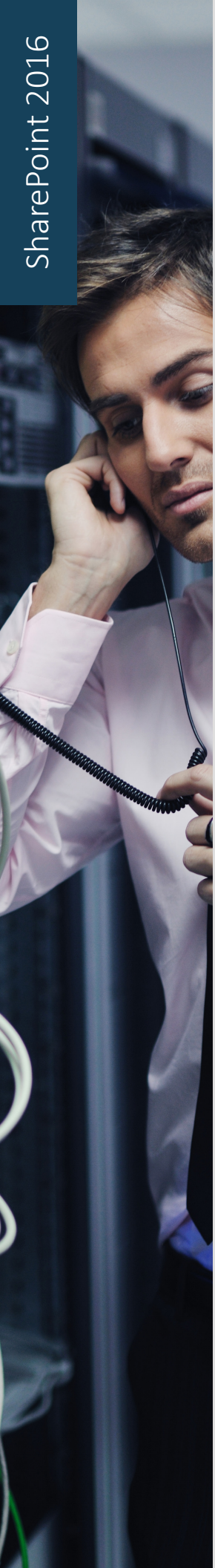
SharePoint 2016 and Data Security

With SharePoint 2016 on the horizon, many organizations are concerned about security-related features, particularly with regards to their integration with the Cloud. In this whitepaper, we'll explore some of the expected changes to data security in SharePoint 2016.

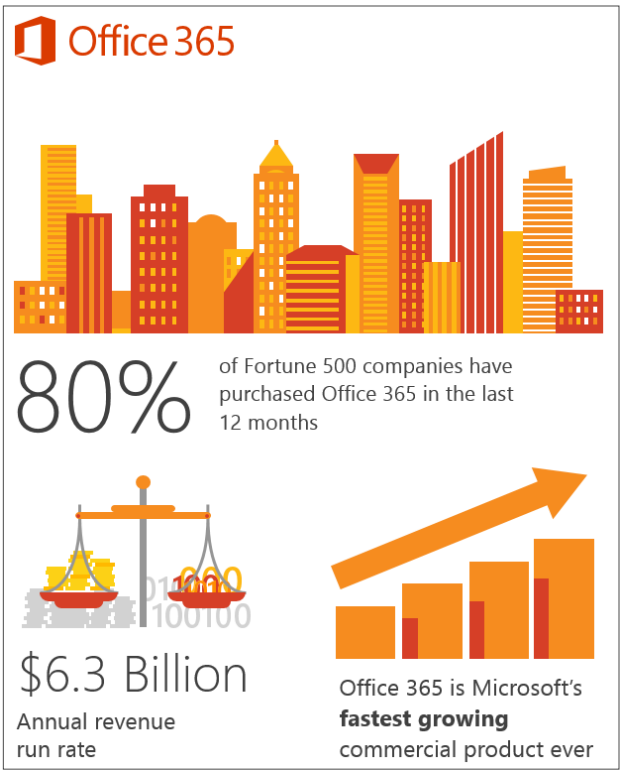
Crow Canyon Software



a brave new world

In recent months we've seen what can happen when sensitive information goes public. The number of data breaches, hacks, and leaks is jaw-dropping in terms of the sheer size and audacity involved. Morgan Stanley, Anthem, the IRS, Adobe, Evernote, eBay, etc... the list goes on and on. All of these companies suffered at the hands of both internal & external threats; typically the culprit was either malicious or, unfortunately, a result of poorly conceived Data Loss Prevention (DLP) policies. Ultimately, the end-results make the methodology moot — the bottom line is that highly sensitive data, such as social security numbers, credit card numbers, business communications, and bank account details were all exposed for the public to see.

Microsoft SharePoint and Office 365, in particular, are in quite a sensitive position. SharePoint has a huge footprint as the go-to content collaboration platform in business, with a 400% monthly active user growth and a 300% year-on-year content growth. By association, Office 365 is also entrenched in American business, with 80% of Fortune 500 companies purchasing Office 365 in the last 12 months. With over $6.3 billion in revenue, Office 365 is Microsoft's fastest growing commercial product in its entire history.



So there are plenty of reasons why Microsoft should be concerned about security in their business platforms. In addition to real-world risk factors, there's also the fact that security is the biggest obstacle standing in the way of Microsoft's dream of an all-Cloud world. Their hybrid philosophy is filling in the gap quite well, out of necessity, but make no mistake that the end-game will put a spotlight on product offerings that are 100% Cloud (i.e., subscription-based).

