BUSINESS TECHNOLOGY SUMMIT 2024

Securing the Cloud: Advanced Security Measures in Azure

Housekeeping

- Please silence your phones. If you need to take a call, feel free to step outside and come back in.
- Sessions are being recorded and will be available after.
- Please use this QR code to take the session survey before heading to the next session.
- Survey responses get you more entries into the raffle at the end of the day. (prizes included Surface headphones, Smart Ray Bans, RayBan Meta Smart Bluetooth Glasses, and lots more).
- Wifi Info: BusinessTechnologySummit

Pasword: journeyteam!

Presenter

ALEX RYAN
PRACTICE DIRECTOR, AZURE

Navigating Cloud Security Challenges

- Cloud Security Defined: Protecting data, applications, and infrastructure from cyber threats in cloud computing environments.
- The Importance of Vigilance: As cloud adoption accelerates, so does the complexity and scale of security threats, making robust cloud security measures indispensable.
- Azure's Commitment: Leveraging cutting-edge security technologies and practices to safeguard assets in the cloud, Azure stands at the forefront of cloud security solutions.

Azure's Security Foundation

Building on a Secure Foundation

Trusted Security Architecture:

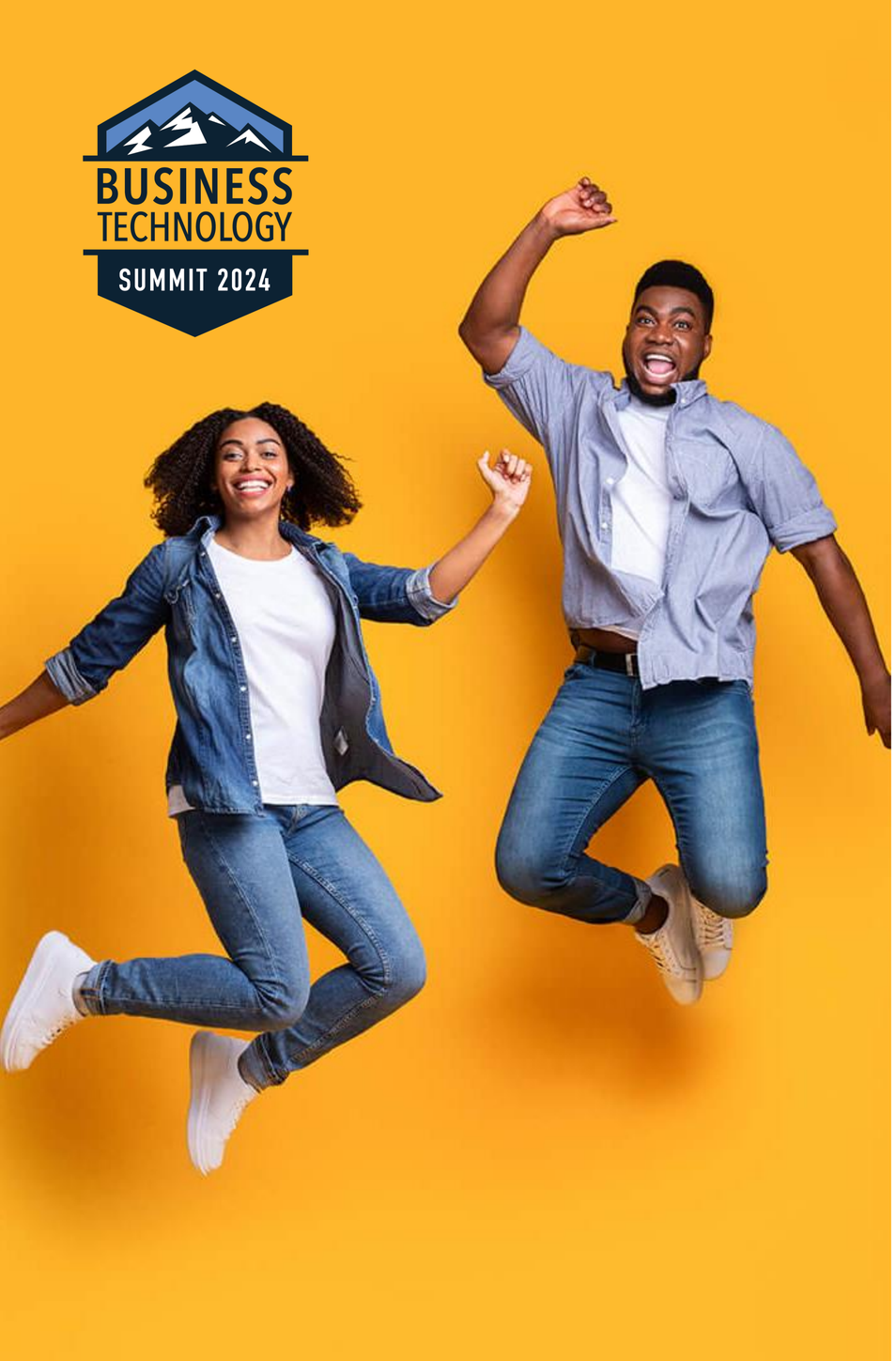
Azure's core infrastructure is designed with security in mind, utilizing state-of-the-art technology and practices to protect data, applications, and infrastructure from cyber threats.

