S&P Global
Market Intelligence
451 Research Business Impact Brief

Productivity Depends Upon Security Practices

The 451 Take

There's no denying that many work trends that began during the pandemic continue today, including hybrid and remote work models and digital transformation, which largely involves modernization of work processes and transformation to cloud-based architectures. Along with these is an increase in worker collaboration, both inside and outside of corporate boundaries with partners, customers, suppliers, all of which require additional user autonomy and place an increasing emphasis on securing those systems. As such, it makes sense that two of the top drivers for digital transformation are improving worker productivity and managing risk — for example, cybersecurity, data privacy and systems reliability (see Figure 1).

Top drivers for digital transformation

Q. In your opinion, what are the main drivers for digital transformation? Please select all that apply.
Base: All respondents (n=500).
Source: 451 Research's Voice of the Enterprise: Workforce Productivity & Collaboration, Digital Transformation, October 2023.

With these two driving forces, it's clear that security and privacy will be foundational elements in the architecture of next-generation productivity and collaboration experiences. And this security-centric approach will have the greatest impact among the tools and technologies that are most associated with worker productivity. Survey respondents indicate that the top three tools that most contribute to personal productivity at work are all-in-one suites with word processing, forms and slideshows (48%), collaboration and communication tools (41%) and file sharing or content management tools to share and manage documents (40%), according to 451 Research's Voice of the Enterprise: Workforce Productivity & Collaboration, Work Execution Goals & Challenges 2023 survey. These are followed by tools such as business systems of record and project management tools.

The least common denominator among those tools is documents. Documents play a key role in individual productivity but are also critical for sales, HR and project management — and their optimization is a strategic investment in next-generation productivity. However, as we noted, increased demand for user autonomy and a growing interactivity with individuals in the extended enterprise (i.e., outside the firewall) demand a renewed focus on securing these documents to drive new business outcomes.

S&P Global
Market Intelligence
451 Research Business Impact Brief

Overly complex, legacy approaches to security and privacy can hamper document productivity by increasing workflow friction and creating confusion around access and editability. On the other hand, too lax a security strategy leads to increased risk of data exposure and compliance issues. The success of next-generation document productivity depends on modern security practices that support the document data and workflow ecosystem, account for changing dynamics in access and enterprise collaboration, and make way for new technology adoption and cloud scalability.

Business impact

Digital transformation maturity enables new opportunities. Digital transformation projects, which are increasingly necessary to establish and maintain competitive advantage and leverage emerging technologies such as generative AI (GenAI) and machine learning (ML), are dependent on cloud platforms and SaaS applications. Overcoming adoption barriers is closely tied to choosing service providers that follow security best practices and compliance regimes. Addressing these risk vectors at the onset and in partnership with document productivity vendors sets the stage for an organization to explore novel capabilities and technologies with less perceived risk — increasing autonomy and potential productivity through areas such as automation.

The extended enterprise becomes easier to manage. The growth of hybrid and remote work, along with increasing collaboration outside the corporate firewall in modern organizations, is creating a document and data management nightmare. There are so many documents and massive quantities of data to manage, along with employees located across multiple geographies inside and outside of the office, all of which adds to the complexity. On top of this, documents are rich targets for attackers because they can contain sensitive information such as personally identifiable information, personal health information or other forms of highly confidential data. Modern security principles that prioritize access management can ensure that the right people have access to the data at the right time, from the right place, making it easier to support document productivity across this new business ecosystem without compromising data privacy.

Document integrations and workflows have room to evolve. Digital transformation requires securing documents as well as the workflows and business processes that use them. A central component in these architectures is the application programming interface (API), and API security is a top concern as these are key points of vulnerability that may be overlooked during the development process; each implemented API expands the organization's attack surface. Cloud-based collaboration platforms make extensive use of APIs, which allow users to easily incorporate their own business systems and data into the collaboration platform. Further complicating the issue is the difficulty of detecting API exploits. Partnering with vendors that make security a top priority — all the way down to the API level — sets the stage for the document productivity strategy to evolve across the SaaS application estate, taking advantage of data integrations and workflow automation with less risk.

Looking ahead

Secure document productivity is a key component of successful digital transformation and will continue to be a key business enabler. Digital transformations, which provide significant advantages in terms of improved ability to compete, rapid adoption of emerging technologies (such as AI/ML) and improved worker productivity and mobility, must also be properly secured. Choosing the right cloud service providers is critical during these projects; doing so can reduce an organization's reticence to move by reducing risk.

Realizing this, secure document productivity vendors have been rapidly shoring up their security regimes, including providing Cloud Security Alliance Service Organization Controls compliance assurances, in addition to supporting industry and governmental compliance requirements. Along with vendor security regimes, organizations should review their document practices, processes and policies. A few examples include requiring document sensitivity labels, using encryption at rest and in motion, leveraging sandboxing technologies to securely examine suspicious documents and moving away from email attachments. The application of digital signatures and e-seals can also help to ensure the integrity of documents. Employing these recommendations will go a long way toward preventing security incidents while protecting the organization's crown jewels.