

MICROSOFT 365 EXECUTIVE SECURITY SCORECARD

ASSESS YOUR ORGANIZATION'S SECURITY MATURITY

A practical self-assessment for business leaders to evaluate security posture, reduce risk, and protect what matters most.



EVALUATE

Assess your organization's security practices across key Microsoft 365 security domains.



UNDERSTAND

Identify strengths, uncover gaps, and understand your security maturity.



PRIORITIZE

Focus on the areas that matter most to reduce risk and improve business resilience.



TAKE ACTION

Use your results to guide strategy and drive smarter technology decisions.



LOCAL EXPERTISE.
BUSINESS FOCUSED.
RESULTS DRIVEN.

Protect your people. Secure your data.
Strengthen your business.



WHY SECURITY MATURITY MATTERS

Security Is No Longer an IT Issue. It's a Business Imperative.

Cyber threats are escalating, business data is more dispersed than ever, and attackers are targeting organizations of all sizes. Microsoft 365 provides powerful security capabilities—yet most organizations are only using a fraction of what's available.



A strong security posture protects your people, your customers, your data, and your reputation—so your business can grow with confidence.

THE REALITY OF TODAY'S THREAT LANDSCAPE



90%

of cyberattacks begin with a phishing email.

Microsoft Digital Defense Report 2023



60%

of small and mid-sized businesses that suffer a cyberattack go out of business within 6 months.

National Cyber Security Alliance



85%

of organizations have experienced a Microsoft 365 data loss event.

Veeam Data Protection Trends Report 2023



Take Control of Your Security Future

This scorecard helps you evaluate your organization's security maturity across key Microsoft 365 domains—so you can identify gaps, prioritize improvements, and make smarter technology decisions.

Security maturity isn't just protection. It's a competitive advantage.



EXECUTIVE TAKEAWAY

Security maturity is about more than technology—it's about building resilience, reducing risk, and enabling your business to operate securely in a digital world.

Strong Security Drives:



Business Continuity

Minimize downtime and keep operations running.



Regulatory Compliance

Meet industry standards and avoid costly penalties.



Customer Trust

Protect sensitive data and strengthen confidence.



Operational Efficiency

Reduce incidents, streamline processes, and lower costs.



LOCAL EXPERTISE.
BUSINESS FOCUSED.
RESULTS DRIVEN.

We help Orange County businesses leverage technology to **work smarter, stay secure,** and **achieve their goals.**



HOW SCORING WORKS

A SIMPLE FRAMEWORK. VALUABLE INSIGHTS.

This scorecard helps you evaluate your organization's security maturity across four critical Microsoft 365 security domains. Answer each question honestly based on your current environment.



INSTRUCTIONS

- ✓ Review each question and choose the answer that best reflects your organization.
- ✓ Assign the corresponding points.
- ✓ Add your points for each domain to calculate your total score.
- ✓ Use the Results Guide on page 8 to interpret your score and plan next steps.

SCORING MODEL

ANSWER	POINTS
 YES Fully implemented and effective	5 POINTS
 PARTIALLY In progress or partially effective	3 POINTS
 NO Not implemented or not effective	0 POINTS

MATURITY LEVELS AT A GLANCE



HIGH RISK

0 – 40 POINTS

Critical gaps exist. You are vulnerable to significant risk and disruption.



ELEVATED RISK

41 – 70 POINTS

Several gaps increase your risk. Improvement is needed.



MODERATE RISK

71 – 90 POINTS

Good progress, but important opportunities remain.



WELL PROTECTED

91 – 125 POINTS

Strong security posture with mature controls and processes.

ASSESSMENT DOMAINS

Your score is calculated across four key Microsoft 365 security domains that protect your business from today's most common threats and support operational resilience.



1. IDENTITY SECURITY

Protects user identities and access to your Microsoft 365 environment.



2. EMAIL & COLLABORATION SECURITY

Safeguards communication channels from threats and misuse.



3. DATA PROTECTION & DEVICE SECURITY

Secures your data and devices wherever work happens.



4. BACKUP & RECOVERY READINESS

Ensures you can recover quickly from data loss or disruption.

“ Security is not a product. It's a process, a priority, and a commitment. ”



Use this scorecard to benchmark your maturity, identify opportunities, and build a stronger security foundation.



1. IDENTITY SECURITY

Protecting the right people with the right access.

Strong identity security is the foundation of your Microsoft 365 security posture. It ensures that the right users have the right access—no more, no less.