Right now the water coolers of the IT world are surrounded by computer professionals excited about next year's big release: SharePoint 2016. A key focal point for this latest iteration of SharePoint is how well it handles security-related issues. The solution is heralded as a prime representation of Microsoft's new hybrid approach, where on-premises installations are supported while facilitating access to Cloud Accelerated Experiences (e.g., search, distributed team sites, and compliance features). This crossover between on-premises and the cloud raises some legitimate concerns about how cloud features are implemented, particularly for compliant-focused sectors. Recently we've been sharing some thoughts about SP2016's new features but, in this whitepaper, we'd like to put the focus on security; specifically, how will SharePoint 2016 address data security?

a balancing act

It's hard to talk about peanut butter without mentioning jelly; afterall, they go hand-in-hand. SharePoint and Office 365 are the peanut butter & jelly of the business/IT world. This past year the integration between them has increased to the point where Microsoft has created a philosophy designed to merge the two worlds: hybrid. The fact is that organizations in compliant-heavy sectors cannot go full Cloud due to regulatory & legal requirements, but they'd love to have access to cloud-based features. Microsoft has addressed this challenge by continuing to support on-premises environments while offering access to the cloud for specific features. This is a balancing act of sorts required largely out of necessity. Some of these cloud features, largely the province of Office 365, include security-related functionalities that will be available to SharePoint 2016 users. This includes areas such as data loss prevention, document deletion policies, and even authentication standards.

controlling data with DLP

Data Loss Prevention (DLP) is a security methodology designed to ensure that end users do not send sensitive information to people outside of the corporate network (either knowingly or unknowingly). Microsoft has embraced DLP with a rollout of functionality to OneDrive for Business and SharePoint Online. The core concept here is that data should be protected no matter where it resides, whether it's in an e-mail being typed in real-time or in a PowerPoint document. Essentially, administrators use the Office 365 Compliance Center to create DLP policies, which are then broadly enforced across all user end-points, such as SharePoint or within individual Office 365 applications. For example, if a user enters questionable information in an e-mail, a notification will appear informing them of the issue — the user can then change the data or, if they have sufficient permissions, can even modify the policy on-the-spot.

The architecture used supports protection for both cloud and on-premises installations. Data at rest and in-transit (e.g., company network - user - cloud) is always encrypted. In addition, administrators have access to full audit logs of all activities in the SharePoint / Office 365 universe.

DLP, sensitive information types, and sharepoint 2016

DLP functionality within the Office 365 framework is also extended to SharePoint 2016 administrators; in fact, a new feature called Sensitive Information Types will be introduced in SP2016. Sensitive Information Types are used to help users search for sensitive content in their existing eDiscovery Center.

Sensitive Information Types are defined by patterns identified by regular expressions (or a function) and are available for use in DLP policies. For example, some types may be designed specifically for detecting highly-sensitive numbers, such as social security numbers, credit card numbers, and bank account numbers. The types combine pattern matching with corroborative evidence (e.g., keywords, checksums) to discover data for analysis — the analysis phase leverages native confidence levels with proximity logic to determine whether data is sensitive or not. Once discovered, additional actions can be specified via the DLP policy (e.g., no export allowed).

With regards to usage, Sensitive Information Types will be built into Enterprise Search. SP2016 users will be able to use the Office 365 Compliance Center to include pre-defined Sensitive Information Types in their DLP policies. At the moment DLP will include 80 different Sensitive Information Types that represent typical data scenarios across a wide range of industry segments and geographies.

intelligent document life management

There are a number of industry sectors, both public & private, that are subject to regulatory compliance measures. Healthcare, government organizations, life science, and utility companies are examples of organizations that are highly regulated and, consequently, must comply with strict information management laws. The continued growth of litigous actions have resulted in the need for companies to follow guidelines with regards to the maintenance, modification, and deletion of sensitive documents.

This isn't as straightforward as it may initially sound. If documents are retained for too long, then they may pose an unnecessary legal risk. If they are modified or deleted too soon, then legal actions may also be taken. Document life management is a tricky business and, fortunately, is a topic that will be addressed in SharePoint 2016.

SP2016 administrators will be able to use the Office 365 Compliance Center to access the Document Deletion Policy Center. Policies created therein can be assigned to a site collection, with each policy comprised of one or more rules (note that only one rule can be active at any time). Policy implementation will be flexible: a mandatory policy can be applied to a site collection or a "menu" of policies can be presented to site owners so that they can select the most appropriate one. SharePoint 2016 will place a particular emphasis on deletion policies and rules.

