ARISTO
CYBER DEFENSE

WHITEPAPER

Ransomware and Microsoft 365 for Business

What You Need to Know

Introduction

Microsoft Windows-based systems remain dominant for small to midsize businesses, and Microsoft 365 (formerly Office 365) SaaS adoption continues its rapid rise. SaaS productivity apps like Microsoft 365 make sense in today's mobile world—the benefits of easy access to documents from any device and easy collaboration are obvious.

Many organizations assume that moving to cloud-based collaboration in Microsoft 365 means email security and backup is no longer necessary. However, this can be a dangerous assumption. Microsoft 365 data is just as vulnerable to ransomware attacks as local data.

In this eBook, you will learn strategies and tactics to help reduce ransomware risk and ensure you can recover data when a ransomware event does occur.

Consider it essential to keep employees' browser software updated.

Reduce Microsoft 365 Ransomware Risks

Ransomware defense begins with up-to-date operating systems, browsers, and applications. Careful configuration of Microsoft 365 email filtering should also be considered essential.

OPERATING SYSTEM

Microsoft found that "devices running Windows 10 are 58% less likely to encounter ransomware than when running Windows 7" in their "Ransomware Protection in Windows 10 Anniversary Update" report. Be certain that your endpoint operating systems are updated and patched.

BROWSER

Browser software must be updated regularly as well. Microsoft 365 works with various browsers, including Chrome, Firefox, Safari, and Microsoft Internet Explorer, and Edge. Google updates Chrome about every six weeks, while Mozilla releases a new version of Firefox roughly every six to eight weeks. Consider it essential to keep employees' browser software updated.

APPLICATION PATCHING

Ransomware and other malware are designed to pursue multiple paths around defenses—so it's not enough to just update browsers monthly. Ongoing application patch management is another critical component of your ransomware defense strategy.

UPDATE DNS

Switch to a DNS service that actively monitors and blocks known malware sites to reduce the risk of ransomware. Several DNS vendors, such as Dyn, OpenDNS, and Untangle, offer these services.

However, relying on OneDrive as a form of backup can result in data loss.

USE SMARTSCREEN FILTERS

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. SmartScreen is available in Microsoft Edge and Internet Explorer browsers.

FILTER EMAIL

Microsoft 365 gives you the ability to block nearly 100 different file types. A core set of executable files is automatically blocked, including: .ace, .ani, .app, .docm, .exe, .jar, .reg, .scr, .vbe, and .vbs. In addition to these defaults, you might also block the following types: .js, .rar, .cpl, and .pif.

Protect Microsoft 365 from threats

With email being the most common attack vector involved in ransomware delivery, it is crucial to ensure your email is secure against such threats.

The basic Microsoft 365 package for SMBs provides some level of security. According to Microsoft, it includes spam filtering and basic threat protection. Unfortunately, this is not enough to secure Microsoft 365 from today's ransomware attacks. Ransomware attacks keep evolving, and new or modified ransomware strains emerge frequently. It is proven that the majority of these threats easily bypass this level of protection. Microsoft, too, recommends using Microsoft 365 in tandem with a more advanced email security solution. Taking a multi-layer approach, deploying an advanced threat protection solution on top of the basic security provided by Microsoft is a must-have nowadays. Many of these solutions are cloud-based and connect to Microsoft 365 through APIs, making them lighter and much easier to deploy than traditional Secure Email Gateways (SEG).

Several advanced threat protection solutions secure not just the email but all Microsoft 365 collaboration and productivity tools, including OneDrive, SharePoint, and Teams. Selecting such a solution will help you protect all communication channels, further reducing the risk of ransomware.

Various security products block malicious content before it reaches the end-user securing from ransomware and phishing, Business Email Compromise, and other attack types. Some of them are perfect for SMBs – they are easy to set up and maintain, seamless to end-users, and most importantly, highly effective.

Back up Microsoft 365 Data

Since Microsoft OneDrive stores a copy of a user's files in the Microsoft cloud, many people believe that it makes backup obsolete. However, relying on OneDrive as a form of backup can result in data loss. Here's why: If a file is deleted or infected on a local device, that change is automatically synced in OneDrive. In other words, the file is automatically deleted or infected on all synchronized devices. With Microsoft Teams usage increasing considerably due to social distancing and other remote work scenarios, this is an even greater concern.

On top of that, Microsoft does not guarantee complete and fast restores of deleted or corrupted Microsoft 365 data. The company does ensure that it won't lose your clients' data. However, it doesn't make any guarantees about recovering data if your client loses it.

When you discover ransomware on a device, remove/isolate that device from the network immediately to prevent ransomware from spreading to other networked devices.

This is commonly referred to as a "shared responsibility model" for data protection:

Microsoft provides:	You must protect against:
• Protection against loss of service due to hardware failure or natural disaster • Short-term protection against user and admin error (Recycle Bin, soft delete)	• Accidental deletion • Hackers, ransomware, and other malware • Malicious insiders • Departing employees

That's why Microsoft recommends third-party backup in the Service Availability section of its Services Agreement.

Third-party Microsoft 365 backup is the best way to protect against accidental or malicious file deletion, other user errors, ransomware, and data corruption. These solutions store backups independently from Microsoft servers and enable granular restores of Microsoft 365 files, folders, and applications.

