The Complete Guide to Azure Migration and Microsoft 365 Security

A PRACTICAL ROADMAP FOR EAST TENNESSEE BUSINESSES READY TO MOVE TO THE CLOUD SECURELY, CONFIDENTLY, AND WITHOUT THE GUESSWORK.

CENTRIWORKS

Security-First Managed IT for Small and Mid-Sized Businesses

centriworks.com · 865-524-1124

Table of Contents

Introduction

Moving to the cloud sounds straightforward, but doing it right takes planning. This section introduces what's at stake and why a thoughtful approach matters from the start.

Page 2

Why Move to Azure and Microsoft 365?

Take a closer look at what's driving businesses to the cloud, from rising hardware costs to remote work and growing security concerns, and what that shift really means day to day.

Page 3

Azure Migration Overview

From early planning to post-migration management, this section breaks the process down into clear, manageable steps.

Page 4

Building a Secure Azure Environment

Security is not something you add later. Here, you'll see how to set up Azure the right way from the beginning, with the right controls in place to protect your systems and users.

Page 5

Microsoft 365 Security

Most security issues start with users, email, or devices. This section focuses on how to protect the tools your team uses every day without making things harder to manage.

Page 6

Protecting Your Data

Your data moves constantly, so your protection needs to keep up. Learn how to keep sensitive information secure no matter where it's accessed or shared.

Page 7

Security Check & Assessment

Not sure where you stand today? This section helps you step back, ask the right questions, and spot gaps that may need attention.

Page 8

Next Steps

Once you understand the landscape, the next step is taking action. This section outlines how to move forward with a clear plan and the right support.

Page 9

Is your Azure migration creating security gaps you don't know about?

Deciding to move to Azure or adopt Microsoft 365 is usually an easy decision. Most business leaders already understand the appeal, from greater flexibility to easier scalability and better support for a modern workforce. The real challenge starts after that decision is made.

Azure handles the infrastructure behind the scenes, while Microsoft 365 is where your team works day to day. Because they're connected through the same identity and security layer, decisions in one directly impact the other.

Without a plan in place, migrations can introduce security gaps that didn't exist before, expose sensitive data during the transition, or leave you with an environment that technically works but lacks structure, visibility, and oversight. According to IBM's Cost of a Data Breach Report, misconfigured cloud environments are one of the most common contributors to security incidents, often increasing both risk and recovery costs.

This is where many businesses run into trouble. The intention is right, but the roadmap is missing.

This guide is designed to give you that direction. Whether you have an internal IT team, work with an outside provider, or fall somewhere in between, you'll find a practical look at the migration process, the security decisions that matter most, and how to better protect your users, devices, and data.

Inside this guide, you'll find:

- **A structured look at the Azure migration process: what happens, when, and why.**
- **The security decisions that matter most, and the ones most often overlooked.**
- **A breakdown of Microsoft 365 security tools and how to use them effectively.**
- **Practical guidance on protecting your users, devices, and business data.**
- **A self-assessment to help you understand where your environment stands today.**

When a cloud migration is done well, it creates a more secure and manageable environment that can grow with your business. When it's rushed, it can introduce risks that are harder to fix later.

Let's walk through what a well-planned migration looks like, and how to make sure yours holds up over time.

Why Move to Azure and Microsoft 365?

Before even considering migration, think about why it's important for your business. Moving to the cloud should solve real problems or support how your business operates today.

Your current environment is starting to cost more than it's worth

On-premises infrastructure has a shelf life. Servers age, software falls out of support, and over time, more effort goes into maintaining old systems than getting value from them. For many businesses, the tipping point happens over time. It might be a server replacement quote, a failed backup, or a security review that brought to light how exposed things really are.

Azure removes the dependency on aging hardware. Instead of large upfront purchases, you pay for what you use, scale when needed, and avoid investing in equipment that loses value immediately.

Your team doesn't work from one place anymore

If your staff work from home, visit client sites, or split time across locations, your systems probably weren't built for it. Microsoft 365 was. It gives your team secure, consistent access to email, files, and collaboration tools from wherever they work.

