Litzia
Clarifying Today's Technology

TECHNOLOGY INSIGHTS

WINTER 2022

Microsoft 365 License Subscriptions Pricing & Terms Change in 2022

Effective March - June 2022, Microsoft enforces its *New Commerce Experience*, a sweeping change to cloud subscription licensing. This change impacts all customers.

In brief, certain Microsoft 365 plans will increase in price and **all plans will incur a 20% premium charge for the privilege of maintaining the current month-to-month agreement terms allowing on-demand change of license counts with no cancellation penalties.**

To avoid the 20% premium, customers must commit to a 1 or 3-year Microsoft Agreement Term for each license subscription. The caveat: no license count reductions, cancellations or refunds are allowed during the term. This change impacts all Microsoft Partners, our customers, and how we must transact business for your Microsoft Cloud services.

Litzia will be reaching out to our Microsoft 365 customers to transition your subscriptions to the New Commerce Experience licensing model that best meets your needs. To get a jump start for budgeting purposes, email *consulting@litzia.com*. Read our ***Important Microsoft Licensing & Security Changes*** brief for more details.

Litzia

LinkedIn
facebook

314 E. Holly St, Ste 205
Bellingham, WA 98225

☎ (360) 714-0565
✉ consulting@litzia.com
www.litzia.com

Implementing a Zero-Trust Security Posture

Executing the basics for your critical "new normal."

As an owner, CIO, or IT Director, you're sick of hearing about it — a **100% year-over-year increase in ransomware and data breaches** impacting private and public sectors. Your first response may be "My company has cyber-liability insurance." Insurance will help pay attorney fees, credit monitoring and damages to employees, customers and vendors, but it won't recover your data, repair your reputation, or replace lost revenue. **60% of small business fold after a major cyberattack, regardless of insurance.**

You know prevention is necessary, but execution is difficult. You're not alone. **Many small and mid-sized organizations lack the most basic zero-trust protections.** Zero-trust is a proactive approach to security that uses continuous verification and adaptive controls to protect against threats in real-time. Let's discuss basic principles.

Verify Explicitly

Authenticate and authorize access based on all data available: User, Device, Location, Service, Data, & Network. Multi-factor Authentication (MFA) prevents 99% of account compromises by forcing a user to complete 2 or more identity-verification steps to access any given system, typically your password and:

- Something you ***have*** (a code, a key)
- Something you ***know*** (a PIN, answer to a security question)
- Something you ***are*** (biometric ID: fingerprint, voice, or retina scan)

If you fear inconveniencing staff, augment the protection MFA offers with the ease of a Single-Sign-On (SSO) solution to continue granting access to users throughout their workday after their first MFA sign-on.

Use Least-Privilege Access

This practice assigns the lowest-level of access necessary to perform the duties of the job for any given role or user. Least-privileged access prevents intruders from gaining the level of access necessary to deploy ransomware across the entire network, sabotage backups, erase activity logs, create bogus accounts and turn off anti-virus protection. Must-do-now permissions & account revisions include:

- Ensure **Admin** roles are securely restricted to a single user/account.
- Setup a separate **Backup Admin** account to secure your backup & disaster recovery system access.
- Create and assign **Conditional Access Policies** to all privileged admin accounts.

. . . Continued Page 2

Choosing a Microsoft Partner: Why Go for the Gold

We know you have a choice regarding your business technology services. Every technology firm touts certifications, but let's be honest — most have no serious requirements behind them. Not true for Microsoft Gold Partners like Litzia.

We are among the top 1% of Microsoft Partners worldwide, passing rigorous training and certification standards for specific competencies. We invest time and money in our people, training and tools year after year to educate and certify in a rapidly-changing industry. Gold also provides us direct and advanced access to Microsoft with guaranteed response times. It's a good thing. We hope you agree!

Gold
Microsoft Partner
Microsoft

. . . Continued from Page 1

Realign your **Active Directory Groups** to job roles; restrict employee permissions only to files and apps they truly need.

Revoke **Local Admin** rights on employer-owned PCs.

Always Assume Intrusion

Constantly monitor your environment, prevent threats in real-time and have a response plan.

Establish written security policies and educate employees.

Implement Microsoft InTune and mobile device management tools for policy controls including encryption, remote wipe, and to block network access when unauthorized apps are installed on endpoints.

Invest in **Advanced Endpoint Security** with rollback capabilities and **Security Operations Center (SOC)** back-end service to detect, alert, kill, and restore in real-time.

