Red River

SECURING YOUR MOBILE WORKFORCE WITH OFFICE 365 **ENTERPRISE MOBILITY + SECURITY**

INTRODUCTION

Today's businesses aren't limited to four walls, a roof, and a single network. They are an amalgamation of many different services, technologies, and people, all connected by the cloud. There are obviously a lot of advantages to this model since it allows team members to work while on-the-go and businesses to expand their potential talent pool.

Powerful tools such as SharePoint and OneDrive make it even easier for teams to coordinate from different locations. As you are no doubt aware, there are disadvantages to operating this way, especially when it comes to security. More endpoints means that there are more open doors for security vulnerabilities. Many times end users, when faced with multiple logins, will just default to a "favorite" and use it across all their applications.

This creates a problem: how does your business leverage the power of a mobile workforce while keeping its data secure?

Microsoft has responded to this problem by creating a tool that secures both apps and devices, all without hindering collaboration. The Microsoft Enterprise Mobility and Security suite offer real-world tools designed to improve the end-user experience with single sign-on, plus keep data safer on any device with multi-factor authentication. But these are only two of the benefits; the O365 EMS suite is the a comprehensive tool that also protects end-user devices and documents, monitors the dark web, and offers conditional access controls from a single administrative portal.

This guide will walk you through Microsoft's Enterprise Mobility and Security package. It will help you understand the costs and benefits of this tool to help improve employee productivity while increasing your data security across the entire enterprise. At the end of the guide, you'll know exactly why Microsoft Enterprise Mobility and Security is the best tool on the market to manage remote employees on any digital device.

WHY OFFICE 365 EMS?

Office 365 Enterprise Mobility and Security addresses two major trends:

- An increasingly mobile workforce that needs to be able to collaborate seamlessly across different locations and devices. Smart Insights suggests that the majority of our workforce today are multi-platform users. They expect to be able to move seamlessly between online content viewed on their personal or corporate smartphone, to a desktop or tablet.

- Data breaches are growing exponentially, with disastrous implications for businesses that suffer a breach. Market Watch says there were 1,300 publicized data breaches in 2017. That's exponential growth from the 200 breaches we saw in 2005. Also, Identity Force said there was a 45% increase in data breaches in 2017 compared to 2016. Some of the biggest names in business have been hacked and had data stolen, from Uber to Equifax, the federal IRS, Orbitz, and Target.

- Data breaches are more frequently tied to theft of end-user credentials. Take the case of Blue Cross Blue Shield, where the mega-insurance carrier was breached when hackers stole employee login credentials. Consumers lost Social Security Numbers, names, birthdates – more than enough information to light up the dark web.

Kiplinger published an article that reads like a who's who of retail hacks so far in 2018, including Lord & Taylor, Panera Bread, Saks Fifth Avenue, Sears, and Best Buy. Every day a new business struggles to keep corporate data safe. Many of these breaches start with a simple employee download of an unprotected app or a malicious email.

Office 365 EMS offers multiple security management tools to shore up the walls of your data security. Microsoft Intune is the engine behind the part EMS offering, and this software allows companies to:

- Manage all of the mobile devices used by employees to access company data. This includes enrolling and inventorying devices for IT managers and configuring them to make sure they follow corporate security policies.
- Manage mobile applications used by those devices and desktops, tablets, or other hardware. It allows you to configure the apps with standard security policies and remove corporate data. You can also update security features and track and report on how the applications are being used.
- Protect corporate information by controlling how it is shared and accessed by the end user, including restricting actions such as downloading, saving, and copying.
- You can also conduct selective or corporate wipe of specific data from the device.
- Applies single sign-on authentication and multi-factor authorization across all enrolled devices.
- Keep personal data separate from corporate data on digital devices. The data accessed with corporate credentials has additional security policies applied, but this does not. cross back over to personal data. That way, IT managers can safely manage access to corporate data without running into privacy and control issues related to personal data.

The Office 365 Enterprise Mobility package can do all these things. Typically, we see the phrase "mobile application management" applied to one or a couple of these features. Microsoft's solution is a comprehensive product that stretches across their ecosystem. In fact, there's no other all-in-one security and productivity package on the market currently that can solve some of the most common problems found in our dispersed networks today.

CHOOSING AN OFFICE 365 EMS LICENSE

Microsoft offers a full suite of a la carte and bundled software options, so we know understanding the differences in licensure can be challenging. For the Office 365 Enterprise Mobility and Security suite, you have two licensing options: E3 and E5 license.

