Controlling Content Chaos

Re-imagine content management for today's hybrid-work, content-critical age.

EGNYTE

These Days Content is the Lifeblood of Most Every Business

Digital files contain the information, knowledge, and wisdom of the most advanced intelligence on the planet: human intelligence. Whether your business is large or small, and regardless of industry, your content is the conduit for innovation, financial planning, customer interactions, and so much more.

Over time, digital businesses have shared files in a variety of ways.

WAVE 1

Digital business file sharing was a complex patchwork of on-premises file infrastructure that formed the backbone of digital work. Microsoft's Windows File Server was released in 1993 and quickly became the de facto tool for businesses, but it required manual patching and supporting technology, such as VPNs, for greater security. Procurement processes could take months, and carried expensive, upfront capital costs.

WAVE 2

Wave 2 saw the introduction of consumer cloud storage into the enterprise, often introduced as "shadow IT", as workers procured virtual storage with just their corporate credit card. This second wave did not replace traditional infrastructure, it only added to the complexity.

WAVE 3

Tech heavyweights Google and Microsoft sought to address the control and complexity issues through unified, cloud-based suites of business apps that bundled file sharing storage and collaboration with word processors, spreadsheets, chat apps, and more. At the same time, specialized productivity apps like Docusign, Slack, Zoom, Trello, Airtable, and Procore addressed themselves to niche markets and use cases. Again, the third wave apps did not replace those of the prior waves, but rather augmented them.

Additionally, while many apps were delivered through a larger suite, most notably Microsoft's, the underlying architecture was anything but simple. For example, creating a Microsoft Teams environment could involve spinning up a SharePoint Online site, an Outlook group and calendar, a Power BI workspace, and a Planner plan, all operating in the background (see more on this here).

Enter the Content Critical Age.
A "Perfect Storm" of Three Concurrent Trends

The last several years have seen many disruptions in the world, even as the COVID-19 pandemic recedes. Companies now need to support distributed data and users amid the shift to remote work. The number and volume of files stored globally continues to grow exponentially. Governments are demanding greater data transparency and protection. And cyberattacks are at an all-time high.

1. NEW WAYS OF WORKING

There is no going back—fully distributed and remote workforces are the new normal. According to Gartner's remote and hybrid workers forecast, **47% of knowledge workers** will work remotely in 2022-23, **compared with 27% in 2019**. In some industries, that number is far higher.

2. NEW THREATS

A lack of data protection, side effects of a global pandemic, and an increase in sophisticated exploits has led to a huge increase in data breaches from increasingly common sources, such as mobile and IoT devices. The sheer volume of data flowing through today's businesses has put a bullseye on the backs of companies, large and small. **According to Accenture, 68% of business leaders feel their cybersecurity risks are increasing.**

3. NEW REGULATIONS

The risks of not governing files are more prevalent and dangerous than ever, and severe consequences are being enforced as stricter data privacy legislation is enacted across the world. Companies are taking note of GDPR, as more regions are expected to emulate the EU legislation. Depending on the industry, organizations may also need to provide proof of compliance with data standards like HIPAA, SOX, NIST 800-171, and ISO 27001, among others. **As tracked by International Association of Privacy Professionals (IAPP), in 2021, state legislatures proposed or passed at least 27 online privacy bills to regulate data markets and protect personal digital rights.**

> "Data is a primary target of adversaries—ranging from state-nexus threat actors looking to purloin data to ransomware threat actors who try to steal data from an environment or lock it up for ransomware and extortion."
>
> - *"2022 SANS Protects: File Storage,"* SANS Institute, March 2022

Yesterday's Tools Were Never Intended For Today's Environment

Technologies that worked well enough in the past were never really designed for today's challenges. We see the implications of this in organizations small and large, resulting in overloaded IT departments, frustrated end-users, and escalating security risks.

Managing multiple file repositories, each with their own controls, has overloaded IT organizations.

51% of SMBs manage more than 10 data repositories.

- "Cybersecurity Trends for Mid-Sized Organizations,"

User frustration is at an all-time high, as content is fragmented across all sorts of locations, including email (77%), collaboration tools (67%), messaging services (64%), and productivity apps (54%). End-users constantly struggle to track down the most up-to-date version of a file, while IT teams lack the visibility to properly monitor and secure resources.

With the risk levels rising, pricing for cyber insurance premiums continues to increase rapidly, only adding to other economic pressures.

Nearly half of SMBs have experienced cybersecurity insurance premium increases of **76%** or more in the past year.