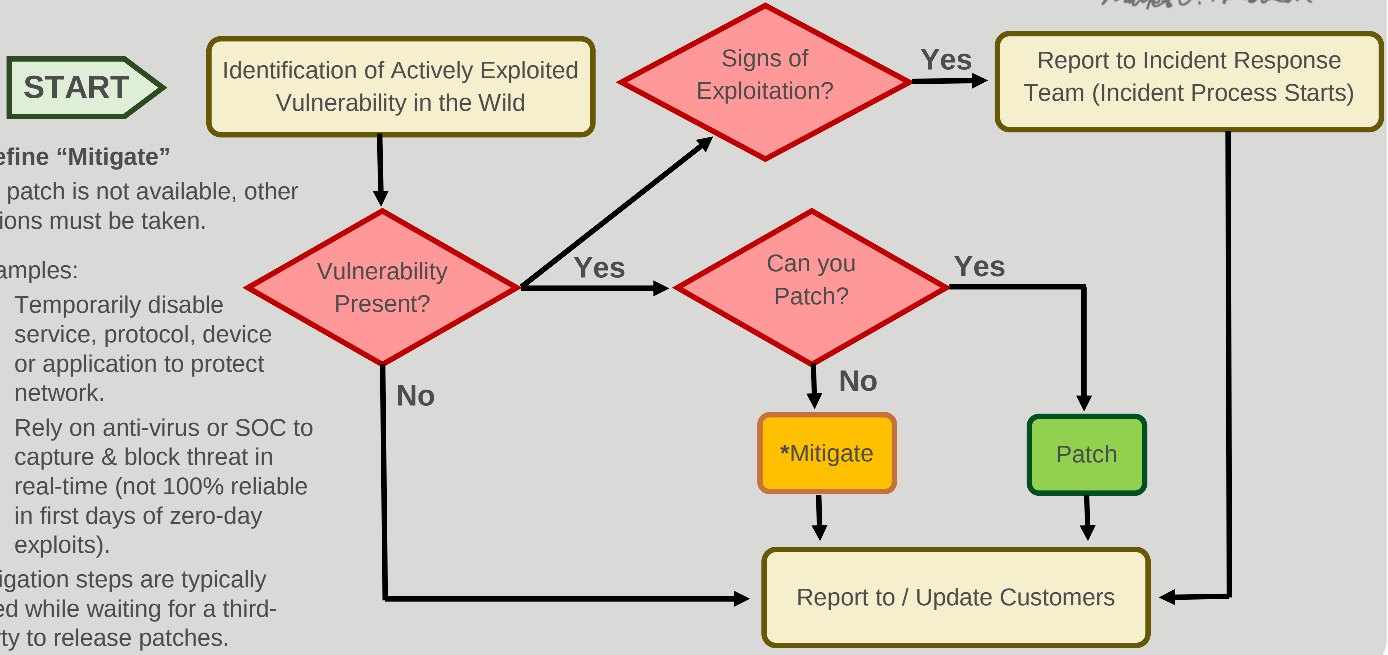
Use a secure, business-class password vault, such as LastPass for Business.

Litzia has the expertise to help you build your Zero-Trust defense. Call 360-714-0565 or email consulting@litzia.com.

Understanding Litzia's Vulnerability Response Process

As a Litzia customer, you receive occasional "Important" alerts from us regarding "zero-day" threats that may impact your business. It's critical to read these messages and response to any questions or authorization requests so Litzia can help your company mitigate risk, install patches, and evaluate recommendations for additional threat protection.

You may wonder why, how and when Litzia decides to send alerts to our customers regarding security threats. We want to share our ***Vulnerability Response Workflow*** to same-page our process. Maybe you'll see value in developing something similar for your internal use. We can help! Call me or the tech team 360-714-0565. Thanks, Matthew O. Henderson


START
Identification of Actively Exploited Vulnerability in the Wild
Vulnerability Present?
Yes
No
Signs of Exploitation?
Yes
Report to Incident Response Team (Incident Process Starts)
Can you Patch?
Yes
No
*Mitigate
Patch
Report to / Update Customers

***Define "Mitigate"**

If a patch is not available, other actions must be taken.

Examples:

- Temporarily disable service, protocol, device or application to protect network.
- Rely on anti-virus or SOC to capture & block threat in real-time (not 100% reliable in first days of zero-day exploits).

Mitigation steps are typically used while waiting for a third-party to release patches.