An E3 license provides all of the core features of Office 365 EMS:

- Multi-factor authentication
- Mobile device management
- Application Management
- Access control
- Advanced security reporting
- Advanced Microsoft Office 365 data protection
- Integrated PC management
- Integrated on-premises management
- Persistent data protection
- Document tracking

The E5 license provides everything in the E3 license, plus:

- Risk-based conditional access
- Privileged identity management
- Intelligent data classification and labeling
- Microsoft Cloud App Security
- Azure Advanced Threat Protection

With an E3 license, you can set basic permissions on what data can be accessed and by whom. With an E5 license, Office 365 EMS will look a number of different factors, including who is trying to access the data, where they are trying to access the data from, what device they are using to access the data, and whether they have permission to access the data. With an E5 license, Office 365 EMS is sophisticated enough to identify suspicious situations and respond accordingly.

For example, if a salesperson downloads a sales resource while in Boise, then 20 minutes later their credentials are used again, but this time to access sensitive company financial information from a location in China, then the EMS can automatically lock the account.

It's important to note that, no matter what license you choose, Office 365 EMS will work on PC or a Mac, Windows tablets, iPad or Android tablets, and most of the mobile devices on the market today. With each single-use user license, you can install these tools on up to five PCs or Macs, five tablets, and five phones.

SETTING UP

OFFICE 365 EMS

There are several steps necessary before rolling out Office 365 EMS. They include:

- Identifying Goals
  Understanding what proprietary data your company needs to protect along with recognizing the data that hacker's might deem important will help inform configuration of Office 365 EMS. What policies will be necessary to protect these vulnerable areas?

- Identifying Leaks
  Discussing and identifying security gaps and vulnerabilities is the next step toward building a wall between your corporate devices and hackers. Do you have users frequenting public Wi-Fi or are they potentially using unsecured devices? Are users downloading games or other media on the same device where they're accessing your data? Knowing the risk is the only way to mitigate it.

- Devising a Plan
  Red River can help your team create and implement a security roadmap with a full suite of Microsoft tools that protect you from leaks in the system. From multi-factor authentication to mobile and ap plication management, we offer comprehensive planning and risk mitigation to keep your data safe.

ROLLING OUT OFFICE 365 EMS

There are really three steps to setting up Enterprise Mobility and Security with Microsoft:

1. Activating Microsoft Azure.
2. Create end-users.
3. Establish Enterprise Mobility and Security.

One of the most requested features in the Enterprise Mobility and Security suite is multi-factor authentication. When an admin sets up the device, the user must supply a password and a response unique to their registered device to verify their identity.

When the user logs in for the first time, they will receive an email with important configuration information, in a handy self-service process for new users. This configuration allows the user to select how they want the two-step process to work; with a text that includes a verification code or some other way.

You can even set up update compliance, which monitors which devices need software updates. It's an incredible tool that lets you see at a glance which devices are safe, and which need updates. It's just another layer in Microsoft's O365 EMS – but a particularly important one.

MAXIMIZING O365 EMS WITH RED RIVER

Organizations are increasingly outsourcing IT support to third-party vendors like Red River. The benefits are clear: We can improve user productivity by providing setup and support for Office 365 products.

Rolling out Office 365 EMS is not an easy task; it takes a specialist to accurately create a plan and then implement EMS to meet the security needs of your company and it’s end-users. Red River routinely develops these security policies and then provides a managed service to monitor best practices.

For organizations that want the security protections found in O365 EMS but don’t have a large IT team to manage it, Red River offers managed security packages to help organizations stay ahead of threats:

- Red River MobilityPlus with Microsoft Intune is a collaborative package of high-end mobile technology managed by a certified Microsoft partner. It includes 24/7 help desk support, training, configuring and monitoring of Office 365 Enterprise Mobility and Security.

- Red River AccessPlus is a managed services package that supports changes, moves, or adds to Micro soft Conditional Access. This service manages the policies for contextual controls, like the user, device, location, and application.

- Red River IdentityPlus manages the process of setting policies that will restrict access, including features like dark web monitoring as an added layer of protection for your business.

Together, these tools create a virtually layer of security for your company, protecting both from user error that will put the company at risk, outdated software lacking the latest security upgrades, and potential threats that can arise from the dark web. Red River is a Microsoft Tier 1 Cloud Solutions provider, offering our customers the best service and expertise for these powerful tools.

CONCLUSION

CSO says fifty-eight corporate records are stolen every second at a cost of $141 per record. These staggering statistics came from the 2017 IBM Ponemon Institute report that put the global average cost per data breach at $3.6 million.

Your employees want the ability to use their personal devices to work from anywhere. One of the biggest challenges today is managing these dispersed teams in a way that ensures their privacy on personal devices while still allowing them access to corporate data without putting your firm at risk of data breach.

Today, the Microsoft 365 Office Enterprise Mobility and Security suite of products can manage every personal or corporate device accessing your network. These tools can be implemented now via a low-cost subscription. Red River is standing by to support these tools in a managed services package that will help you create top-of-the=line security at an affordable price.

Secure your mobile workforce ASAP, contact Red River to learn more.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.