# Practical Guide to Microsoft and Google Product Security

# Introduction to Authentication and Account Security

# Understanding the Basics of Authentication

- **Authentication:** The process of verifying the identity of a person or device. It is a critical component of security frameworks, ensuring that access to resources is granted only to those with verified identity.

- **Why It's Foundational:** Authentication acts as the first line of defense against unauthorized access, serving to protect user identities and secure sensitive data from potential breaches.


LSU

# Enhancing Security Through Two-Factor Authentication

- **Introduction to 2FA:** A security process that requires two different forms of identification to access an account. It adds an extra layer of security by combining something you know (like a password) with something you have (like a phone to receive a code).

- **Examples of 2FA methods:**
  - **SMS Codes:** Sent to your mobile device, often seen as accessible but vulnerable to interception.
  - **Authentication Apps:** Such as Google Authenticator or Microsoft Authenticator, which generate time-sensitive codes.
  - **Hardware Tokens:** Physical devices that generate a security code, offering a high level of security.

- **Steps to enable 2FA on Microsoft and Google accounts:**
  - **For Microsoft:** Go to your account settings, select 'Security' and then 'More security options', and follow the prompts to set up two-step verification.
  - **For Google:** Visit your Google Account settings, navigate to 'Security', find 'Signing in to Google', and click on '2-Step Verification' to start the setup.

LSU

# Building Stronger Defenses with Effective Passwords

- **Attributes of Strong Passwords:** Emphasizes the necessity for passwords to be long (at least 12 characters), complex, and unique.

- **Tools for managing passwords, such as password managers:**
  - **Password Managers:** Tools that generate, retrieve, and store complex passwords securely. Examples include LastPass, 1Password, and Dashlane.

- **Microsoft and Google's built-in features for password security checks:**
  - **Microsoft:** Account security page provides password health and security tips.
  - **Google:** Security Checkup feature assesses your passwords' strength and security across your Google Account.

LSU

# Account Recovery Options

- **Importance of Recovery Options:** These options are essential for regaining access to your account if you forget your password or if your account is compromised. They also serve as an additional layer of verification to confirm your identity.

- **How to securely configure recovery options in Microsoft and Google accounts:**
  - **Microsoft:** Access your account settings, navigate to the security tab, and add or update your recovery email and phone number.
  - **Google:** In your Google Account settings, go to the "Security" section and choose to add or update recovery options.

LSU

# Evaluating Security Questions in Digital Security

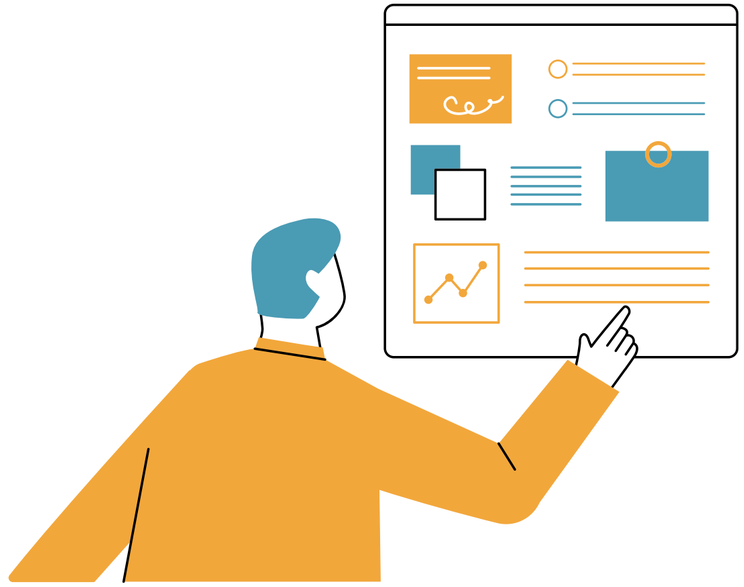
- **Best practices for choosing and answering security questions:**
  - **Choosing Questions:** Opt for questions with answers that are not publicly accessible or easily guessed.
  - **Answering Tips:** Consider using fictional answers that are memorable to you but unpredictable to others, and treat them like additional passwords.

