



# Disaster Recovery Validation


---

**Mike Schipper, CEO & Founder**

*"We'll be the last IT provider your business will ever need."*

 (616) 421 - 8325

 [info@trustedinsite.com](mailto:info@trustedinsite.com)

 @TrustedInsITe



Technology  
Strategy



Hybrid  
Cloud



Information  
Security



Office  
Mobility



Systems  
Management



Compliance  
Strategy

# InsITe Disaster Recovery Validation

If the unthinkable happens, it can sink a perfectly healthy business. Data backup has been around a long time, but recent advances have significantly improved the ability to back up data and offer new, efficient ways to recover. Without the ability to recover to proper specification, what good is a backup? Data should also be secured, monitored, and recovery should be periodically tested.

## Test your disaster recovery before you really need it

### We make it easy

Our assessment will quickly uncover gaps and opportunity for improvement, no commitment required. We then provide a plan and cost estimates for improvements.

### All Encompassing

Ensure data protection across all of your systems and data storage locations. InsITe will provide long-term disaster recovery solutions based on the whole picture.

### Manage It

InsITe provides Managed Security Services that can protect you end to end. If you have specific compliance requirements, we'll come up with a plan for you! InsITe provides managed backup services that can protect you end to end on a continual basis. Have specific recovery requirements? We'll come up with a plan!

#### Deliverables:

- + Peace of mind
- + Complete **documented security landscape**: Systems, Devices, People
- + Risk mitigation action plan
- + Complete **cost estimate** to address gaps
- + Understanding of today's security landscape

# Prevent customer and business data from falling into the wrong hands.

**Enforce who can open documents**

Document encryption monitoring and remediation

**Don't accidentally share confidential information**

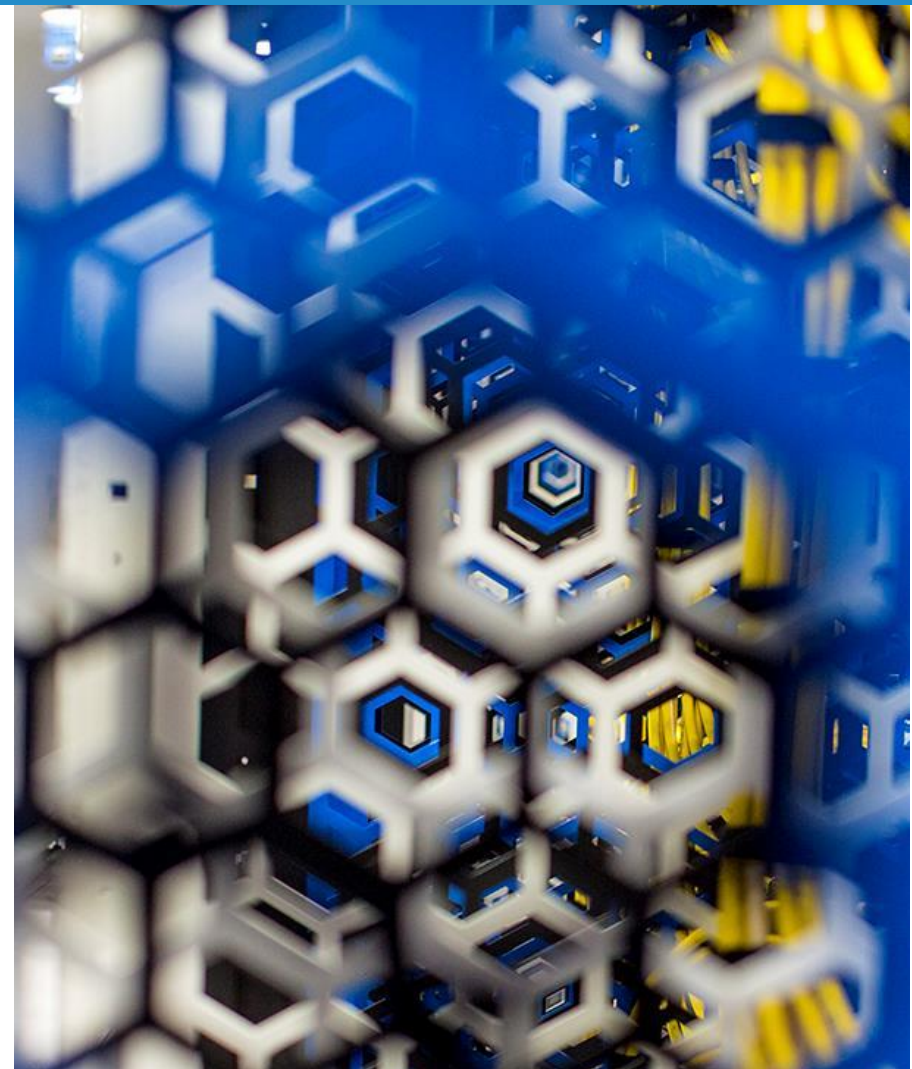
Monitoring and enforcement for access to shared files in email and team sites