- "Cybersecurity Trends for Mid-Sized Organizations,"

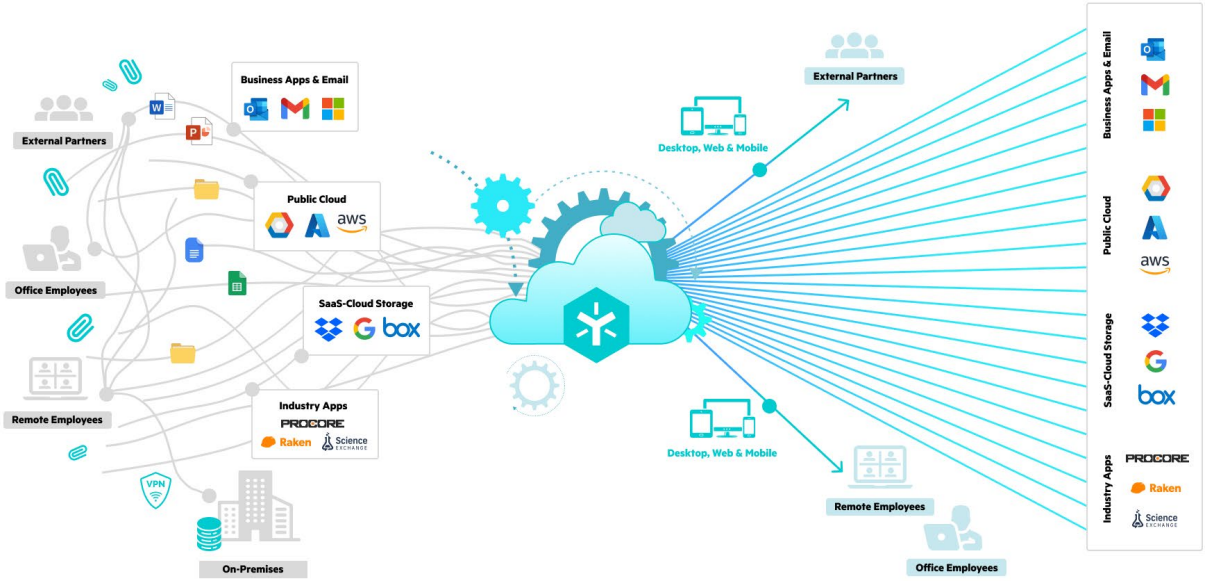
A New Architecture for the New Normal

Clearly the challenges are mounting, and the task ahead can seem daunting—but there is good news. The companies that have reimagined their content architecture for this new era have seen impressive results.

These forward-thinking companies have made the shift to a modern foundation of technologies and processes. They've increased productivity by empowering end-users with collaboration tools that work from anywhere. At the same time, they've decreased risk by giving IT the governance capabilities they need to maintain visibility and control across data sources.

But, as the left of the image pictured below illustrates, the modern software stack can quickly become a jumbled mess. In that scenario, external partners, in-office staff, and remote employees need to access much of the same information and apps, but they do so in different, disjointed ways. This creates redundancies, increases attack surfaces, and slows productivity.

If companies truly want to take advantage of this new normal, they should look to emulate the right side of the illustration. All repositories—public cloud, on premises, SaaS apps—should point to a central, compliant location that unifies the data across repositories and business applications, and secures it for access from anywhere. No more VPNs, attachments, or manual backups.



1 REDUCED IT COSTS; INCREASED PRODUCTIVITY

The Hakkasan Group eliminated expensive on-premises infrastructure to support an increasingly remote workforce. By moving to a cloud-based file sharing and content management system they saw **$2.4 million in productivity and security gains while achieving an ROI of $3.4 million over three years**. They reduced their data center and office footprints by eliminating legacy file servers, and they increased employee productivity through integrations with commonly used tools like Adobe, DocuSign, Salesforce, and Slack.

2 CENTRALIZED CONTROL

Marketing agency, MullenLowe created a **"single source of truth"** for its data by integrating its myriad data sources into one repository. This helped users find the right versions of the files they needed, but it also led to better auditing, automated compliance reporting, and centralized visibility for IT. Simplified implementation of data retention policies and file recovery capabilities provided an additional layer of support in the event of a ransomware attack or accidental deletion.

3 NEW BUSINESS OPPORTUNITIES

Engineering firm SM&E moved from a mishmash of collaboration and storage technologies to a **unified platform to accelerate the next stage of growth** for the company when starting work with larger, more sophisticated clients who required advanced data protection and cybersecurity certification, like adherence to the CMMC 2.0 framework for businesses that work with the U.S. Department of Defense.

4 SIMPLIFIED ADMINISTRATION

Biotech incubator Third Rock Ventures supplies its startups with **storage and collaboration tools** that support audit trails, data management at scale, and improved workflows right out of the box. By simplifying IT operations from the start, their startups have jump started their growth by focusing more on the business and less on the underlying tech.

A Change in Perspective

Fundamental changes in how IT teams and end users operate don't come around often. This type of paradigm shift can be painful for companies entrenched in their ways, which is why it's essential to understand the value in such a move. Here are just a few examples of how the changing business landscape is putting pressure on companies to modernize their content management strategy.

APP, DRIVE SPECIFIC → ANY CLOUD, ANYWHERE

It's a multi-cloud world, and your users need access to all their favorite business apps, whether that's productivity suites like Microsoft 365 and Google Workspace, or specialized services like Docusign or Procore. A modern file server links all these apps together and supports access to cloud-based tools on any device, from anywhere.