Global Compliance and Certifications:

Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, GDPR, HIPAA, and FedRAMP, ensuring that your data is handled securely and in accordance with regulatory requirements.

Proactive Protection Layers:

Incorporating multiple layers of security measures including network security, data encryption, threat intelligence, and identity management tools to provide comprehensive protection.

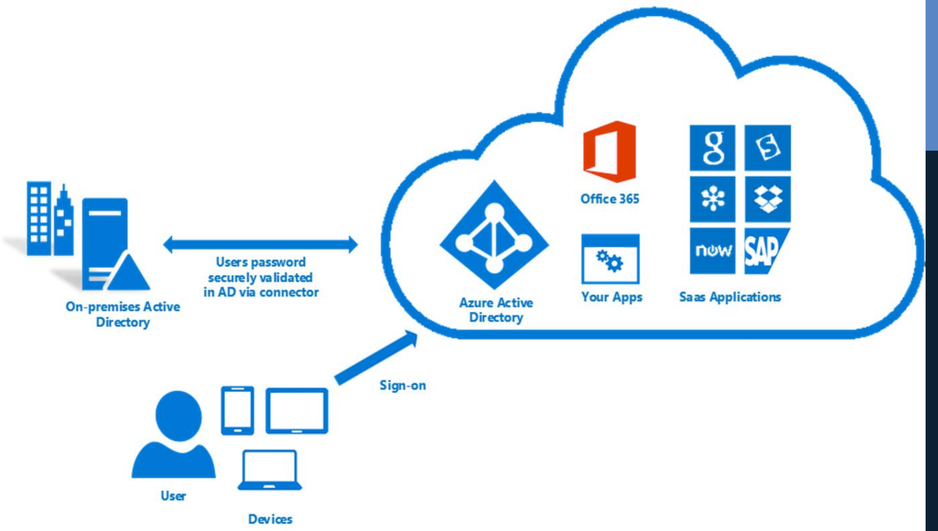


Mastering Access Control with Azure

- Centralized Identity Management: Entra ID serves as the backbone for secure, single sign-on (SSO) access to cloud and on-premises applications, streamlining identity management across the enterprise.

- Robust Access Policies: Implementing Role-Based Access Control (RBAC) and Conditional Access policies (CA) to ensure users have only the permissions they need, minimizing the risk of unauthorized access.

- Enhanced Security with Multi-Factor Authentication (MFA): Entra ID's Multi-Factor Authentication significantly bolsters security by requiring multiple forms of verification, effectively safeguarding against identity theft and other cyber threats.



