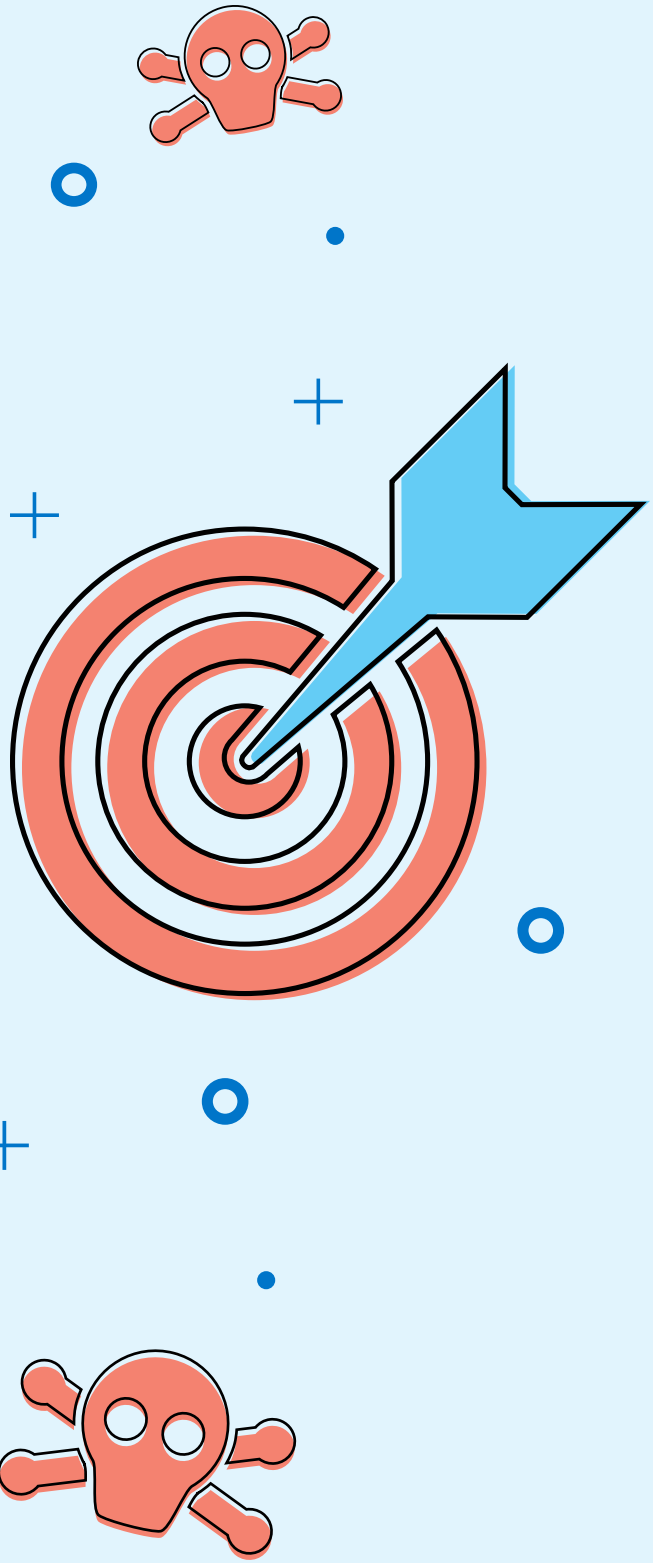
EBOOK

Defending Office 365 Data from Ransomware



Office 365 Business and Ransomware: The Lurking Threat

For small to midsized businesses Microsoft Windows based systems remain dominant. Windows continues to be the operating system most widely used on desktops and laptops. And Microsoft Office remains the most widely used work office suite.

So it's no surprise that Windows systems remain the top target for ransomware, too. A stunning 100% of IT professionals reported they had seen Windows systems infected by ransomware, as reported in Datto's State of the Channel Ransomware Report. Ransomware typically encrypts your files and promises to decrypt data after a ransom payment.

The collaborative capabilities of Office 365 make ransomware defense more challenging. Before Office 365, you wrote a Word document on your laptop, saved it on your system or file server, then emailed it as an attachment to share outside your organization. Copies of your file could exist in several places: your laptop, a file storage server, your sent email, and the inbox of the recipient.