**Encrypt corporate data on mobile devices**

Separation of personal information and business information on phones and tablets

**Prove that you've kept information safe**

Archiving and compliance reporting for email and/or backup and disaster recovery



# Is your data secure?

---

Is your data secured regardless of where it's stored or shared?

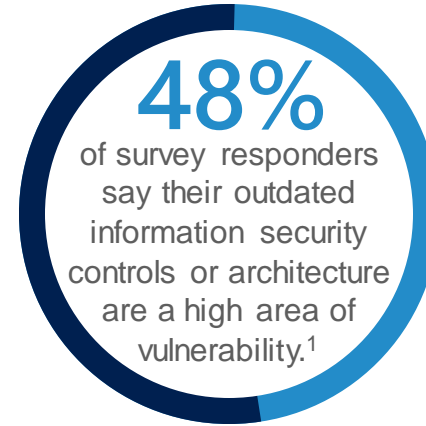
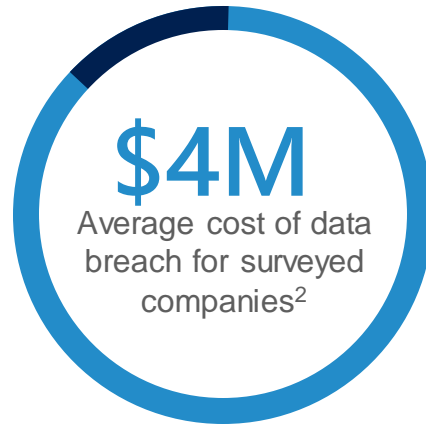
Does a data compliance policy control access to sensitive information?

Do you have the ability to classify and encrypt sensitive data?



# Control and protect information

---



Help enterprise customers protect business data while enabling user productivity and collaboration across devices and locations.



**Manage cloud application usage:** Get the security of on-premises systems for cloud applications.



**Protect against data leakage:** Have control over the access to information, no matter where it's stored or who it's shared with.



**Protect against malware and phishing attacks:** Help protect your customers' mailboxes against new malware threats and sophisticated attacks.



**Respond to security incidents:** Streamline and speed up document reviews and improve adherence to data retention policies.

<sup>1</sup> 2016 EY Global Information Security Survey <http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016>.

<sup>2</sup> 2016 Ponemon Institute Cost of a Data Breach Study <https://securityintelligence.com/media/2016-cost-data-breach-study/>

# Secure Content

## Protect content: creation, transit, consumption

Use cloud applications without putting company information at risk by adding protection, ranging from access privileges to data encryption.

- Shadow IT Detection: Discovering Apps and Risk Scoring
- Intelligent Classification and Tagging of content
- Document encryption, tracking, revocation
- Monitoring shared files and responding to potential leaks
- Data segregation at a device/app level



# Secure the Front Door

## Identity-Driven Security

Go beyond passwords and protect against identity compromise, while automatically identifying potential breaches before they cause damage.

- Risk-based Conditional Access and Multi-Factor Authentication
- Advanced security reporting
- Identify threats on-premises
- Identify high-risk usage of cloud apps, user behavior, detect abnormal downloads, prevent threats



# Secure Devices

## Workplace Issued or BYOD Devices

Manage company and BYOD devices to encrypt data and ensure compliance, automatically detect suspicious activities, and quickly block, quarantine, or wipe compromised devices.

Shadow IT Detection: Discovering Apps and Risk Scoring

- Conditional Access
- Device and App access level controls: PIN
- Device and App encryption at rest
- Save-As, Copy, Paste restrictions
- Device and App level data wipe





# Protect Your Business Today!

For more information, visit [www.trustedinsite.com](http://www.trustedinsite.com)

(616) 421 - 8325  
[tellmemore@trustedinsite.com](mailto:tellmemore@trustedinsite.com)  
[www.trustedinsite.com](http://www.trustedinsite.com)