Data Protection in Azure

Comprehensive Data Encryption

Utilization of Industry-Standard Protocols

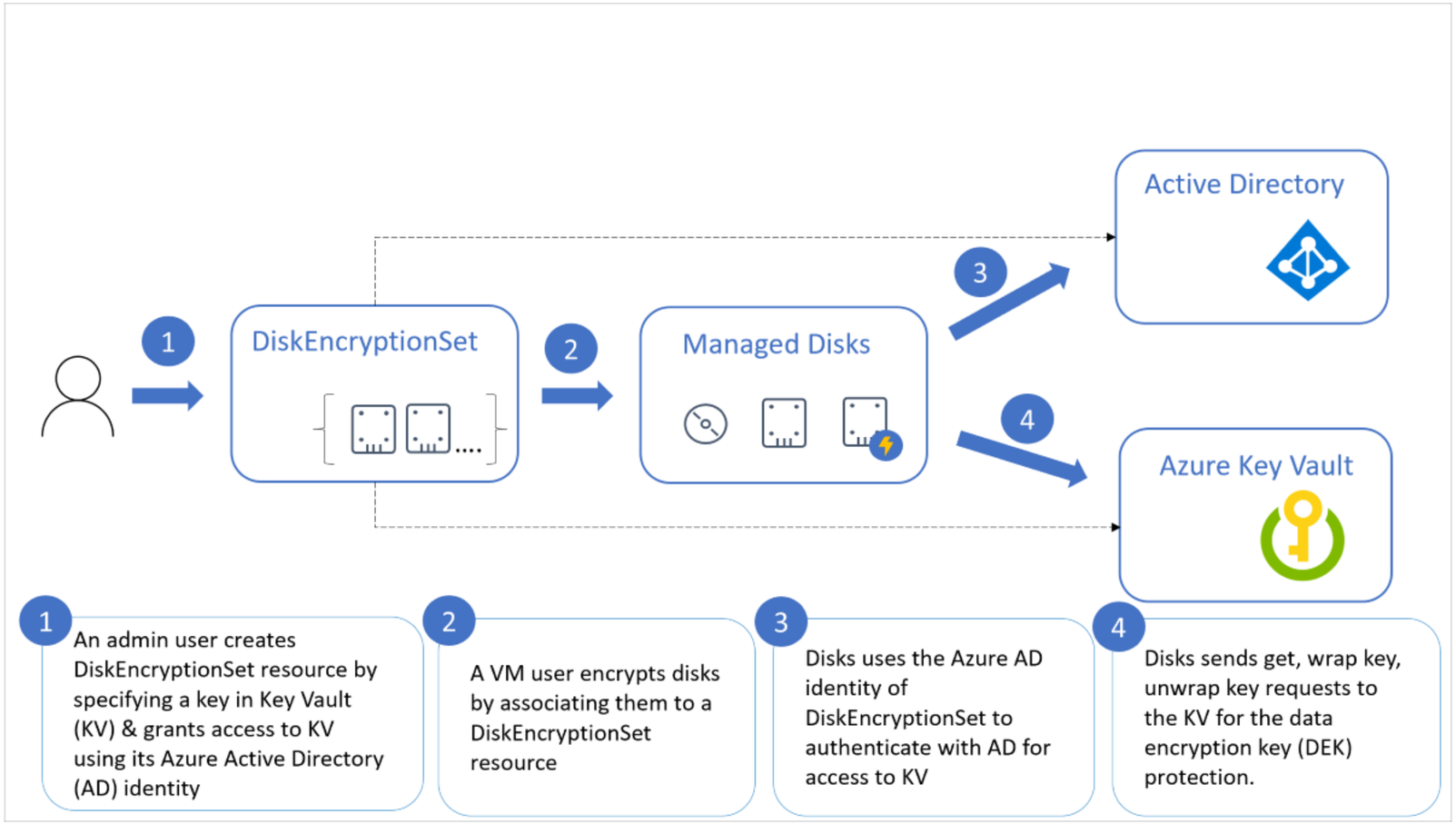
Azure employs advanced encryption standards such as AES-256 for data at rest and TLS 1.2+ for data in transit, aligning with global security best practices to ensure the highest level of data protection.