Administrators will be able to create deletion rules that enable them to specify a time period until deletion, when to calculate the deletion date (i.e., from date of creation or date of last modification), and whether to delete the document permanently or simply move it to the Recycle Bin. Policies can even include multiple deletion rules and site owners will be able to select the rule that is most relevant for their site.

overall security improvements

SharePoint 2016 has caught up with some industry security standards in terms of e-mail encryption and logon authentication. First, e-mails sent from SharePoint will now be encrypted using StartTLS connections. StartTLS increases the efficiency of computer resources by enabling users to automatically upgrade existing, non-encrypted connections to encrypted ones. The end-result is that servers can serve more users with less processing and memory overhead. In addition to Microsoft, other major service providers that have switched to StartTLS include Amazon, Dropbox, Facebook, Google, and Yahoo.

With an eye to its future in the cloud, Microsoft has switched from Windows authentication to SAML, a claims-based authentication method. The former, though workable, was not exactly scalable in terms of multi-vendor environments that support cloud and/or Internet based models. SAML, the Security Assertion Markup Language, offers a standardized singular point of authentication — user credentials never leave the firewall boundary. Identities do not need to be saved or synchronized,

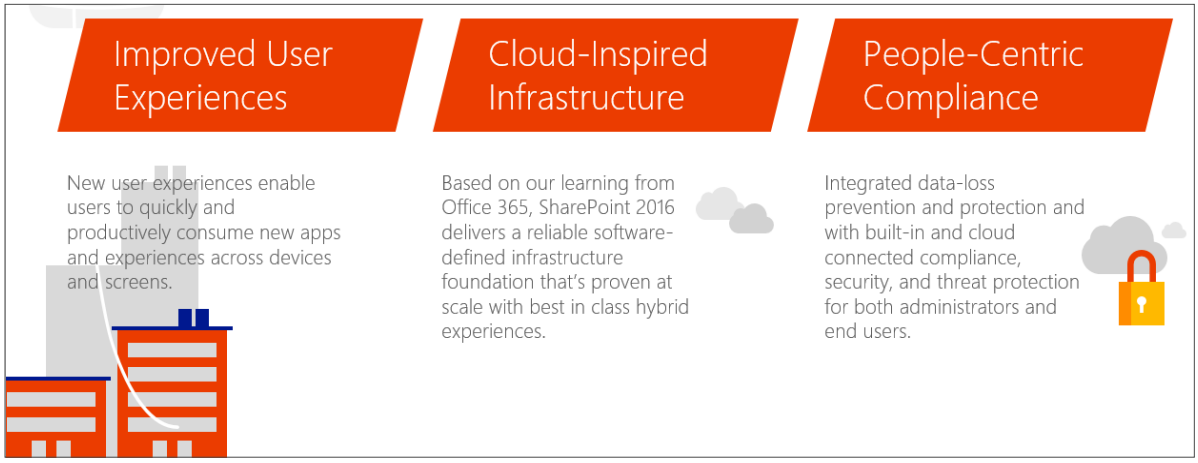
effectively minimalizing the likelihood of user credential compromise. Lastly, SAML is single sign-on friendly, enabling users to access multiple applications without the need to create/manage individual credential sets.

laying the foundations for cloud security

With an eye to the big picture, Microsoft is steadily laying the groundwork for an increasingly robust cloud-centric environment for SharePoint 2016 and also Office 365. On-premises installations will be around for quite awhile, due largely to regulatory requirements for compliancy-reliant business sectors. The growth of the Cloud, though, is starting to outpace traditional on-premises based functionality. Eventually on-premises functionality will be limited to the storage of critical and sensitive information, but this will take some time. In the interim we have Microsoft's hybrid approach, which effectively builds a bridge between cloud-friendly Office 365 and on-premises SP2016 environments with Cloud Accelerated Experiences.

All of this ties into the topic of security because organizational engagement with cloud services will always be prefaced by the question, "Is it safe? Will our information be at risk?". The more security that Microsoft bakes in to SharePoint and Office 365, the more likely that new customers will feel at-ease with the overall service offering.

Microsoft's vision for SharePoint 2016 includes not only improved user experiences, but a cloud-inspired infrastructure coupled with people-centric compliance — the latter two being highly interdependent. In short, the cloud is not viable unless users feel secure.



SharePoint 2016 will offer some interesting new functionality but, more than anything, it will be the foundation for future versions built on increasingly tighter cloud-based security. The hybrid approach is pulling all of us closer & closer to a world in which on-premises is used for highly-specific purposes while the Cloud reigns supreme. These are interesting times and we look forward to helping you explore your own unique SharePoint path.

Crow Canyon Systems

W: www.CrowCanyon.com
E: sales@crowcanyon.com
T: 1-888-706-0070