Microsoft

Protect Your Data: 7 Ways to Improve Your Security Posture

Enterprise mobility, the flood of workplace devices, Software-as-a-Service application, and the cloud have transformed the way business operates, allowing business owners and employees to become both more mobile and more productive.

But the shift to mobile, cloud-based business has produced other changes as well, like a proliferation of personal mobile devices being used in work situation, dissolving business perimeters, and a greater use of public – or off domain – networks. While these shifts often result in increased productivity, they can also put businesses' sensitive data at greater risk of security threats, attacks, or breaches.

Is it possible to give employees the mobility and productivity they need in a modern workplace while also protecting your data? Yes.

In this eBook, we will discuss seven ways businesses can better protect data, and the actionable steps they can take to reduce vulnerability.

Protect Your Data: 7 Ways to Improve Your Security Posture is the first in a series of eBooks from Microsoft on the topic of security.

7 Ways to Improve Your Security Posture

- Reduce threats with identity and access management
- Manage mobile device and apps
- Leverage conditional access
- Increase enterprise data protection
- Prevent data loss
- Enable secured collaboration
- Reduce malware exposure

Reduce threats with identity and access management

Often the weakest links in security are employees, whether by accidentally leaking sensitive data or exposing their credentials in social networks. This is in part because maintaining control over applications across corporate data centers and public cloud platforms has become an increasingly complicated challenge.

Workers want to access resources and technology from a variety of locations and devices. This increased mobility can result in a number of complications from a security perspective including password and location-based access management concerns.

External attackers seek corporate vulnerabilities – like leaked credentials – to access networks and steal customer information, intellectual property, or other sensitive data. This puts your business at severe risk of financial, legal, or public relations damage. Internal breaches can expose your data to risk as well. How do you ensure control of the what, the when, the where and the who of application access?

Identity and access management can help reduce the risk.

- Eliminate the need for multiple credentials with a single identity to access cloud and on-premise resources
- Limit individual access to what employees need to do their jobs.
- Revoke access privileges when an employee changes roles, leaves the company, or no longer requires access to certain shares.
- Enforce second factor authentication based on risky behaviors.

- *More than 80 percent of employees admit to using non-approved software-as-a-service (SaaS) applications in their jobs*[1]

[1] Source: "The hidden truth behind shadow IT – six trends impacting your security posture" (Frost & Sullivan)

Learn more:

- *Identity + Access Management*

Manage mobile device and apps

As the Bring Your Own Device (BYOD) trend grows and the use of Software-as-a-Service (SaaS) applications proliferates, security concerns multiply. Critical data is being stored with greater frequency in the public cloud, which is not always governed by the same security standards as private cloud or on-premises solutions. This reality is forcing businesses to adapt quickly to maintain tight security.

Anytime devices are stolen, lost, or simply left unattended data is left vulnerable and under-protected. It's also vulnerable when your corporate data leaks into personal applications. In this age of BYOD, how do you help protect your data without compromising employee productivity?

Begin with the basics:

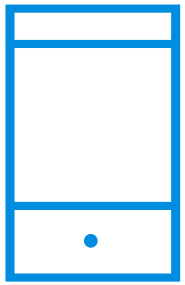
- Don't disrupt the user flow; make it easy and natural for them to comply. Consider managing important applications rather than the entire device.
- Be transparent about what IT is doing to employee devices.
- Protect only the corporate data. Look for solutions that enable employees to freely use the device for their personal purposes.

- *An estimated 52 percent of information workers across 17 countries report using more than three devices for work*[1]

[1] Source: "Employee devices bring added security concerns," by Cindy Bates (Microsoft US Small and Midsize Business Blog)

Learn more:

- *Microsoft Intune*



Leverage conditional access

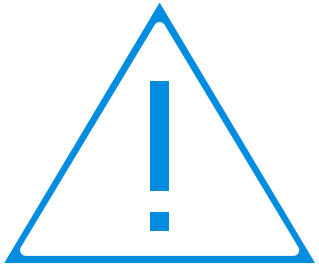
Conditional access restricts access to corporate resources based on either user identity, or device health. It's also about enforcing policies based on location and application data sensitivity. For example, accessing a Customer Relationship Management (CRM) application from a café requires multi-factor authentication because of both the location of the user and the sensitive data of the CRM system. Another example would be in email. A device must be compliant with policies, like encryption and PIN, to access corporate email. Properly enforcing conditional access policies across a company can improve an overall security posture.

What are your first steps to getting a policy in place?

- Define a mobile device access policy that works for your business. You can either require full management of the device or just management of critical applications like Outlook to access corporate email.
- Leverage dynamic groups to give employees access to the applications they need based on their roles.
- Enforce multi-factor authentication this adds a layer of protection by requiring users to authenticate themselves two ways. The first method may be the traditional user name and password combination. The second often involves a physical component that would be virtually impossible to duplicate. For example, swiping a card key and entering a PIN, logging into a website and using a one-time password, logging in via a VPN client with a digital certificate, or scanning a user's fingerprint.