Seamless Integration Across Services

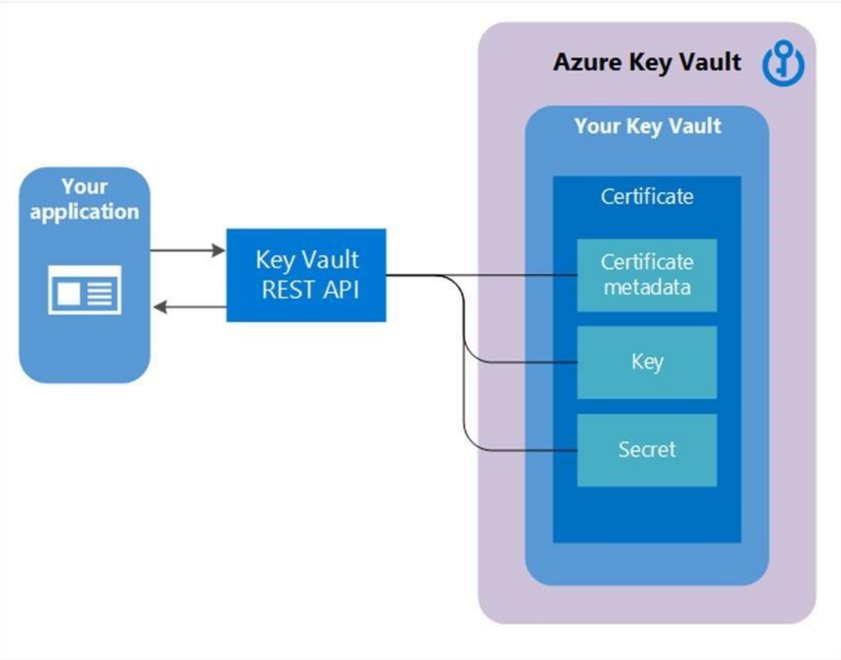
Encryption in Azure is deeply integrated across all cloud services, offering automatic encryption for data stored in Azure Blob Storage, Azure Files, and Azure SQL Database, among others, without compromising performance.

Customizable Encryption Options

Azure gives you the flexibility to manage your own encryption keys through Azure Key Vault, or to use Microsoft-managed keys for simplicity. This allows businesses to tailor their encryption strategy to meet specific security and compliance requirements.



Data Protection in Azure



Azure Key Vault

Centralized Key Management

Azure Key Vault centralizes the management of cryptographic keys, secrets, and certificates, offering a secure, streamlined approach to safeguard sensitive information.