IT COMPLEXITY → IT SIMPLICITY

Modern companies manage more than 10 content repositories, and employees interact with content via an excess of email, collaboration, messaging, and productivity applications. The only way to effectively manage the natural sprawl of content is with a unified management console that can provide visibility and control of data inside these disparate applications - allowing employees to use the tools they love, while IT maintains centralized control from a single dashboard.

SILOED → INTEGRATED

Collaboration tools that support distributed collaboration, like Gmail, Teams, and Slack, are experiencing exponential growth. These tools, as well as industry-specific apps, require native ways to access content from a single, trusted source of truth. Otherwise, emplopyees' daily routine consists of hopping between applications, looking for the right file.

PERIMETER AND PEOPLE DEFENSES → DATA-FIRST SECURITY

Companies typically focus on perimeter defenses or user behaviors, but distributed workforces and dwindling IT resources is forcing them to rethink these siloed models. Data is critical to a business' continuous operations, so it needs a robust platform that offers extremely granular governance and security controls. And by combining data security with collaboration and cloud integration, businesses have the ability to secure their data and their organization.

CUMBERSOME → INTUITIVE

Most file sharing solutions are built with friendly, intuitive interfaces. However, if you look a little deeper, you'll find that they become considerably more complex and constrained as you move beyond the traditional file access and sharing use case. IT needs intuitive, automated ways to:

- Manage users, groups, roles, and permissions
- Support real-time co-editing and co-authoring
- Enforce secure sharing controls and lifecycle management policies

MODERN CONTENT

A Modern Content Architecture

The modern content architecture delivers on everything IT needs from traditional file shares, combined with everything end-users love about cloud apps like Microsoft 365 and Google Workspace, in one, unified platform.

Of course, getting there won't happen overnight. Egnyte has developed a content management maturity model to help companies make this shift. This model analyzes IT readiness in four categories—infrastructure, administration, collaboration, and security and governance—and places companies on a spectrum, from "initial" to "optimized." Here's a high-level overview of some of what is included in the model.

	INITIAL/DEVELOPING	MANAGED/OPTIMIZED
INFRASTRUCTURE	▶ Self-managed on-premises hardware and software that requires cumbersome patching, refreshes, procurement, and data backup ▶ Disparate repositories with overlapping, duplicate content ▶ Integrations that are expensive and require customized development	▶ Majority IaaS and SaaS, with hosting, scaling, backup, and recovery handled by providers ▶ Centralized repository to automatically sync files across on-premises and cloud sources ▶ A pre-built catalog of applications integrations available through a managed solution provider
ADMINISTRATION	▶ Dedicated IT admin manages a high-touch, complex environment spread across multiple portals ▶ High ticket count driven by self-managed infrastructure ▶ Manual user provisioning across multiple systems and content sources	▶ Infrastructure provided as a service, with a single unified management interface ▶ Few end-user requests due to standardization and the implementation of self-service features ▶ Automated, real-time provisioning across domains through an integrated identity management system
COLLABORATION	▶ Corporate-only devices, with content accessed remotely via VPN ▶ Files accessed via disorganized file servers, with no workflow or integration capabilities to keep projects on track ▶ Single-user editing, leading to duplicate data and versions across multiple repositories	▶ BYOD support, with remote access optimized for performance by geo-location within a cloud repository or intelligent local caching ▶ A single platform for sharing, workflows, versioning, and commenting, including integrations with key business apps ▶ Real-time, multi-user editing, with robust version control to avoid publication and restore older file versions
SECURITY AND GOVERNANCE	▶ No formal policy for data classification and data lifecycles, with efforts done on an ad hoc, manual basis ▶ Poor monitoring that limits the ability to partition sensitive data and provide sufficient reporting for audits and compliance ▶ Inability to identify unusual access due to a lack of reporting or logging	▶ Formal, company-wide content classification framework that automatically manages data access, protection, lifecycles, and workflows ▶ Robust monitoring that tracks and partitions sensitive data and supports centralized reporting, logging and data awareness ▶ Automated, behavioral-based detection of unauthorized access. Logs centralized and visualized in a single dashboard

From Content Chaos to Content Cohesion

The old tools are not going away, but the old architecture needs to change. As we've documented throughout this report, the challenges are too complex and the stakes are too high to stick to the status quo.

To truly succeed in the modern era of work, companies need to break away from data silos, excess IT management overhead, and insufficient security and governance. They need a simple, intuitive platform championed by IT and end-users alike through centralized control, reduced CapEx and complexity, and files that are easy to find and collaborate on.

> **"Now teams can work from home, from the coffee shop, from their kid's Little League game...The people, and firms, who can integrate work and life will eat the lunch of those who can't, and Egnyte gives us that flexibility."**
>
> ***- Rob Sloyer, VP of Innovation & Strategic Services | KAST Construction***

To learn more, read the Egnyte Product Review by the **SANS Institute.**

EGNYTE

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multi-cloud businesses. More than 17,000 organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere. Investors include GV (formerly Google Ventures), Kleiner Perkins, Caufield & Byers and Goldman Sachs.

For more information, visit **www.egnyte.com.**

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com