Thanks to shared files and OneDrive sync, your files may be in more places than ever. A user that shares a document with colleagues can end up with copies on multiple laptops. Each person with editing access might sync a copy to their system. When one person gets ransomware, files get encrypted -- then the encrypted versions sync through to everyone else. The same is true for Sharepoint Online. As most business critical data is created in Sharepoint Online libraries, it's important to note that ransomware is easily spread there via the sync client.

In fact, 29% of IT professionals reported that their clients had encountered ransomware that targeted Office 365. It takes just one visit to a malicious site, one accidental download, or one infected attachment to unleash ransomware.

The following strategies and tactics will help reduce your ransomware risk, protect your networks and devices, and ultimately help you recover your data when a ransomware event occurs.

A once or twice-a-year browser deployment **leaves people needlessly vulnerable** to known and patched problems.

UPDATE TO REDUCE RANSOMWARE RISKS

Ransomware defense begins with an up-to-date operating system, an up-to-date browser, and up-to-date patches. For a single user, that's relatively easy to achieve. But businesses must manage a large number of devices. While tools exist to help upgrade, update, and patch systems at scale, too often administrators leave things alone. In the real world we see out-of-date, unpatched software more than necessary. So review the following items to reduce your ransomware risk wherever possible.

Operating System

Microsoft system requirements list Windows 7 Service Pack 1 as the oldest desktop operating system suggested for Office 365. Remember, though, that Microsoft first released Windows 7 in 2009, and that mainstream support for it ended in January 2015.

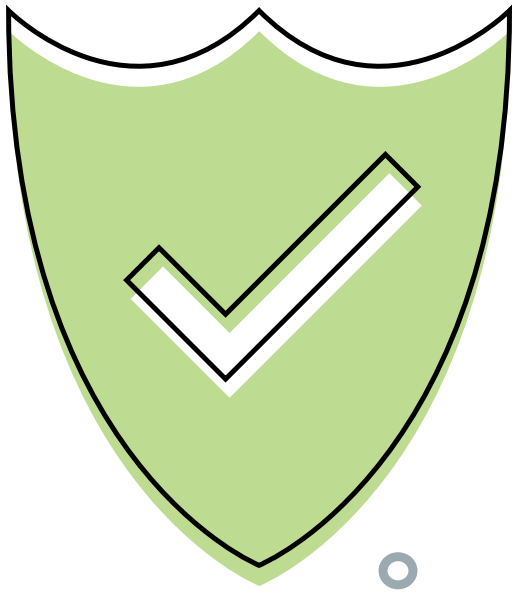
The first step is simple: run Windows 10 to reduce your ransomware risk. Microsoft found that "devices running Windows 10 are 58% less likely to encounter ransomware than when running Windows 7" in a "Ransomware Protection in Windows 10 Anniversary Update" report.

Browser

Microsoft built Office 365 to work with a variety of browsers, including Chrome, Firefox, and Safari, as well as Internet Explorer and Microsoft Edge. If you deploy Chrome, Firefox, or Safari in your environment, make sure these stay current, as well. Google updates Chrome about every six weeks, while Mozilla releases a new version of Firefox roughly every six to eight weeks. A once or twice-a-year browser deployment leaves people needlessly vulnerable to known and patched problems.

Of Microsoft's two browsers, choose Edge to reduce ransomware risks. Edge lacks support for some legacy features, such as ActiveX, that increased the potential for

A third-party DNS service provider may block specific sites. Some businesses use DNS to filter a variety of websites spanning from social media to online retailers.



security problems in Internet Explorer. If you use Internet Explorer, upgrade to Internet Explorer 11, which will run on Windows 7 Service Pack 1 systems and all newer Windows operating systems. Both Edge and Internet Explorer 11 offer SmartScreen Filters to help guard against malicious sites and downloads.

Patches

Finally, while it may seems obvious, apply patches promptly. Ransomware and other malware pursue multiple paths around defenses—so it's not enough to just update to devices monthly. An unpatched laptop that connects to your network, servers, or OneDrive today, may deliver malicious code to encrypt every file it can find tomorrow. So patch promptly.

THREE TACTICS TO THWART OFFICE 365 RANSOMWARE THREATS

DNS

Switch to a DNS (domain name system) service that actively monitors and blocks known malware sites to reduce the risk of ransomware. Unless you've custom-configured some settings, it's very likely that a site's DNS provider is the internet service provider. When anyone on the network types, say, "www.datto.com" in a browser, that request goes to the DNS provider.

