You just migrated to Office 365. So did all your sensitive data.

Your move to the cloud brings new opportunities as well as new security concerns.

What security and compliance risks do you face in the cloud?

- 68% of organizations have non-compliant emails, which are high-risk vectors in cloud environments.  
- 90% of malware is installed via email attachments.  
- 66% of organizations lost access to critical email content.  
- 28% of phishing emails were bound to infected users.  
- 24% of phishing emails were attached to infected users.  
- 46% of phishing attacks were targeted.  
- 28% of email breaches included a phishing element.  
- 22% of breaches and incidents involved a phishing element.

“Although many security tools are offered in the standard contract through Microsoft, it’s imperative that Office 365 customers don’t skip over the fundamental basics.”

Jeff Falcon, Principal Security Architect, CDW

68% of non-compliant emails

90% malware attack

66% email loss

28% phishing email attack

24% phishing email attack

46% phishing email attack

22% breach & incident

28% breach & incident

46% breach & incident

What could a data breach cost your company?

Average cost of a cloud data breach:

$2,800,000

$2,550,000

$2,900,000

$2,600,000

Average cost by industry:

Education: $1.5M

Financial: $2.3M

Health: $11.5M

Telecom: $1.2M

Office 365 has built-in security.

But end-to-end threat protection is your responsibility.

Now What?

Get The Guide to Protecting Microsoft Office 365, from ESG.

Download Now

“Office 365 offers baseline security features baked in and ready to go. But to get the maximum security you have to make an effort to add capabilities and turn them on.”

Payton Moyer, President and COO, MLS Technology Group

57% listed Office 365 as one of the top 5 applications in need of user access and data loss prevention controls.