Security threats have outpaced most on-premises setups

Traditional environments weren't designed to handle today's attack patterns. As threats have evolved, many on-prem systems have struggled to keep up, especially without consistent updates and monitoring.

> According to Verizon's Data Breach Investigations Report, a significant majority of breaches involve small and mid-sized organizations, with common entry points including compromised credentials, phishing, and unpatched systems. Azure and Microsoft 365 include built-in controls to address these risks when properly configured.

The economics can work in your favor

Cloud platforms shift spending from large, unpredictable capital purchases to a more consistent monthly cost. That level of predictability matters when you're managing a budget.

That said, just because you've made the move to the cloud doesn't necessarily mean that you'll automatically save money. A poorly planned migration can lead to overlapping systems, unnecessary licensing, or security gaps that require expensive fixes later. The financial benefit comes from doing it right the first time.

What this means in practice

The businesses that see the most value from Azure and Microsoft 365 are not the ones that moved the fastest. They're the ones that began with a clear plan. They knew which systems to migrate, in what order, and how to secure them from the start.

That's what the rest of this guide is designed to help you do.

Understanding the Azure Migration Journey

An Azure migration works best when there's a clear plan in place.

When issues come up, it's usually because a step was skipped, rushed, or not fully thought through. A successful migration follows a structured process in which each phase builds on the one before it.

Here's what that typically looks like:

1. Plan & Align

Before getting started, define your goals, scope, and what success looks like. This step sets the direction for everything that follows and helps keep everyone aligned on priorities, timelines, and expected outcomes.

2. Discover & Assess

Next, take a close look at your current environment. This includes identifying all servers, applications, and workloads, along with their connections. This step often reveals outdated systems or potential risks that should be addressed before moving forward.

3. Decide on the Right Approach

With a clear understanding of the environment, determine the best path for each workload. Some systems can be kept as they are, while others may need updates or be retired altogether. Making the right decisions here helps avoid unnecessary costs and prevents old issues from carrying over.

4. Prepare Your Azure Environment

Before moving anything, make sure the Azure environment is ready. This includes setting up access controls, security policies, network configurations, and identity management so everything is structured and secure from the start.

5. Start with a Pilot Migration

Rather than moving everything at once, begin with a small group of low-risk workloads. This allows for testing the process, confirming everything is working as expected, and making adjustments early if needed.

6. Migrate in Phases

Once the pilot is successful, continue in planned stages. Each phase should follow a consistent process to help minimize disruption and allow time to address any issues along the way.

7. Validate & Optimize

After each phase, review how everything is performing. Check for stability, security, and overall performance, and adjust to improve efficiency and manage costs.

8. Decommission Legacy Systems

Once your systems are up and running in Azure, you can begin phasing out your on-premises infrastructure. This step is often put off, but doing it sooner helps cut costs, reduce security risks, and keep your environment easier to manage.

9. Managing Your Environment Over Time

Moving to Azure isn't the finish line; it's just the beginning. From there, it's all about keeping things running smoothly with regular monitoring, security updates, performance improvements, and adjustments as your business grows.

A structured migration protects your business both during and after the move. The greatest risks come not from technology, but from neglecting essential preparation or testing. Skipping these steps can jeopardize continuity, security, and future success. Make them non-negotiable.

Building a Secure Azure Foundation

Security shouldn't be added after migration. It needs to be built into the environment from the start, before the first workload moves to the cloud.

Many of the security issues businesses face in Azure aren't caused by the platform itself. They come from environments that lacked clear controls. Taking the time to build a strong foundation early prevents those gaps from forming later.

Here's what a properly secured Azure environment looks like across each layer.

Identity & Access: The Foundation of Everything

Every security decision in Azure starts with identity. Centralizing identity through Microsoft Entra ID allows you to manage access consistently across users, devices, and applications.

Multi-factor authentication should be enforced for all users, especially administrators. Access should follow a least-privilege model, where users have only the privileges they need to do their jobs. When identity is properly controlled, compromised credentials alone are far less likely to lead to a breach.