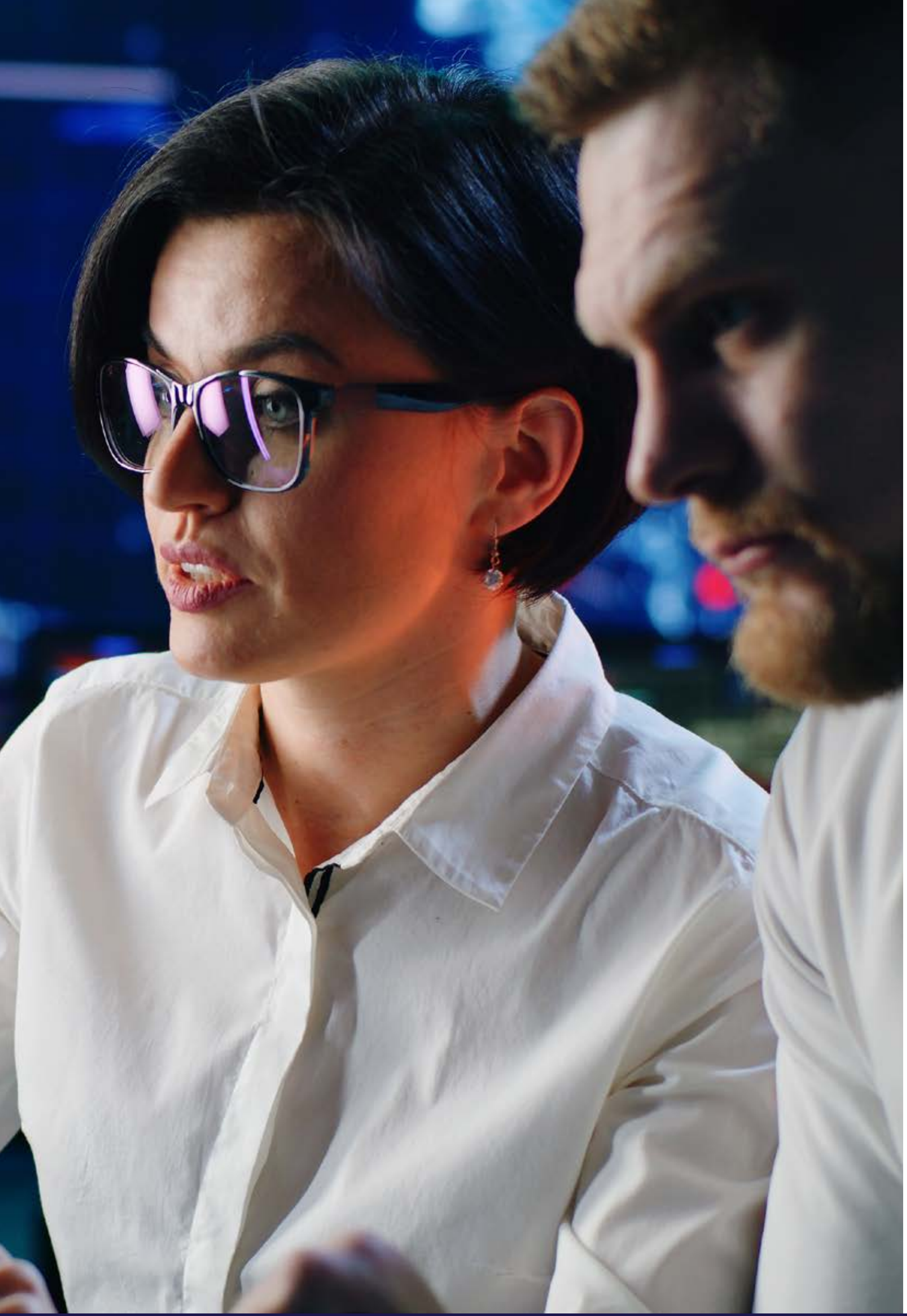
Recovering from an Attack

Even with precautions in place, attacks still occur and machines get infected. The following tips will help you minimize the extent of an attack and help you get back up and running quickly:

GO OFFLINE

When you discover ransomware on a device, remove/isolate that device from the network immediately to prevent ransomware from spreading to other networked devices. Unplug any ethernet cables and turn off any WiFi connections on the device.

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 FROM BACKUP

As noted above, creating regular backups of your data is the only way to be confident you can recover quickly from a ransomware attack. Remember that not all Microsoft 365 backups are created equally. For example, some solutions do not maintain folder structures in backups. So, after restoring files, users must rebuild and reorganize. This is a time-consuming, manual effort that impacts employee productivity—especially following a ransomware attack that impacts many users.

Still, others lack comprehensive support for the entire Microsoft 365 suite.

For example, some products lack protection for Teams. So, when selecting a Microsoft 365 backup tool, look for a secure, automated solution with support for the Microsoft 365 apps you rely on.

For example, Aristo SaaS Protection+ provides:

Advanced Threat Protection (SaaS Defense)	Simple, and Secure Microsoft 365 Data Protection (SaaS Protection)	Comprehensive Microsoft 365 Support (SaaS Defense & SaaS Protection)
• Detection and prevention of advanced threats • Minimal time to detection • Seamless deployment and management • No delay to end-users • Robust reporting	• Automatic backup to the Aristo Cloud • Point-in-time restore and export • Unlimited storage • Flexible retention • Easy on-boarding • 24/7 support	• Exchange • OneDrive • SharePoint • Teams

Conclusion

Ransomware attacks can result in significant, costly business downtime. Thankfully, there are ways to reduce risk and protect from threats.

Keep your systems current, leave less secure legacy browsers behind, and patch your systems promptly. Shield your network with filtered DNS, and rely on Microsoft's SmartScreen to keep people safe from malicious sites and downloads as they browse. Keep harmful files, links, and content out of email shared drives and chat tools with Advanced Threat Protection such as Aristo SaaS Defense.

Finally, take steps to backup your data. Rapid recovery of your data and systems is possible after a ransomware attack, but only if you have comprehensive backups.

To learn more, request a demo today.

ARISTO
CYBER DEFENSE

214-430-3522 ext. 101
info@aristocyber.com