ASSESSMENT QUESTIONS	YES 5 POINTS	PARTIALLY 3 POINTS	NO 0 POINTS
 1. MULTI-FACTOR AUTHENTICATION (MFA) Is MFA enabled for all users, especially administrators and remote users?			
 2. PRIVILEGED ACCESS CONTROLS Are admin accounts limited, protected by MFA, and used only when necessary (just-in-time)?			
 3. ACCESS REVIEWS Are user access and permissions reviewed regularly and promptly updated?			
 4. CONDITIONAL ACCESS POLICIES Are conditional access policies in place to restrict access based on risk, device, and location?			
 5. IDENTITY MONITORING & ALERTS Are suspicious sign-in activities monitored with alerts and automated response where possible?			

YOUR SCORE



WHAT THIS MEANS

Identity is the #1 target for attackers. Strong controls here reduce the risk of unauthorized access, data breaches, and costly business disruption.

TIP



Use Microsoft Entra ID (formerly Azure AD) security features to enforce least privilege access and reduce identity risk.



STRENGTH IN ACTION

Organizations with strong identity controls are up to 80% less likely to experience a breach.

KEY CAPABILITIES TO CONSIDER

- Microsoft Entra ID Premium P1/P2
- Multi-Factor Authentication
- Privileged Identity Management (PIM)
- Conditional Access Policies
- Identity Protection & Risk-Based Sign-In



BUILD A STRONGER FOUNDATION.

Secure identities. Reduce risk. Protect your business.



TECHNOLOGY STRATEGY REVIEW

Let's evaluate your results and build a plan that strengthens your security posture.



2. EMAIL & COLLABORATION SECURITY

Secure communication. Stop threats before they reach your people.

Email remains the #1 attack vector for most businesses. Strong email and collaboration security helps block phishing, malware, and business email compromise.

ASSESSMENT QUESTIONS	YES 5 POINTS	PARTIALLY 3 POINTS	NO 0 POINTS
 1. MICROSOFT DEFENDER FOR OFFICE 365 Is Defender for Office 365 enabled to protect against phishing, malware, and suspicious links/attachments?	☐	☐	☐
 2. ANTI-PHISHING POLICIES Are anti-phishing policies configured to detect and block advanced phishing attacks and spoofing?	☐	☐	☐
 3. SAFE LINKS & SAFE ATTACHMENTS Are Safe Links and Safe Attachments enabled to scan URLs and files in real time?	☐	☐	☐
 4. USER AWARENESS TRAINING Do employees receive regular security awareness training focused on phishing and social engineering?	☐	☐	☐
 5. COLLABORATION SECURITY CONTROLS Are external sharing, guest access, and sensitive link settings reviewed and restricted as needed?	☐	☐	☐

YOUR SCORE

/25

POINTS



WHAT THIS MEANS

Strong email and collaboration security reduces the risk of successful phishing attacks, protects sensitive information, and keeps business communication safe.

TIP



Review and test your phishing simulations. The more prepared your people are, the stronger your defense.



THE BUSINESS IMPACT

Organizations with mature email security controls experience up to 70% fewer successful phishing attacks.

Source: Microsoft Digital Defense Report 2023

KEY CAPABILITIES TO CONSIDER

- Microsoft Defender for Office 365
- Anti-Phishing & Anti-Spoofing Policies
- Safe Links & Safe Attachments
- Security Awareness Training
- External Sharing & Guest Access Controls





SECURE EVERY CONVERSATION.
Attackers are getting smarter. Your email and collaboration security should be too.



TECHNOLOGY STRATEGY REVIEW
Let's review your email and collaboration security posture and create a plan to strengthen it.



Schedule your **Technology Strategy Review** today.



3. DATA PROTECTION & DEVICE SECURITY

Protect what matters most. Secure your data and the devices your business depends on.

Your data is one of your most valuable assets. Strong protection and secure devices reduce risk, support compliance, and keep your business running.

ASSESSMENT QUESTIONS	YES 5 POINTS	PARTIALLY 3 POINTS	NO 0 POINTS
 1. DATA LOSS PREVENTION (DLP) Are DLP policies in place to help identify, monitor, and protect sensitive data across email, files, and endpoints?			
 2. INFORMATION PROTECTION Are sensitivity labels and encryption used to classify and protect important business information?			
 3. DEVICE MANAGEMENT Are devices managed through Microsoft Intune with security policies and compliance enforcement?			
 4. ENDPOINT PROTECTION Is Microsoft Defender for Endpoint enabled to prevent, detect, and respond to threats on devices?			
 5. DATA RETENTION & GOVERNANCE Are retention policies and legal holds configured to meet compliance and governance requirements?			