Network Security

Your network should be designed to limit exposure and control how systems communicate.

Use virtual networks and subnets to segment resources. Apply firewalls and security rules to restrict traffic between systems and to and from the internet. The goal is to contain risk. If something is compromised, it should not be able to move freely across your environment.

Computer & Application Security

Virtual machines and applications need to be hardened before and after deployment. This includes keeping systems patched, enabling endpoint protection, and reviewing configurations for anything exposed to the internet. Reducing the attack surface is one of the most effective ways to prevent issues before they start.

Data Protection

Data should be protected by default, not added later as a fix. Encryption should be in place for data at rest and in transit. Access to storage and databases should be tightly controlled. Tools like Azure Key Vault help secure secrets, keys, and certificates so they are not exposed or mismanaged.

Monitoring & Threat Detection

Visibility enables you to respond quickly when something goes wrong. Centralized logging and alerting give insight into activity across your environment. Threat detection tools can identify unusual behavior, while automated responses can help contain issues before they escalate.

Governance, Backup & Recovery

Security isn't just about prevention. It also includes being prepared for recovery. Define configuration standards to prevent drift over time. Establish backup and recovery processes and test them regularly to make sure they work. A well-designed Azure environment is not only secure but also resilient and manageable.

Security needs to be built in before anything moves to Azure. Each phase of migration should be checked against your security baseline, not reviewed after the fact.

Microsoft 365 Security: Protecting Your Most Common Entry Points

Most security incidents don't begin as sophisticated attacks; they often start with something simple. A stolen password. A phishing email that gets clicked. An unmanaged device connecting to company data.

According to Verizon's 2025 Data Breach Investigations Report, credential theft is involved in 33% of SMB breaches, with social engineering responsible for a large share of the rest. Microsoft 365 is where your users spend most of their time, which makes it one of the most important areas to secure.

Identity Is the Control Plane

If an attacker has a valid username and password, they have access to everything that the account can reach.

That's why multi-factor authentication is one of the most effective controls you can put in place. When combined with Conditional Access policies that evaluate device compliance and sign-in risk, you can block the most common entry points attackers rely on.

- Enforce MFA for all users, without exceptions
- Use Conditional Access to restrict access from non-compliant or unmanaged devices
- Separate administrator accounts from standard user accounts
- Limit the number of Global Administrators

Device Security: Intune & Defender for Business

Devices are often the weakest link, especially when they are unmanaged or inconsistently secured.

Microsoft Intune allows you to enforce compliance policies such as minimum operating system versions, disk encryption, and active antivirus protection. Devices that do not meet these requirements can be blocked from accessing company resources.

Microsoft Defender for Business adds another layer of protection, with real-time protection, endpoint detection and response, and automated remediation across Windows, macOS, iOS, and Android. Together, these tools give you visibility and control over every device connecting to your environment.

Email Protection: Your Most Common Entry Point

Email remains one of the most common ways attackers gain access to business systems and data.

Microsoft Defender for Office 365 provides protection through anti-phishing controls, Safe Links for real-time URL scanning, and Safe Attachments that analyze files before they reach users. These controls reduce the likelihood of a successful attack and limit the impact if one gets through.

Collaboration Security: Teams, SharePoint & OneDrive

Security doesn't stop at email. Collaboration tools extend access to files and data across your organization and beyond.

Apply malware scanning to SharePoint and OneDrive. Restrict anonymous sharing and require authentication for external access. The same level of control applied to email should extend to every place your team stores or shares information.

Most Microsoft 365 security tools are included in Business Premium, but they are not fully configured by default. Many businesses are already paying for protection they are not using. Proper configuration is what turns Microsoft 365 into a secure platform.

Protecting Your Data Across the Organization

Data doesn't stay in one place. It gets emailed, shared externally, downloaded, and accessed from multiple devices. If your security only protects the systems where data is stored, it breaks down the moment that data moves. Effective data protection ensures security stays with the content itself.