Simplification of Application Secrets Management

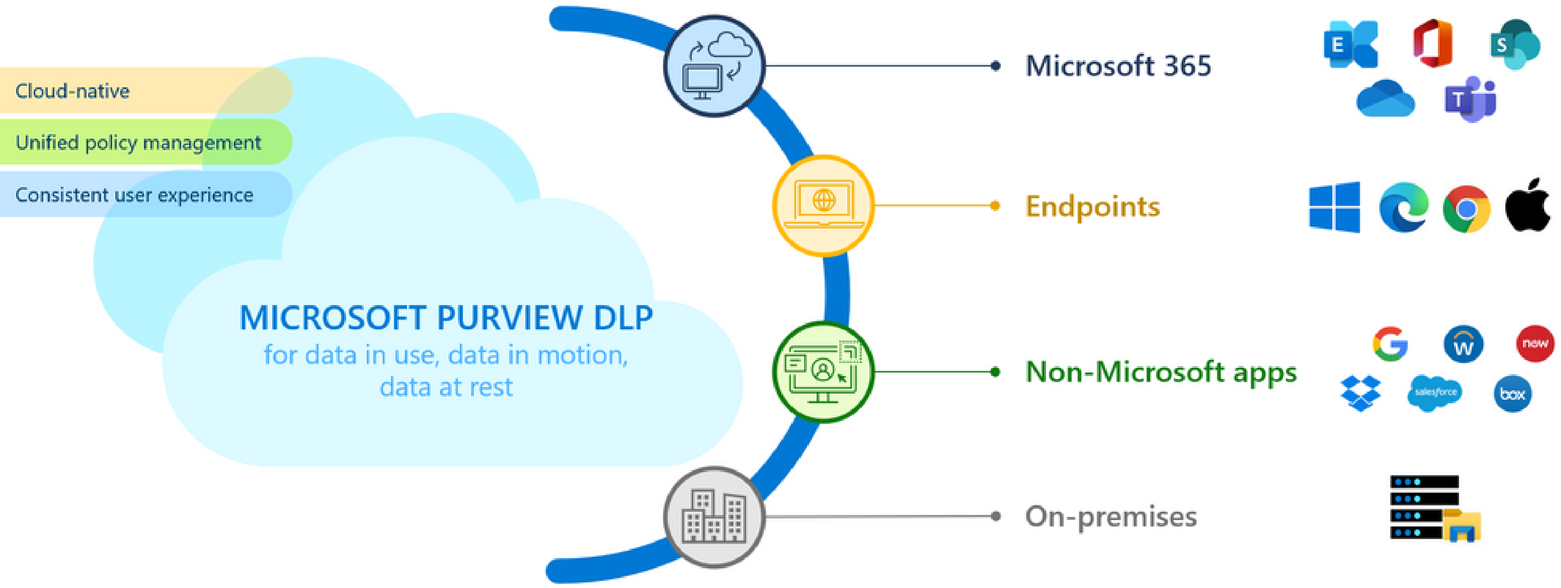
Developers can use Azure Key Vault to eliminate hard-coded keys and secrets in their code, significantly reducing potential security vulnerabilities.

Automated Rotation and Management of Secrets

Key Vault supports the automated rotation of keys and secrets, helping to maintain a strong security posture by ensuring outdated or potentially compromised credentials are replaced regularly. This automation not only bolsters security but also reduces the administrative overhead associated with manual key rotation policies.

Data Protection in Azure

A unified and cloud-native solution



Data Loss Prevention (DLP)

Advanced Detection and Classification

Azure DLP leverages sophisticated algorithms to automatically identify and classify sensitive information across your cloud environment, including personally identifiable information (PII), financial data, and confidential business documents.

Real-time Monitoring and Alerts

With Azure DLP, organizations benefit from real-time monitoring of their data, receiving instant alerts when sensitive information is at risk of being shared or accessed improperly.

Automated Policy Enforcement

Azure DLP enables the creation and enforcement of comprehensive data protection policies that automatically apply encryption, access restrictions, or other protective actions based on the sensitivity of the data.

BUSINESS TECHNOLOGY SUMMIT 2024

Threat Detection & Response

- Azure Security Center
- Azure Sentinel
- Automated Security Responses
- Integration with Microsoft Threat Intelligence

Azure Security Center

Unified Security Management

Azure Security Center serves as a central hub for managing security across your entire Azure and hybrid environment. It aggregates security alerts and recommendations from various sources, providing a single view that helps streamline your security management process.