- **Alternatives to security questions for enhancing account security:**
  - **Using MFA:** Multi-Factor Authentication provides a more secure alternative by requiring additional verification methods.
  - **Authentication Apps:** Use apps like Google Authenticator or Microsoft Authenticator, which offer secure token-based authentication.

# Manage Access Controls and User Permissions

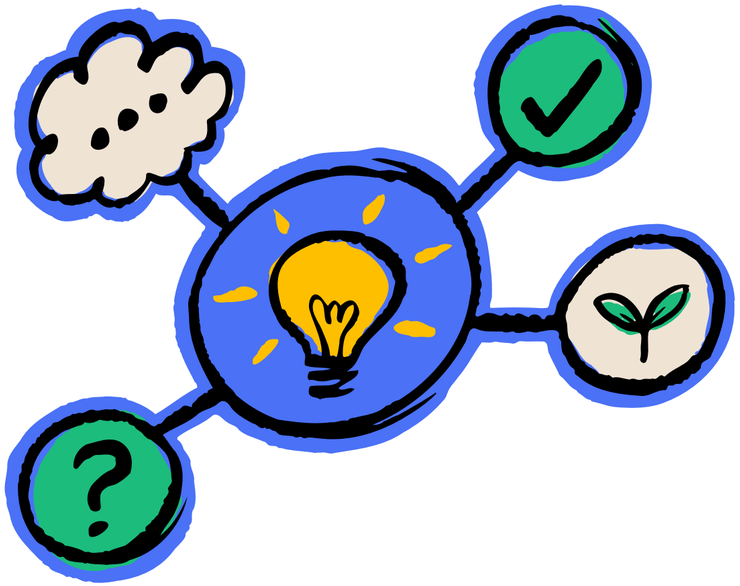
# Understanding Least Privilege

- Minimizes damage from compromised accounts.
- Reduces human error in granting excessive permissions.
- Simplifies access control management.



# The Power of RBAC

- Predefined roles with specific permissions.
- Streamlines access control for an organizations.
- Simplifies user provisioning and de-provisioning.



