



TECH HEADS

THInc. 365™

Managed Security Service for Microsoft 365

KEY INSIGHT:

Working remotely has become the new normal, accelerating the adoption of Cloud Computing and making companies **INCREASINGLY VULNERABLE** to cyberattacks.

EXPERTS AGREE:

Many companies rushed to implement Microsoft 365 for remote workers amid the pandemic, overlooking security best practices. Threat intelligence research has revealed

A MASSIVE INCREASE OF OVER 600% of cyberthreat indicators.

The Department of Homeland Security has advised businesses to prepare for new cybersecurity threats arising from remote working arrangements.

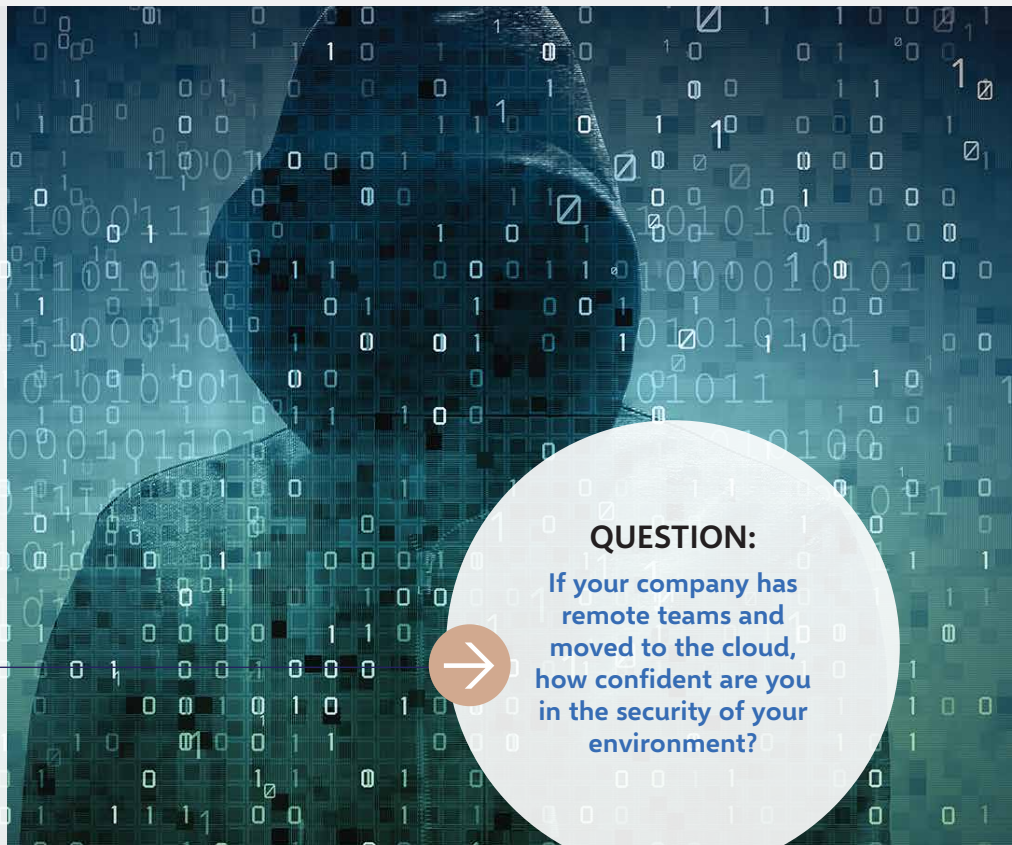
WHAT'S CHANGED?

Lack of security controls on managed endpoints

Increased number of potential devices to target

Increased use of cloud based apps and collaboration tools

Increased phishing and social engineering attacks



QUESTION:

If your company has remote teams and moved to the cloud, how confident are you in the security of your environment?



OUR PROMISE:

WE TAKE ACTION TO SECURE MICROSOFT 365

Tech Heads worked with cybersecurity experts at Microsoft to develop and operationalize a playbook for securing Microsoft 365, including the following core activities:

CONFIGURATION of Microsoft 365 according to best practices, optimized for your environment, including Exchange Online protection, Defender for Microsoft 365, and Multi-factor authentication.

BACKUP of the entire Microsoft 365 environment including emails, contacts, calendars, tasks, plus SharePoint, OneDrive, Groups, and Teams to protect data from accidental deletion, corruption, or from being held hostage by ransomware.

MONITORING is included to identify threats and escalate to a dedicated security operations team for mitigation and remediation.



Monthly Service Model

Rest easy knowing you are continually protected against increased threat activity.

I am very impressed with the playbook Tech Heads has developed around securing Microsoft 365.

I HAVE NOT SEEN ANOTHER PARTNER TAKE SUCH A THOROUGH APPROACH.



MATT SOSEMAN

Cybersecurity Architect
Microsoft

4 AREAS OF PROTECTION:



DATA

As a central hub of operations, Microsoft 365 contains sensitive and valuable data.



IDENTITY

Protect your users against brute force attacks and social engineering.



ENDPOINTS

Ensure every device, even those used by remote employees is securely configured.



EMAIL

Verify mail senders and protect from spam, fraud, and phishing attacks.



MICROSOFT 365 SECURITY DONE RIGHT... FOR YOU.

CALL 503.639.8542

7070 SW FIR LOOP
PORTLAND OR 97223