YOUR SCORE



WHAT THIS MEANS

Effective data and device security protects sensitive information, prevents data loss, and ensures your team can work securely from anywhere.

TIP



Classify your data.
Encrypt what matters.
Control access.
Secure devices.
Reduce your risk.



DATA IS YOUR BUSINESS

Organizations with strong data protection practices are **3x more likely** to maintain customer trust after a breach.

Source: IBM Cost of a Data Breach Report 2023

KEY CAPABILITIES TO CONSIDER

- ✔ Data Loss Prevention (DLP)
- ✔ Microsoft Purview Information Protection
- ✔ Microsoft Intune Device Management
- ✔ Microsoft Defender for Endpoint
- ✔ Retention Policies & Legal Holds



PROTECT SENSITIVE DATA.

Know where your data lives, classify it, and protect it with the right controls.



SECURE EVERY DEVICE.

Enforce policies, keep devices compliant, and reduce your attack surface.



STAY COMPLIANT.

Meet regulatory requirements and be prepared for audits and investigations.



4. BACKUP & RECOVERY READINESS

Be prepared. Recover with confidence.
Minimize downtime and data loss.

Ransomware, accidental deletion, and outages happen. A strong backup and recovery strategy ensures your business can recover quickly and keep moving forward.

ASSESSMENT QUESTIONS	YES 5 POINTS	PARTIALLY 3 POINTS	NO 0 POINTS
 1. BACKUP COVERAGE Is Microsoft 365 data (Exchange, OneDrive, SharePoint, Teams) backed up beyond the native 30-day recycle bin?			
 2. RECOVERY TIME OBJECTIVES (RTO) Are documented RTOs defined for critical systems and data to minimize business disruption?			
 3. RECOVERY POINT OBJECTIVES (RPO) Are RPOs defined to limit the amount of data loss your organization can tolerate?			
 4. REGULAR TESTING Are backups and recovery processes tested regularly to ensure they work when needed?			
 5. BUSINESS CONTINUITY PLAN Do you have a documented business continuity plan that includes data recovery and communication procedures?			

YOUR SCORE



WHAT THIS MEANS

A strong backup and recovery strategy is your safety net. It reduces downtime, protects your data, and ensures your business can recover and continue to serve your clients.

TIP



Don't rely on the default recycle bin. Implement a solution that provides long-term backup, granular recovery, and testing.



RECOVERY IS RESILIENCE

Organizations with tested backup and recovery plans experience **4x less** downtime and recover **2x faster**.

Source: IBM Cost of a Data Breach Report 2023

KEY CAPABILITIES TO CONSIDER

- Third-Party Backup for Microsoft 365
- Defined RTOs & RPOs
- Automated Backup Verification
- Regular Recovery Testing
- Business Continuity Planning



PROTECT WHAT MATTERS.

Back up your critical Microsoft 365 data and ensure it can be recovered when you need it most.



PREPARE FOR THE UNEXPECTED.

Outages, ransomware, and human error can happen. Recovery readiness keeps your business running.



TEST. VERIFY. RECOVER.

Regular testing gives you confidence that your backups and recovery plans will work when it counts.



YOUR RESULTS & NEXT STEPS

Know your score. Understand your risk.
Strengthen your security.

Add up your points from each of the four domains for your total score out of 100 points. Use the guide below to understand your results and identify your priority focus areas.

TOTAL SCORE SUMMARY



0 – 40 POINTS HIGH RISK

Critical gaps exist. You are vulnerable to significant risk and disruption. Immediate action is required.



41 – 70 POINTS ELEVATED RISK

Several gaps increase your risk. Improvement is needed to reduce exposure and strengthen security.



71 – 90 POINTS MODERATE RISK

Good progress, but important opportunities remain to reduce risk and improve resilience.



91 – 100 POINTS WELL PROTECTED

Strong security posture with mature controls and processes. Keep monitoring and improving.

YOUR DOMAIN SCORES



1. IDENTITY SECURITY

Protecting the right people with the right access.

/25
POINTS



2. EMAIL & COLLABORATION SECURITY

Secure communication and stop threats before they reach your people.

/25
POINTS



3. DATA PROTECTION & DEVICE SECURITY

Protect what matters most and secure the devices your business depends on.

/25
POINTS



4. BACKUP & RECOVERY READINESS

Be prepared. Recover with confidence and minimize downtime and data loss.

/25
POINTS

TOTAL SCORE

/100



There is no such thing as a perfect score.
Security is a journey, not a destination.