A third-party DNS service provider may block specific sites. A third-party DNS service provider may block specific sites. Some businesses use DNS to filter a variety of websites spanning from social media to online retailers. More complex configurations can block certain sites from specific user groups, but allow access from other groups' systems. Several vendors, such as Dyn, OpenDNS, and Untangle, offer these services.

DNS service providers can also block access to malicious sites. This blocking can work two ways: by blocking a request when a person inside an organization attempts to access a harmful site, or—if malware is already inside an organization—by blocking attempts by malware inside the organization to "phone home" outside the organization. When a device on the network requests a site identified as a ransomware source, the DNS provider prevents access. Instead of a fresh serving of malware, you see a notification that the requested site is blocked, often with a suggestion to contact a network administrator if you believe the site to be blocked in error.

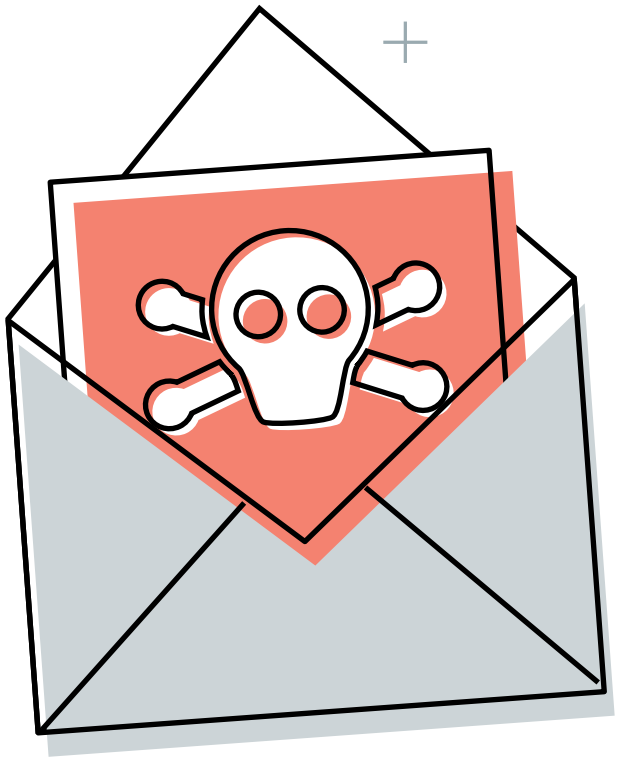
SmartScreen policies

Microsoft's SmartScreen filters work to block harmful sites and downloads at the browser level, much like a DNS provider can at the network level. The system calculates a risk score, based on a variety of factors, then warns the user of potential harm. SmartScreen works within both Microsoft Edge and Internet Explorer 11 browsers.

An administrator can configure SmartScreen to act either as an advisor or a blocker. When set as an advisor, a person will see a warning when either visiting a potentially harmful site or downloading a potentially harmful file. But the warning can be ignored.

To ensure that SmartScreen filters are active, configure three group policies:

- Configure the SmartScreen filter setting to turn SmartScreen on,
- Prevent bypassing SmartScreen prompts for files, and
- Prevent bypassing SmartScreen prompts for sites.



Microsoft gives Office 365 administrators the ability to **block any of nearly 100 different file types**.

(On your own system, see SmartScreen settings for Internet Explorer in Tools > Safety settings, or for Edge in Settings > View Advanced Settings.)

With these settings, SmartScreen will block visits to sites identified as harmful and also prevent downloads of unverified files.

Email

Email attachments often deliver a ransomware payload. "Here's the file you need," reads the text of the email—with an attachment. Too often, the recipient opens the file—and realizes later that it really wasn't a needed file, but instead a malicious app.

Microsoft gives Office 365 administrators the ability to block any of nearly 100 different file types. The most secure setting would be to simply delete all attachments. Anyone really needing to share files with people could upload a file to OneDrive, then share access. The recipient would receive a notification via email—but not the actual file! — and could then login to OneDrive to view files "Shared with me".

You should block files likely to be harmful. According to a Microsoft Security Intelligence Report from June 2016, the file types most often blocked by Office 365 Advanced Threat Protection were Word (.doc, .docm), JavaScript (.js), and executable files (.exe, .scr, .com, .pif, .cpl).

