by CCPs.

Productivity

Integrated and intuitive designs that offer seamless cross-device access to files, productivity and business applications. Support for file editing, real-time content collaboration, annotation and note taking — natively or through integration with third-party suites.

Offerings with this capability provide intuitive interfaces and integrated, user-centered design for end users to sync, share and access files in different working models (for example, in the office, remotely or on mobile devices). This capability focuses on features that enhance user productivity with files, such as capture, editing, assigning to folders and sharing. Interfaces include support for transparent and automatic round-trip data synchronization between devices and the cloud service/server; multiple levels of mobile file sharing among devices, applications and with people inside and/or outside the organization; and access to files in on-premises repositories by direct access or replication to a cloud repository.

Collaboration and Social

Collaboration capabilities help users to work jointly on projects using a common set of documents. They include recommendations, commenting, sharing, co-authoring, markup, tasks and gamification. The "workspace" construct enables a persistent secure space for extended content collaboration.

These capabilities are critical to extending content collaboration among teams, across organizational boundaries and collaboration with individuals or groups outside the organization. Social tagging, favorite ratings, forwarding, notifications, workflow approvals, signatures and mapping content usage extend the file synchronization and sharing functionality as an asynchronous channel for processing content.

Content Management

Features and functionality that enable the structured management of documents and content, including file versioning, standard and user-defined metadata, searching, retention policies, e-discovery, archiving and migration support.

Content management capabilities include support for features that involve the capture, viewing, editing, control and management of documents in web browsers and/or mobile apps, either through embedded native capabilities or through third-party apps. Version controls and recall, check-in/check-out, file permissions and rights, metadata and automatic tagging, and viewers and editors for different file formats and types belong to this category. Enhanced capabilities also include content life cycle management, lightweight records management, file holds, image and capture, activity tracking, plus business process management and content workflow support.

Integration

The ability to integrate with back-end systems and services — such as network file systems and front-end business tools, office suites, enterprise content management, and business process applications — through ready-to-use connectors.

Integration should be available for both front-end and back-end content creation and management services. Connectors may be available for a range of enterprise applications and systems including cloud storage services, content editing suites, collaboration suites, business applications, and network storage infrastructure. Front-end integration includes extensions into productivity, line of business and other process applications that support content creation, collaboration, sharing and processing. Back-end integration includes administrative functions and interfaces that CCP services manage either on-premises or in the cloud (including data repositories, directories, workflow and business process applications). Most CPPs integrate with Microsoft Office 365 today. Fewer CCPs offer integration with Google Docs or workstream collaboration tools such as Slack, but we are finding these integrations on product roadmaps.

Platform

The availability of a content platform enabling customers and developers to access, leverage and extend the CCP content repository through, for example, APIs, development tools, application management — building new business applications or integrating existing ones, or customizing CCP applications.

A platform offering enables customers to extend, customize and optimize content collaboration capabilities through APIs and interfaces with other content services (for example, content management, security, searching, storing and metadata) and across storage, deployment and repositories.

Infrastructure

The optimization of enterprise data infrastructure through the synchronization and integration of files across repositories, applications, servers and devices.

This capability is relevant for implementations where data infrastructure modernization, data residency and other data centralization use cases are needed. Data infrastructure addresses data location, federation of repositories and content storage in different deployments such as on-premises, cloud and extranets. Data migration, legacy application repository integration, mobilized workforce, digital workplace file sharing, data residency optimization and cloud storage initiatives are examples of data infrastructure use cases for CCP.

Administration

Support for different server and endpoint operating systems, system administration, dashboards and reporting tools, platform services and deployment models, such as public cloud, on-premises, hybrid and private cloud.

Administration includes deployment support for different server and endpoint operating systems (especially mobile systems) and different service delivery models (such as public cloud, on-premises, hybrid and private cloud). Centralized administration includes dashboards and controls that allow administrators to manage synchronization, as well as provision, manage, track and protect content through policies, granular controls and remote management with mobile management capabilities. Dashboards on performance and usage allow administrators to understand usage and optimize the system. CCP as a platform for content sharing, syncing and management is an emerging capability that allows customers to build a service-oriented, content-sharing ecosystem.

Security

Features that control security (including encryption at all stages of the process), location and administration settings for users, content and endpoints, access control, logging, key management, identity, authorization, and group management.

