BINARY TREE®
Powering Enterprise Transformations®

Keeping financial data secure on the go with Microsoft EMS

> *"With the move towards mobility and use of the cloud for employees, against a backdrop of the rising number of cybersecurity attacks, I firmly believe that Binary Tree services with MSFT EMS is uniquely positioned to be the champion of change for this new work experience and digital transformation."*
>
> *~ Jack Bofinger, CTO at SNB*

People these days work from anywhere and everywhere. Which means IT teams face the challenge of keeping their organization's data secure. No matter where their users roam, what device they use, or what network they log on to.

A goal of letting people work from anywhere

That's why many organizations are moving to Microsoft 365. They want to free their users to be more productive wherever, whenever, and however they want—while still keeping sensitive data secure as if a user were working onsite.

Our experts recently worked with a large financial institution that wanted to adopt Microsoft 365 for exactly these reasons. They wanted to empower their users to stay secure and productive on their favorite apps and devices.

A concern with security in the cloud

But like many organizations, the client was initially cautious about security in the cloud. Given the sensitive nature of their business, they needed to make sure their data stayed protected across mobile devices, which run a higher risk of being lost or stolen.

"Take out your cell, unlock it, and hand it to the first stranger you see," says Jon Monroe, Senior Solutions Architect at Binary Tree. "That's what this client worried it could be like if they moved their data to the Microsoft cloud."

To overcome this concern, they needed to make sure that devices in the cloud followed strict rules to access their systems. Namely, that mobile devices should:

- Be domain joined
- Join on an approved network
- Have multi-factor authentication in place

Implementation

Roll out of Microsoft EMS across their systems and devices.

- Set up data center IP and VPN as trusted networks
- Turn on Azure Multifactor Authentication
- Join or register mobile devices to Azure Active Directory
- Create conditional access policies to restrict access
- Test everything to make sure it was working as expected
- Expand these security policies to other workloads of Microsoft 365

STERLING NATIONAL BANK

Case Study Highlights

Move to: Microsoft Office 365
Location: United States
Industry: Finance

Customer Profile

Sterling National Bank is a regional bank holding company who provides a full range of banking and financial services and has assets totaling $30 billion following a merger and acquisition.

Customer Situation

Sterling wanted to migrate to Microsoft 365 to empower their mobile users to be more productive anytime, anywhere, and on any device. But first, they had to allay some concerns about security in the cloud.

Solutions

- Microsoft Enterprise Mobility + Security

Benefits

- Control identity + access in the cloud
- Get identity-driven security
- Manage mobiles apps + devices
- Protect information

Results

Now, the client is setup to protect their data, manage devices, and make sure only approved users have access. They can also track usage patterns to quickly spot security threats.

All of this has led to their IT team giving the green light to move ahead with the full range of Microsoft 365 workloads. Which means their mobile users can enjoy a higher level of collaboration and productivity through their favorite apps and devices.