TURN INSIGHT INTO ACTION

A strong security posture is key to protecting your business, your people, and your future. Let's build a plan that closes gaps and strengthens your Microsoft 365 security foundation.



PRIORITIZE WHAT MATTERS

Focus on your highest risk areas for the greatest impact.



BUILD A PLAN

Create a roadmap with clear steps, ownership, and timelines.



STRENGTHEN YOUR DEFENSES

Implement the right controls, policies, and training.



REVIEW & IMPROVE

Continuously measure, monitor, and improve your security posture.

SCHEDULE YOUR TECHNOLOGY STRATEGY REVIEW

A no-obligation session with our Microsoft 365 experts.

- Review your score and results
- Identify your biggest risks
- Get expert recommendations
- Build your security roadmap



SCHEDULE TODAY!



STRONGER TOGETHER.
We're here to help you protect what matters most.

IThinkSource is your trusted Orange County partner for Microsoft 365 security, strategy, and support.



Microsoft
Solutions Partner



WHY ORANGE COUNTY BUSINESSES CHOOSE ITHINKSOURCE

Local Expertise. Business-Focused. Results-Driven.

For more than 24 years, IThinkSource has helped Orange County organizations leverage technology to work smarter, reduce risk, and achieve their business goals. As a trusted Microsoft Solutions Partner, we deliver secure, reliable, and scalable solutions tailored to your unique needs.



Modern Work
Security
Infrastructure
Azure

OUR CORE CAPABILITIES



SECURITY & COMPLIANCE

Protect your business with proactive security, modern identity management, and compliance expertise.



MANAGED IT SERVICES

Reliable, responsive IT support that keeps your systems running smoothly and your team productive.



MICROSOFT 365 CONSULTING

Expert guidance and implementation for Microsoft 365 to maximize adoption, security, and ROI.



CLOUD & INFRASTRUCTURE

Design, migrate, and manage secure cloud environments that scale with your business.



BUSINESS CONTINUITY & BACKUP

Minimize downtime and protect critical data with proven backup and disaster recovery strategies.



vCIO & STRATEGIC TECHNOLOGY PLANNING

Align technology investments with your business goals and build a roadmap for future success.

PROVEN. TRUSTED. LOCAL.

We're proud to help organizations across Orange County strengthen security, improve efficiency, and drive growth with confidence.



95%+ CLIENT RETENTION

Long-term partnerships built on trust, results, and exceptional service.



THOUSANDS OF ENDPOINTS PROTECTED

Securing businesses across Orange County with proactive, layered defense.



ORANGE COUNTY BASED SUPPORT TEAM

Local experts who understand your business and are here when you need us.



MICROSOFT CERTIFIED EXPERTS

Highly trained professionals delivering enterprise-grade solutions and support.



Your business deserves a technology partner that puts security and success first.

We don't just implement technology—we become an extension of your team, focused on what matters most: protecting your business and helping it thrive.

Let's build a stronger, more secure future—together.

Contact us to learn how IThinkSource can help your organization maximize Microsoft 365 security and performance.

LET'S SECURE WHAT'S NEXT.

A Technology Strategy Review designed to help Orange County business leaders identify risks, align technology with business goals, and build a practical roadmap for the future.



WHAT YOU'LL GAIN

- ✓ Review your Microsoft 365 security posture
- ✓ Identify security, compliance, and operational risks
- ✓ Evaluate backup and recovery readiness
- ✓ Review identity and access controls
- ✓ Understand gaps and improvement opportunities
- ✓ Develop a technology roadmap aligned with business objectives



WHO IT'S FOR

- CEOs
- Presidents
- COOs
- CFOs
- IT Directors
- Operations Leaders



WHY ITHINKSOURCE

- Orange County-based technology advisors
- Microsoft Solutions Partner
- 24+ years serving local businesses
- Security-first approach
- Strategic, business-focused guidance



- ✓ Modern Work
- ✓ Security
- ✓ Infrastructure
- ✓ Azure

READY TO STRENGTHEN
YOUR SECURITY POSTURE?

**SCHEDULE YOUR
TECHNOLOGY
STRATEGY REVIEW**

 (949) 679-5140

 ithinksource.com

 Irvine, California



SCHEDULE TODAY



IThinkSource has been an invaluable partner in helping us strengthen our security, improve reliability, and plan for the future. They understand our business and deliver results we can count on.



LOCAL EXPERTISE.
BUSINESS FOCUSED.
RESULTS DRIVEN.