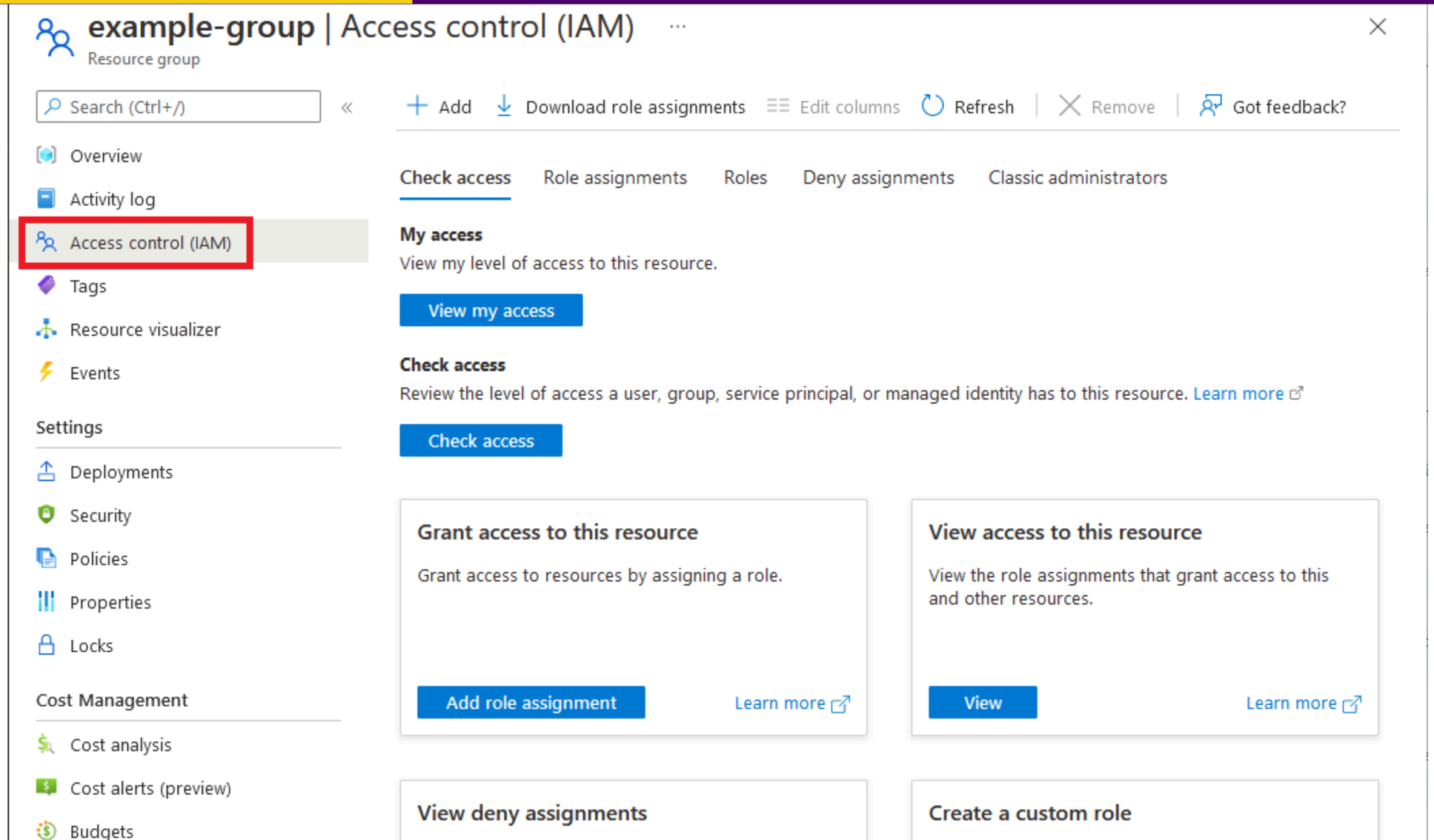
LSU

# Managing User Permissions in Microsoft

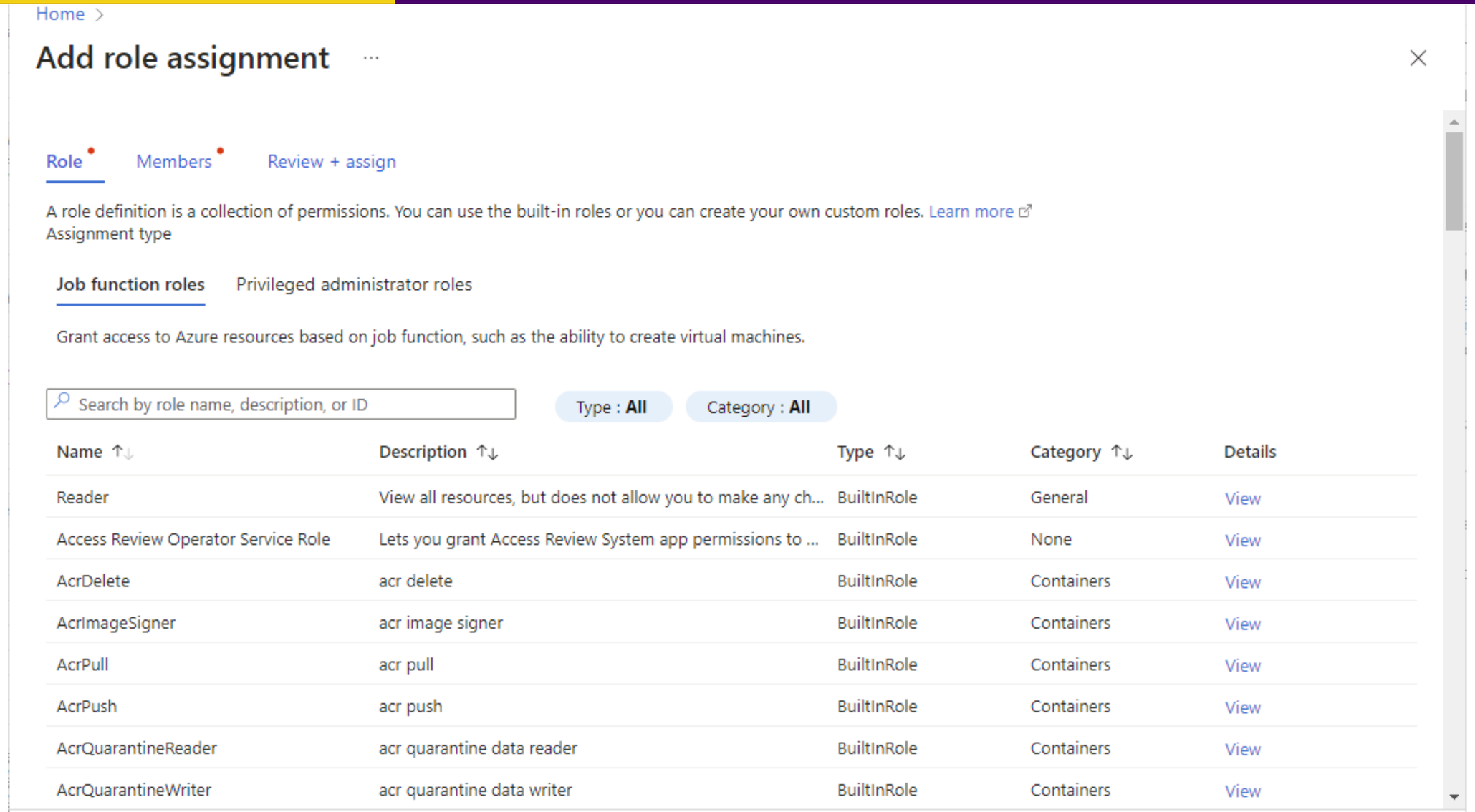
- **Active Directory:** Centralized directory service for managing user accounts, groups, and permissions in Windows environments.
- **User Accounts:** Create user accounts with unique usernames and strong passwords.
- **Security Groups:** Group users with similar access needs for efficient permission assignment.
- **Group Policy Objects (GPOs):** Define access permissions for resources (files, folders, applications) at the domain, site, or organizational unit (OU) level.