Critical protection capabilities include permissions and access control, group management and access settings, data loss prevention (DLP), file holds, rights management, remote wipe, file retraction, encryption, and key management. Integration with Lightweight Directory Access Protocol (LDAP), Active Directory for authentication, single sign-on with centralized administration of group policies, permissions, user access and lockout, and device restrictions are also primary security features.

Many CCPs also provide policy-based DLP, data residency, content retraction, auditability of content for compliance and legal holds, separation of personal and enterprise content, group and granular access, and rights assignment.

Use Cases

Workforce Productivity

This use case focuses on general-purpose, nonroutine working experiences by individuals on documents, from different locations and across multiple devices.

It includes enhanced syncing and access capabilities and supports all client devices (mobile and desktop) for file access, sharing, syncing, optimized content aggregation and search for individuals and teams. Workforce productivity focuses on the capabilities required for a productive mobilized working experience, whether it's using mobile devices, teleworking or remote working. Client interfaces, including mobile apps, web clients, desktop plug-ins and offline usage are key features in workforce productivity. Critical capabilities include security and protection features needed to enable safe mobile content use, syncing of files for content consistency across devices, and file-version capture for rollback and historical file access.

This use case covers all devices and client interfaces (especially mobile devices) where users are allowed bidirectional access to view and work on documents and other content regardless of their physical location. Additional interaction — with commonly used productivity applications, line-of-business and content management tools, and repositories — is an important criterion for this use case.

Extended Collaboration

This use case focuses on file sharing inside or outside the organization, for collaborative content processes include editing, commenting, notification and data protection.

It supports the sharing of content both across an organization and with external parties that need access to files for collaborative and co-working scenarios. Granular controls and permissions allow for collaborative or business processing capabilities such as file approval, signatures, editing and document modifications. CCPs are used to support process optimization activities with external constituents such as contract negotiation, sharing of published content, co-development of products, knowledge sharing and solving customer relationship problems. This use case relies most heavily on security, identity, content management, collaboration and social capabilities.

Infrastructure Modernization

This use case focuses on reorganizing data infrastructure, replacing file and FTP servers, moving content to the cloud, data residency and backup/recovery automation.

It includes the use of CCPs for back-end file management and data movement for application or data center purposes. Organizations use CCP efficiencies and capabilities for one-time or multiple syncing activities. CCP data center modernization scenarios include the migration (or coexistence) of legacy applications, file share consolidation, content preloading for projects and onboarding, extensibility for business processing, and secure sharing. This use case relies heavily on content security, connectors to back-end content repositories (on-premises or in the cloud), content syncing, versioning and cloud architectures.

Centralized Content Protection

This use case focuses on centralized content oversight and governance in a secured environment.

Features include policy enforcement, data protection, data residency, reporting, file retention and legal holds. The use case supports centralized administration, dashboards and tools for enterprise content oversight and governance in the highly distributed CCP environment. Administration tools provide the ability to set policy-based access and permissions, content classification and tagging for management and protection of content files across the entire environment or for certain locations, folder or files. Governance is supported through analytics of users' activity and content.

Centralized content security and enforcement — including data residency, encryption key management, centralized rights management, device control and remote data wiping, separation of personal from enterprise data, and DLP — are key governance capabilities. Advanced solutions offer deeper compliance requirements coverage with dashboards for interrogating logs and usage of content and files. They target special collaboration activities in regulated sectors such as legal, healthcare or financial services.

Lightweight Workflow

This use case focuses on automation of simple content flows for effecting document-based processes that can be triggered by user events, actions on files or metadata values.

This use case is relevant to organizations aiming to implement lightweight document-centric workflows, among individuals or teams, inside or outside the organization. Document management, collaboration and business application integration are key capabilities that can be supported by CCPs. Features leverage the CCP content ecosystem, controls, syncing and sharing capabilities to support lightweight content processing, especially with external parties, for the editing and sharing of information. Workflow can be triggered manually or automatically via user-defined triggers or events, with task tracking and notifications to users. Advanced offerings can operate as a business processing coordination layer among third-party systems, such as document signing or line-of-business applications. This enhances the usage, sharing and processing of documents for more seamless user experiences when working with business documents.

Vendors Added and Dropped

Aligning with the companion Magic Quadrant for CCP, this Critical Capabilities report covers only products from vendors that qualified for inclusion in 2017. Nonetheless, a range of other products are available to support the five use cases, not only in the CCP market.

Added

Ctera

HighQ

Dropped

Varonis — the vendor does not qualify in this year's CCP Magic Quadrant and Critical Capabilities reports because its product, DatAnywhere, does not meet inclusion criteria for mandatory product features including collaboration support, connectors for integration with other content repositories, and business applications.