Learn more:

- *Azure Active Directory conditional access*
- *Conditional access overview*
- *Conditional access with Microsoft Intune*
- *Office 365 with Mircosoft Intune*
- *Windows 10*



Increase enterprise data protection

Mobile workplaces can greatly increase productivity and access to work-related resources, but they also increases the risk of accidental data leaks through apps and services like email, social media, and the cloud. Providing a safer environment for employees to work remotely is key to maintaining a more secure business while enabling mobile productivity. For example, an employee might send the latest engineering pictures from their personal email account, copy and paste information into social media, or save an in-progress report to their personal cloud storage. How can you allow personal devices, but without compromising the security of your data?

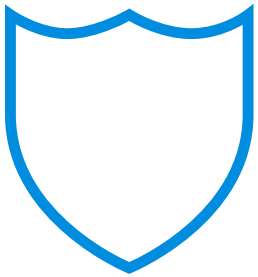
Enterprise data protection (EDP) helps protect against potential data leakage to unauthorized apps or locations without taking away from an employee's work experience.

To get started:

- Ensure devices are fully encrypted in case they are lost or stolen.
- Enable EDP in your enterprise environment, which will allow you to manage and regulate apps and data without making unnecessary changes.

For more information, see:

- *Windows 10 Enterprise Data Protection*
- *BitLocker Overview*
- *Microsoft Intune*



Prevent data loss

Sharing documents through email and other online tools is an important productivity tool for workers, but to err is human. Employees can easily send information to the wrong recipient, or attach the wrong document, inadvertently sharing access to sensitive data. Security professionals must understand the risks and benefits of data sharing and develop appropriate plans to minimize data loss to keep greater security. That said, how do you allow employees to share files in email without endangering your sensitive information?

Start by reducing the likelihood of a leak:

- Learn more about the data loss prevention (DLP) capabilities within your ecosystem to protect your data where it is stored, when it is moved, and when it is shared. For example, an email can be limited to distribution within an organization or carry a digital rights management qualification that restricts who can open it.
- Extend DLP beyond email as well. Certain word processor, spreadsheets, and presentation programs also offer restricted access options that prevent unauthorized users from opening files.

For more information, see:

- *Office 365 Data Loss Prevention (DLP)*
- *Microsoft Office 365*

Enable secured collaboration

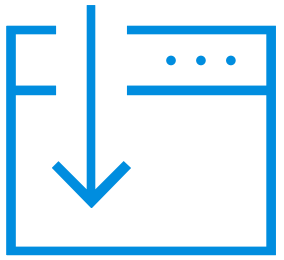
When it comes to sharing information, convenience often trumps security, which makes for a security professionals living nightmare. Workers can get creative with how they share information, putting your data in jeopardy and your company at risk of losing critical data. How do you encourage workers to collaborate while minimizing risks of compromised information?

Offer a flexible, easy-to-use, secured solution that meets their needs.

- Establish secured tools for sharing information, and ensure the right workers have access. This includes a secured document sharing solution, such as a SharePoint, restricted-access network share, or cloud-based solution.
- Require a digital rights management or other secured email solution to be used when sending sensitive materials through email.
- Provide easy and secured information-sharing workflow to enable both internal and external collaboration

Learn more:

- *Azure Rights Management*
- *Sharing protected files*
- *Sending encrypted emails*
- *Mircosoft Office 365*
- *SharePoint*
- *Microsoft Azure*



Reduce malware exposure

Malware infections can often be traced back to user error. Phishing and spoofing schemes have become extremely sophisticated, tricking users with fake emails from trusted brands, luring them in with fake news stories, and convincing them to download innocuous-seeming apps that contain hidden attacks. You can't stop users from surfing the web, using social media or accessing personal email on their own devices. How can you help them do these everyday tasks more safely?

Education is your first line of defense.

- Ask employees to read basic guidance and/or complete training that details common methods of malware attack.
- Teach users to double check URLs in email to make sure they seem relevant, accurate, and legitimate. And consider implementing email protection solutions that can help prevent malware and phishing attempts from reaching employees' inboxes.
- Suggest that workers limit their app usage to those downloaded from a reputable source.

Learn more:

- *Windows 10*
- *Windows Defender*
- *Windows Device Guard*
- *Mircosoft Office 365*

Focusing on these 7 areas and stand to improve your organization's security

Allowing workers to be mobile does not have to mean endangering your data's security. With proper planning, the right tools, and education, you can give your employees the freedom to work anywhere, anytime while minimizing risk.

Learn more about cybersecurity