LSU

# Managing User Permissions in Microsoft



# Managing User Permissions in Microsoft

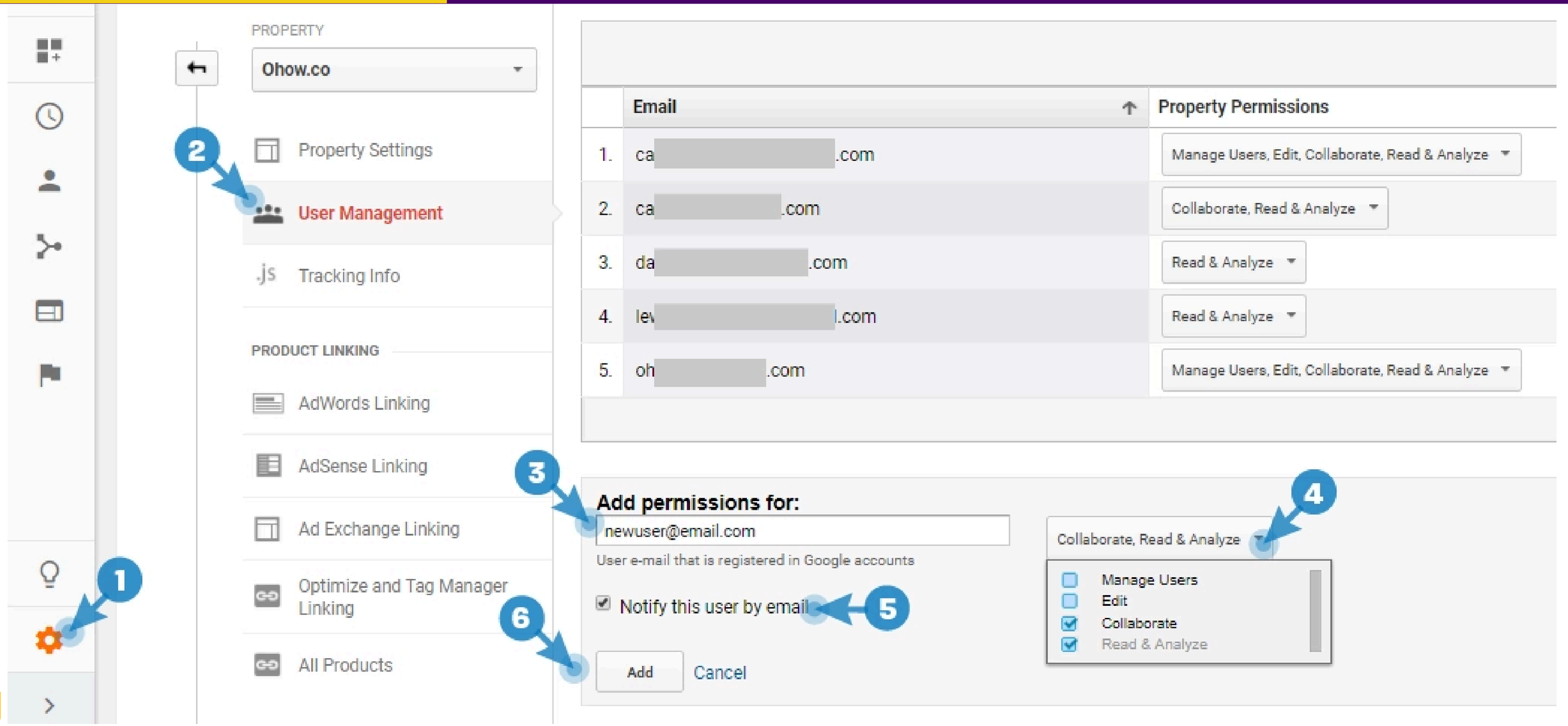


# Managing User Permissions in Google

- **Google Admin Console:** Centralized platform for managing user accounts, groups, and access settings in Google Workspace.
- **User Accounts:** Create user accounts with unique usernames and enforce strong password policies.
- **Google Groups:** Group users with similar access needs for efficient permission sharing within Google products (Gmail, Drive, Docs, etc.).
- **Admin Roles:** Predefined roles with varying permission levels for Google Workspace administration tasks.

LSU

# Managing User Permissions in Google



# Security Configurations and Privacy Settings

# Key Security Settings In Microsoft

- **Azure Active Directory (AAD) Identity Protection:** Detects potential vulnerabilities affecting an organization's identity.
- **Conditional Access Policies:** Enforce specific access controls based on conditions such as user identity, location, device health, and sensitivity of data.
- **Multi-Factor Authentication (MFA)**
- **Data Loss Prevention (DLP):** Identifies, monitors, and protects sensitive information to prevent accidental or intentional exposure.
- **Microsoft Defender Antivirus:** Provides real-time protection against software threats like viruses, malware, and spyware.

LSU

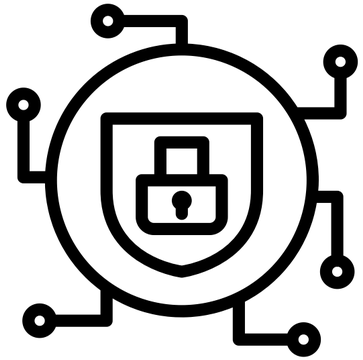
# Security settings to protect data in Microsoft

**Enable Multi-Factor Authentication (MFA)**:

- Go to the Azure Active Directory admin center.
- Navigate to "Users" > "Active users" > "Multi-Factor Authentication".
- Enable MFA for all users to add an extra layer of security to their accounts.