Inclusion Criteria

The inclusion criteria for this Critical Capabilities report are identical to "Magic Quadrant for Content Collaboration Platforms." For completion, we report the full list:

Offering — Vendor has a CCP offering for business, based on core EFSS capabilities.

Revenue — Its CCP product and service revenue (for 2016) must be more than $20 million.

Geography — Vendor has a presence in at least two geographic regions, with some personnel dedicated to the relevant product. No more than 70% of revenue may come from one geographic region.

Commercial availability — The CCP product has been generally available since 1 September 2016.

Packaging — The CCP product must be available as a separately billed, stand-alone product. CCP capabilities alone, bundled with a different product from the same vendor, are considered extensions and are insufficient for inclusion.

Total users — There must be at least 500,000 active, paid users among all the organizations that are licensed to use the product.

Largest deployment — At least one deployment must have 10,000 users.

References — Five customers must have deployed the service or product for a minimum of six months, and have at least 1,000 paid users. Two of the references must have at least 4,000 paid users.

In addition, vendors' CCP offerings must support a selected range of **product capabilities:**

File synchronization — This is support for transparent and automatic round-trip data synchronization between devices and the cloud service/server, or across multiple devices, for selected files or folders.

File sharing — This is support for multiple levels of file (and folder) sharing among devices belonging to the same person; different applications on the device; and people inside and/or outside the organization.

File access — This is access from a client application or a browser to files stored in on-premises or cloud repositories, by direct access or copy to an internal repository. Use of third-party connectors is acceptable, but native support is rated higher.

User productivity — This includes document view, editing and annotation in the mobile, desktop and browser app, either through embedded native capabilities or through third-party tools (e.g., Office 365).

Mobile — This includes a native application for iOS and Android. Support for Windows and other platforms is optional.

PCs — This is support for sync on Windows PCs and Mac OS through a native stand-alone application. Web browser or email client plug-ins, as well as support for Linux platforms, are optional.

Security — This includes password authentication, lockout after a period of inactivity, selective remote wipe of the app and related files on the device, and data encryption at rest and in transit.

Management — This refers to integration with LDAP, Active Directory or other directories via identity federation for authentication, single sign-on, group policies, and centralized management tools that allow administrators to manage synchronization and control the content, access rights and user activity. Integration with enterprise mobility management (EMM) is optional.

Integration — Products must support at least one type of integration with corporate data repositories, on-premises or in the cloud — for example, Microsoft SharePoint Server or SharePoint Online, Microsoft OneDrive for Business (on-premises or online with Office 365), Google Drive, Dropbox, AWS or Salesforce — or data infrastructure such as network-attached storage.

Platform — Products must include a content platform offering, with APIs, navigators, documentation, development tools, application management, ecosystem of partners, etc.

Delivery model — This means availability as cloud services in public or private clouds, or as hybrid deployment, combining on-premises repositories with cloud-based CCP functionality.

Features provided by partners must be tightly integrated with the vendor's product and invisible to the end user.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), 3 = Standard (most or all defined requirements achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	
Collaboration and Social	
Workforce Productivity	5%
Extended Collaboration	25%
Infrastructure Modernization	0%
Centralized Content Protection	10%
Lightweight Workflow	0%
Content Management	
Workforce Productivity	15%
Extended Collaboration	15%
Infrastructure Modernization	0%
Centralized Content Protection	10%
Lightweight Workflow	25%
Infrastructure	
Workforce Productivity	0%
Extended Collaboration	5%
Infrastructure Modernization	30%
Centralized Content Protection	0%
Lightweight Workflow	5%
Administration	

Workforce Productivity	5%
Extended Collaboration	10%
Infrastructure Modernization	25%
Centralized Content Protection	15%
Lightweight Workflow	10%
Integration	
Workforce Productivity	10%
Extended Collaboration	5%
Infrastructure Modernization	20%
Centralized Content Protection	5%
Lightweight Workflow	15%
Mobility	
Workforce Productivity	25%
Extended Collaboration	5%
Infrastructure Modernization	0%
Centralized Content Protection	10%
Lightweight Workflow	10%
Security	
Workforce Productivity	5%
Extended Collaboration	15%
Infrastructure Modernization	10%
Centralized Content Protection	30%
Lightweight Workflow	5%
Productivity	
Workforce Productivity	25%
Extended Collaboration	20%
Infrastructure Modernization	0%
Centralized Content Protection	15%
Lightweight Workflow	0%
Platform	
Workforce Productivity	10%
Extended Collaboration	0%
Infrastructure Modernization	15%
Centralized Content Protection	5%
Lightweight Workflow	30%