To see why this matters, consider a simple scenario. An employee downloads a financial report from SharePoint and emails it to a client using a personal device. If that file isn't protected, it can be forwarded, saved, or accessed by anyone who receives it. If the same file is labeled and encrypted, access stays restricted, even after it leaves your environment.

Classify Before You Protect

Microsoft Purview sensitivity labels allow you to classify data into categories such as Public, Internal, and Confidential. Once applied, these labels automatically enforce controls. Confidential files can be encrypted, restricted from forwarding, or blocked from external sharing without relying on users to make the right decision every time.

This removes guesswork. Instead of expecting employees to decide how sensitive a file is in the moment, the system automatically applies the appropriate level of protection.

Data Loss Prevention (DLP)

DLP policies help prevent sensitive information from being shared inappropriately, whether by accident or on purpose.

These policies can detect data such as social insurance numbers, financial information, or health records before it leaves your environment. They apply across email, Teams, SharePoint, and OneDrive, and can be configured to alert users, block actions, or require justification based on the situation.

For example, if a user attempts to send a spreadsheet containing payroll data outside the organization, a DLP policy can stop the action or prompt the user to confirm the intent before proceeding.

External Sharing Controls

Not all external sharing is risky, but uncontrolled sharing is.

Set clear boundaries by limiting sharing to approved domains, requiring authentication for access, and applying expiration dates to shared links. These controls allow your team to collaborate with clients and partners without leaving access open longer than necessary.

Without these controls, shared links can remain active indefinitely, often without anyone realizing who still has access.

Encryption & Access Governance

Encryption should apply at rest, in transit, and when files are shared. Access governance ensures that permissions are regularly reviewed so that only the right people have access.

Permission creep, where users accumulate access they no longer need, is one of the most common and overlooked risks in Microsoft 365 environments. Regular access reviews help prevent this from becoming a long-term exposure.

> Security should follow the data, not just the system it lives in. A file that leaves SharePoint should carry the same protections it had inside it.

How Secure is Your Environment Right Now?

At this point, you might be wondering how your current setup compares.

The reality is, most environments aren't fully locked down. Not because of negligence, but because things change over time. New users, new devices, and new tools can introduce gaps that go unnoticed.

The questions below are a simple way to check where things stand.

Quick Self-Assessment

- Are all users required to use multi-factor authentication?
- Can unmanaged or personal devices access company email and files?
- Do you have visibility into unusual or suspicious login activity?
- Are your devices monitored and required to meet compliance standards?
- Is sensitive data in Microsoft 365 classified and protected?
- Do you have a clear process for responding to a security incident?
- Are your Microsoft 365 security tools fully configured, not just licensed?

If you answered "no" or "not sure" to any of these, there are gaps in your security posture. Most of these issues are not difficult to fix, but they do require deliberate configuration and ongoing attention.

Not Sure Where You Stand? That's a Good Place to Start.

Centriworks has been helping East Tennessee businesses build secure, reliable technology environments since 1964. We are a security-first Managed IT provider, CompTIA Security Trustmark+ certified, with a CISSP on staff. Our team specializes in guiding small and mid-sized businesses through the type of migration and security work outlined in this guide.

If this guide raised questions about your current environment, the next step is understanding where you stand. We offer a no-pressure technology assessment that gives you a clear picture of your environment and what it will take to move forward with confidence.

Three Ways to Get Started

Technology Assessment
A full review of your current IT environment, with a clear and prioritized roadmap for improvement.

Migration Planning Session
A focused discussion around your migration goals, timeline, and what a structured move to Azure would look like for your business.

Microsoft 365 Security Review
A detailed review of your current Microsoft 365 configuration, showing what is protected, what is not, and how to close the gaps.

CENTRIWORKS

About Centriworks

Centriworks works with businesses across East Tennessee at every stage. Some are ready to move. Others are still figuring out what they have. If you're looking for a clearer picture of your environment, we're here to help.

Contact us at:
Phone: (865) 524-1124
Website: centriworks.com

Headquarters:
3505 Sutherland Avenue
Knoxville, Tennessee 37919