Protect Your Data: 7 Ways to Improve Your Security Posture
There’s no question that enterprise mobility, the flood of workplace devices, SaaS apps and the cloud have transformed the way business operates.

Companies rely on collaboration and mobility to gain agility, improve performance and guide decision making. Mobile devices and applications in particular are powerful tools to stay productive. But as the number of mobile devices increases, app hosting is moved from owned to public or off-domain networks, and as antiquated business perimeters dissolve, companies face greater risks to security and non-compliance.

For instance, multiple log-ins, storing information in disparate, unmanaged locations or sharing information without full protection heightens vulnerability and increases the risk of data loss—including the risk of competitors stealing proprietary information or critical data being compromised or corrupted. Which begs the question:

Is it possible to give employees the mobility and productivity they crave while protecting your data?

Is it possible to let business groups use the new applications and systems to be more agile?

In this eBook, we will discuss seven common data protection concerns facing companies like yours and the steps you can take to reduce the threats. This is the first in a series of eBooks Microsoft will be publishing on security.
7 Ways to Improve Your Security Posture

- Reduce threats with identity and access management
- Manage mobile devices and apps
- Leverage conditional access
- Increase enterprise data protection
- Prevent data loss
- Enable secured collaboration
- Stop malicious code
Reduce threats with identity and access management

As you know, maintaining control over applications across corporate datacentres and public cloud platforms has become a significant challenge. Workers want to access data resources from a variety of locations and devices. Once on the network, they need access to a variety of resources that change over time. And, employees may request access to corporate resources to get their work done away from their desk.

Unfortunately, the weakest links are often employees, whether by accidentally leaking sensitive data or exposing their credentials on social networks. An external attacker could use those credentials to access the network and steal customer information, intellectual property and other sensitive data. And 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 behaviours.

More than 80% of employees admit to using non-approved software-as-a-service (SaaS) applications in their jobs

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

Learn more:

- Identity + Access Management
Data Protection

Begin with the basics:
• Don’t disrupt the user flow; make it easy and natural for them to comply
• Be transparent on what IT is doing to its devices
• Protect only the corporate data

As the Bring Your Own Device (BYOD) trend and the use of Software-as-a-Solution (SaaS) applications proliferate, security concerns multiply. As companies rely more heavily on SaaS application, some of their critical data lives in the public cloud and therefore is at greater risk and not controlled by the same standards IT has today.

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

An estimated 52% of information workers across 17 countries report using more than three devices for work.¹


Learn more:
• Microsoft Intune
Leverage conditional access

Conditional access is restricting access to corporate resources based on either user identity or device health. It is 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 with email. A device must be compliant with policies, like encryption and PIN, to access corporate email.

What are your first steps?

• Put in place a mobile device access policy. You can either require full management of the device or just the 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 in 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 Microsoft Intune
• Windows 10
Increase enterprise data protection

Allowing employees to use their own devices increases the risk of accidental data leaks through apps and services like email, social media and the cloud. These are outside of your control. 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. You want to allow personal devices, but without compromising the security of your data. How can you do both?

Enterprise data protection (EDP) can help protect against this potential data leakage to unauthorised apps or locations without taking away from the employee experience.

To get started:
- Enable EDP in your enterprise environment, allowing 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

To err is human—but we all know that the cost can be steep. Sharing documents through email is an important productivity tool for workers, so security professionals are caught in a conundrum: How do you allow employees to share files via 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 organisation or carry a digital rights management qualification that restricts who can open it.
- Extend DLP beyond email as well. Certain word processor, spreadsheet and presentation programs also offer restricted access options that prevent unauthorised users from opening documents.

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 professional’s 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 minimising 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
- Microsoft Office 365
- SharePoint
- Microsoft Azure
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 defence.
• Ask employees to read basic guidance and/or complete training that details common methods of malware attack.
• Double check URLs in email to make sure they seem relevant, accurate and legitimate.
• Suggest that workers limit their app usage to those downloaded from a reputable source.

Learn more:
• Windows 10
• Windows Defender
• Windows Device Guard
• Microsoft Office 365
Focusing on these 7 areas and stand to improve your organisation’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 minimising risk.

Learn more about cybersecurity