**Implement Data Loss Prevention (DLP)**:

- Data loss prevention > Overview > Data loss prevention settings > Endpoint settings.



LSU

# Key Security Settings In Google

- **Two-Factor Authentication (2FA)**
- **Google Advanced Protection Program:** Provides enhanced security features for Google accounts, such as stronger authentication and protection against phishing.
- **Google Security Checkup:** Allows users to review and adjust their security settings, including account recovery options and connected devices.
- **Encryption:** Encrypts data both in transit and at rest to protect it from unauthorized access.
- **Google Play Protect:** Scans Android apps for malware and other security threats before they are installed on devices.

LSU

# Security settings to protect data in Google

**Enable Two-Factor Authentication (2FA)**:

- Go to the Google Admin console.
- Navigate to "Security" > "Basic settings" > "2-step verification".
- Enable 2FA for all users to enhance account security.

**Configure Data Loss Prevention (DLP)**:

- In the Google Admin console, navigate to "Security" > "Data protection" > "Data Loss Prevention".
- Set up DLP rules to prevent the sharing of sensitive data via email or other Google Workspace applications.

**Enable Advanced Protection Program (APP)**:

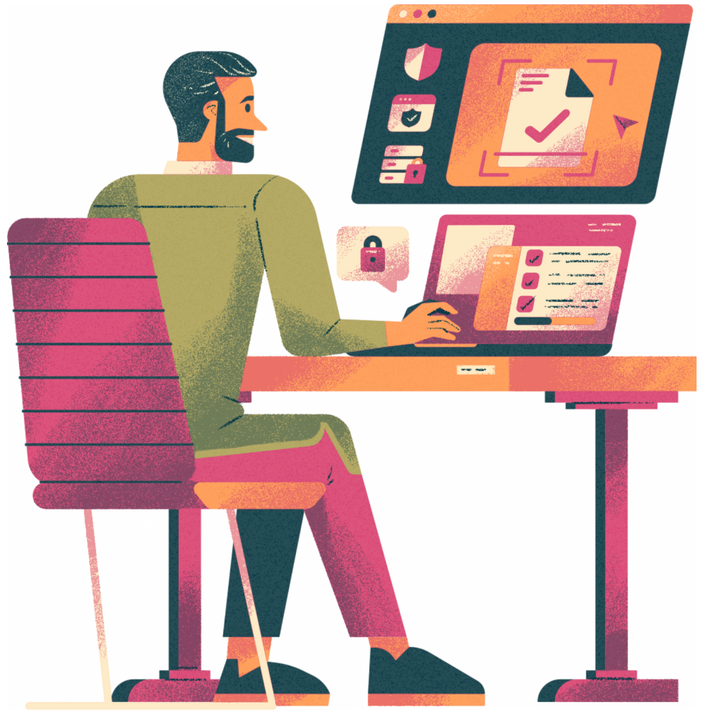
- Encourage users to enroll in Google's Advanced Protection Program for enhanced account security.

LSU

# The importance of endpoint security

Why is endpoint security so important? Endpoint security protects data from attackers and can help mitigate risk.

- Data Protection
- Prevention of Data Breaches
- Protection Against Phishing Attacks
- Compliance Requirements
- Secure Remote Work
- Protection of Intellectual Property
- Maintaining Business Continuity



LSU

# Updates, Patches, and Staying Informed on Security Features

# Intro to Patch Managment

- Today, we'll delve into the critical aspect of maintaining the security of your business through regular updates, patches, and staying informed about the latest security features.

- As small businesses in Baton Rouge, it's vital to understand the proactive measures needed to protect your valuable assets from cyber threats.

- Let's explore how keeping your Microsoft and Google products up to date with the latest security patches and features can significantly enhance your business's security posture and resilience against evolving cyber risks.