Total	
Workforce Productivity	**100%**
Extended Collaboration	**100%**
Infrastructure Modernization	**100%**
Centralized Content Protection	**100%**
Lightweight Workflow	**100%**
As of August 2017	

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	
Collaboration and Social	
Accellion	3.8
BlackBerry	3.9
Box	3.9
Citrix	4.6
Ctera	1.7
Dropbox	4.0
Egnyte	4.2
Google	4.5
HighQ	4.0
Intralinks by Synchronoss	4.0
Microsoft	4.2
Axway (Syncplicity)	3.5
Thru	3.1
Content Management	
Accellion	3.5
BlackBerry	4.8
Box	5.0
Citrix	4.8
Ctera	3.5
Dropbox	4.5
Egnyte	4.9
Google	3.5
HighQ	2.8

Intralinks by Synchronoss	4.6
Microsoft	4.4
Axway (Syncplicity)	4.0
Thru	4.0
Infrastructure	
Accellion	4.6
BlackBerry	4.2
Box	4.2
Citrix	5.0
Ctera	4.8
Dropbox	3.2
Egnyte	5.0
Google	3.8
HighQ	3.5
Intralinks by Synchronoss	4.4
Microsoft	4.4
Axway (Syncplicity)	5.0
Thru	4.4
Administration	
Accellion	4.4
BlackBerry	4.1
Box	4.1
Citrix	4.4
Ctera	4.5
Dropbox	4.2
Egnyte	4.8
Google	3.8
HighQ	3.7
Intralinks by Synchronoss	3.3
Microsoft	4.1
Axway (Syncplicity)	4.4
Thru	4.2
Integration	
Accellion	3.2
BlackBerry	4.1

Box	3.0
Citrix	3.4
Ctera	1.6
Dropbox	2.5
Egnyte	3.5
Google	4.0
HighQ	1.1
Intralinks by Synchronoss	3.0
Microsoft	2.5
Axway (Syncplicity)	3.2
Thru	2.1
Mobility	
Accellion	4.2
BlackBerry	4.4
Box	5.0
Citrix	5.0
Ctera	4.7
Dropbox	5.0
Egnyte	4.2
Google	3.6
HighQ	1.7
Intralinks by Synchronoss	3.1
Microsoft	4.5
Axway (Syncplicity)	4.6
Thru	4.2
Security	
Accellion	4.3
BlackBerry	4.7
Box	4.5
Citrix	4.2
Ctera	3.6
Dropbox	3.8
Egnyte	4.4
Google	3.7
HighQ	2.9

Intralinks by Synchronoss	4.0
Microsoft	4.4
Axway (Syncplicity)	4.7
Thru	4.2
Productivity	
Accellion	4.8
BlackBerry	4.6
Box	3.7
Citrix	4.2
Ctera	3.5
Dropbox	4.8
Egnyte	3.6
Google	4.6
HighQ	3.9
Intralinks by Synchronoss	3.6
Microsoft	4.4
Axway (Syncplicity)	4.1
Thru	4.2
Platform	
Accellion	4.1
BlackBerry	4.4
Box	4.4
Citrix	4.0
Ctera	3.8
Dropbox	4.4
Egnyte	4.4
Google	4.4
HighQ	3.9
Intralinks by Synchronoss	3.9
Microsoft	3.8
Axway (Syncplicity)	4.2
Thru	4.2
As of August 2017	

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	
Workforce Productivity	
Accellion	4.13
BlackBerry	4.46
Box	4.29
Citrix	4.42
Ctera	3.61
Dropbox	4.42
Egnyte	4.15
Google	4.02
HighQ	2.85
Intralinks by Synchronoss	3.62
Microsoft	4.15
Axway (Syncplicity)	4.15
Thru	3.91
Extended Collaboration	
Accellion	4.12
BlackBerry	4.37
Box	4.16
Citrix	4.45
Ctera	3.20
Dropbox	4.16
Egnyte	4.28
Google	4.08
HighQ	3.32
Intralinks by Synchronoss	3.87
Microsoft	4.23
Axway (Syncplicity)	4.08
Thru	3.80
Infrastructure Modernization	
Accellion	4.17
BlackBerry	4.24
Box	4.00
Citrix	4.30