To block these settings, login to your Office 365 Admin account, select the Security & Compliance tile, choose Threat Management, then Anti-malware. There, you may either edit the default configuration, or add additional screening criteria. A core set of executable files is blocked, including the following types: .ace, .ani, .app, .docm, .exe, .jar, .reg, .scr, .vbe, and .vbs. In addition to these defaults, you might also block the following types: .js (JavaScript file extension), .rar (a compressed file type), as well as .cpl and .pif, to protect against the most common concerns.

You may be able to **revert to an earlier version of a ransomware-encrypted file**, since OneDrive for Business saves file version histories.

You may also block attachments for specific sender or recipient users, groups, or domains. In a work setting, you might choose to prohibit attachments among management, but allow attachments among the C-level. When you create your anti-malware rule, choose the sender or recipient settings (found near the bottom on the rule configuration screen).

RECOVERING FROM AN ATTACK

Go offline

When you discover ransomware on a system, remove the system from the network immediately. Unplug any ethernet cables and turn off any WiFi connections on the device. If you can't change the WiFi setting, move the device out of range of your network. Isolate the system to prevent ransomware from infecting other networked systems.

Disable sync services, such as OneDrive Sync to prevent the system from syncing any ransomware-encrypted files to OneDrive and other cloud services. Pause the OneDrive sync client on the local device, if possible.

Restore files with OneDrive for Business

You may be able to revert to an earlier version of a ransomware-encrypted file, since OneDrive for Business saves file version histories. From a system not affected by ransomware, access OneDrive in the browser, select a file, then choose "Version History". A list of the saved versions of the file—with modification dates—will display. You can view earlier versions of the file, then choose "Restore" when you find a version not affected by ransomware.

Version history has limits, though.

You may still need to attempt to recover files from the ransomware-affected device. Run a **complete scan of the system** with your security software.

Restore works file by file. Choose a file, choose version, restore. You're done in a few seconds. Then repeat that process for every file. That can take time—and may not be practical if ransomware has encrypted thousands of files.

Version history works well for Office documents, such as Word, Excel, and PowerPoint files. But OneDrive for Business won't keep version histories for files from non-Office applications. So that Autocad, Photoshop, or video file saved to OneDrive won't offer the "version history" option. As of January 2017, unless your file is a Microsoft Office file, only one version will be saved.

Finally, version history is a setting. It can be turned off. If it has been turned off, this method of data recovery won't work.

Attempt on-device recovery

You may still need to attempt to recover files from the ransomware-affected device. Run a complete scan of the system with your security software. Or, try a complete scan with Microsoft's Malicious Software Removal Tool, followed by Windows Defender Offline. Hopefully, some combination of the above will remove the ransomware from your system to allow you to access files safely.

Restore from backup

An uninfected copy of your data offers the only real protection from ransomware. If you know your data is backed up, you can start again: erase your device, re-install your apps, then restore your data.

Datto SaaS Protection delivers cloud recovery of your Office 365 data. You can select a time before your files were locked by ransomware to restore. Datto SaaS Protection restores your email, files, folders, contacts and calendar items in their original, unlocked formats.

And, since it is in the cloud, you could even switch to a different device, login and restore your data to Office 365 from your Datto SaaS Protection data snapshots.

Datto SaaS Protection saves and secures your data. The system backs up your data automatically three times a day, and it encrypts your data to protect it. The systems have passed SOC 2 Type II audits, and include several audit logs, internal controls, and monitoring to ensure your data is always available.

Rebuild / Reimage

After you've recovered your data, you next need to restore your system to a healthy state. Often, you'll do this by restoring a standard disk image that contains your operating system and a default set of apps. Most large organizations store a few standard setups to aid a fast recovery. In the worst case, you'll have to meticulously reinstall everything manually: wiping the drive, installing an operating system, then re-installing your apps, then recovering your data from backups.

SUMMARY

Keep your systems current, leave less secure legacy browsers behind, and patch your systems promptly. Shield your network with filtered DNS, and similarly rely on Microsoft's SmartScreen to keep people safe from malicious sites and downloads as they browse. With a few tweaks to Office 365 settings, keep harmful attachments out of email.

Above all: back up your data. Rapid recovery of your data and systems is possible after a ransomware attack... but only if you have a backup.

For more information please contact:
Derrick Martin | Partner
Phone: 954-637-3090
Email: derrick@mwltec.com
MWL Technology, LLC | http://www.mwltec.com