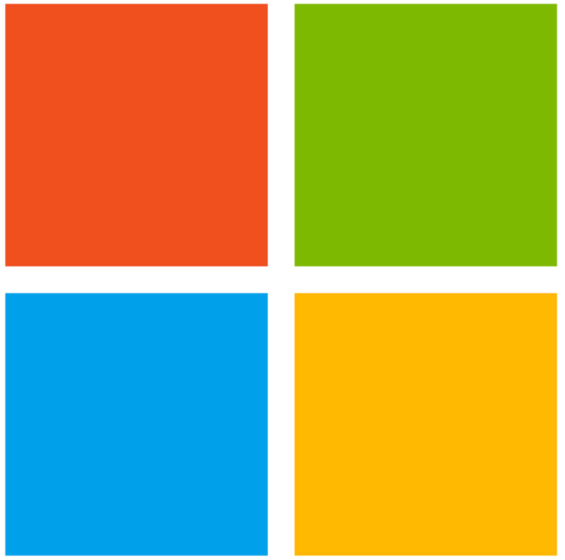
LSU

# Importance of  Microsoft Updates

- **Microsoft Updates:**

- Automatic Updates: Microsoft provides automatic updates through Windows Update, ensuring that your Windows operating system and other Microsoft software receive the latest security patches and features seamlessly.

- Patch Management: Implement a robust patch management strategy to regularly check for and apply updates across all devices and software, including servers, workstations, and applications.



LSU

# Importance of Google Updates

- **Google Updates:**

- Chrome Browser: Google Chrome browser receives automatic updates to ensure that you have the latest security features and protections against online threats.

- Android Devices: Android devices are regularly updated with security patches and system updates to address vulnerabilities and enhance device security.

LSU

# Risks of Not Updating

- **VULNERABILITY:** Outdated software often contains known security vulnerabilities that cyber attackers exploit to gain unauthorized access to systems and steal sensitive data.

- Hackers continuously target outdated software, exploiting vulnerabilities to launch various cyber attacks, including malware infections, phishing scams, and ransomware.

LSU

# Risks of Not Updating

- **DATA BREACHES:** Outdated systems are more susceptible to data breaches, putting your business's confidential information, customer data, and financial records at risk.
- A single data breach can have severe consequences, including financial losses, legal liabilities, and damage to your brand reputation and customer trust.
- **COMPLIANCE ISSUES:** Failure to update software may lead to non-compliance with industry regulations, such as GDPR, HIPAA, or PCI DSS, which mandate the protection of sensitive data and implementation of security best practices.
- Non-compliance can result in hefty fines, legal penalties, and damage to your business's credibility, impacting your ability to operate and compete in the market.

LSU

# Strategies for Staying Informed

- **FOLLOW OFFICIAL CHANNELS:** Subscribe to Microsoft Security and Google Security blogs, newsletters, and social media channels to receive timely updates on new security features, patches, and vulnerabilities.
- Stay informed about best practices, security advisories, and actionable insights from industry experts to enhance your organization's cybersecurity posture.

- **TRAINING AND AWARENESS:** Educate employees about the importance of software updates and security best practices through regular training sessions, workshops, and awareness campaigns.
- Empower employees to recognize and report suspicious activities, phishing attempts, and potential security threats to the IT department or designated security personnel.

LSU

# Conclusion

- **RECAP:** Regular updates are imperative for maintaining the security of your business's digital infrastructure.
- Outdated software poses significant risks, including vulnerabilities, data breaches, and compliance issues.
- Staying informed about security updates and threats is essential for effective cybersecurity management.
- **KEY TAKEAWAYS:** Stay proactive: Enable automatic updates for Microsoft and Google products to ensure continuous protection against evolving cyber threats.
- Educate and empower: Train employees to recognize and report security threats and foster a culture of cybersecurity awareness within your organization. Also collaborate with IT professionals to leverage their expertise on emerging threats.

LSU