opentext™

What's new in OpenText eDOCS 16.5

OpenText™ eDOCS, is a highly-flexible, secure, document management solution integrated with Microsoft® Office, which empowers legal users and other business users to quickly and easily, find, save, collaborate on and share information so they can focus on what is most important.

opentext™

Contents

opentext™

Many organizations suffer from a decentralized document management system, non-standardized naming conventions, multiple sub-folders and lack of version control.

Important updates on OpenText eDOCS: Improved experience within Microsoft Outlook

Seamless experience across all devices, desktop, mobile and now, Microsoft® Outlook®

- Search (faster, easier, filtering)

- Intuitive user experience

- Administration of cases/matters/projects

- One centralized location

Records Management with eDOCS

Classify, manage and govern records, including physical, electronic, emails and images from existing eDOCS implementations

- Popular OpenText™ InfoCenter interface now includes OpenText™ Records Management.

- No need to navigate away from InfoCenter to perform Records Management functions

- Improved filtering

- Fastest and quickest way to access information

opentext™

Introducing eDOCS Defense

Two additional layers of defense

1. Encryption at Rest

2. Activity monitoring

Data protection at rest aims to secure inactive data stored on any device or network. Attackers often find data at rest a more valuable target than data in motion. eDOCS Defense, a new eDOCS module, addresses the gap in protection of sensitive data at its core.

Companies face the constant, rising threat of data breaches each year. But the cost of a breach differs for every organization. How much would it cost yours?

1. Do you know how much a data breach could cost your organization?

2. What are the associated risks of a data breach?

3. How can eDOCS Defense mitigate those risks?

Why eDOCS Defense?

Attorneys have ethical and legal duties to protect information relating to clients. Encryption and Activity monitoring are important considerations in addressing these duties.

If not properly protected, laptops and portable media can be recipes for a security disaster. One survey reported that 70 percent of data breaches resulted from the loss or theft of off-network equipment (laptops, portable drives, PDAs and USB drives).[1]

- Insider threats are the cause of the biggest security breaches out there and extremely costly to remediate

- According to a 2017 insider threat report, 53 percent of companies estimate remediation costs of $100,000 and more, with 12 percent estimating a cost of more than $1 million.[2]

[1] Verizon Data Breach Investigations Report (2017)
https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/

[2] ibid

opentext.com/contact