Continuous Assessment and Recommendations

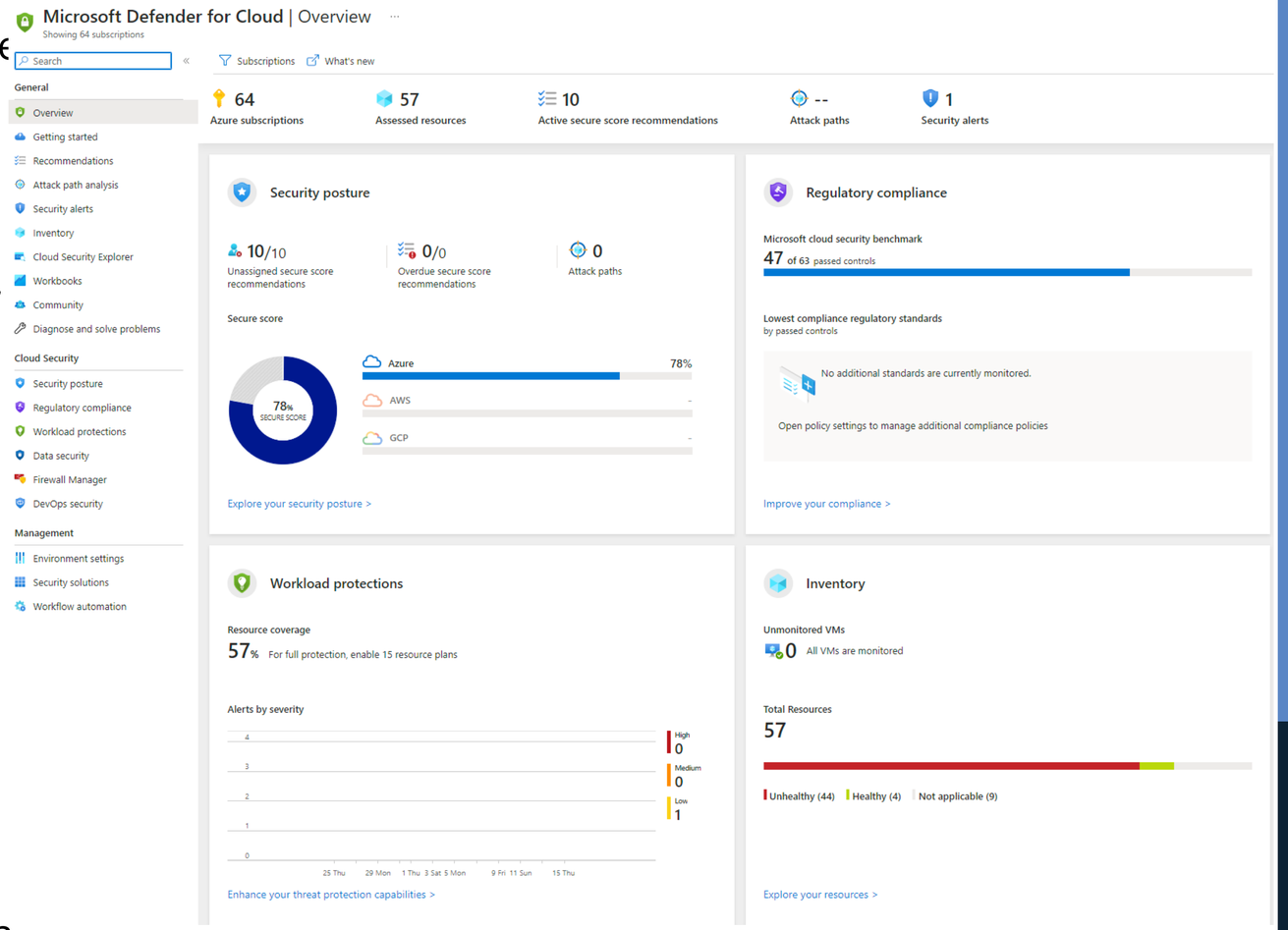
Leveraging continuous scanning and AI-driven analytics, Azure Security Center evaluates the security posture of your resources 24/7. It identifies potential vulnerabilities and misconfigurations, offering actionable recommendations to remediate issues.

Advanced Threat Protection

Azure Security Center includes advanced threat detection capabilities that utilize global threat intelligence, machine learning, and behavioral analytics to identify and alert on potential threats in real time.

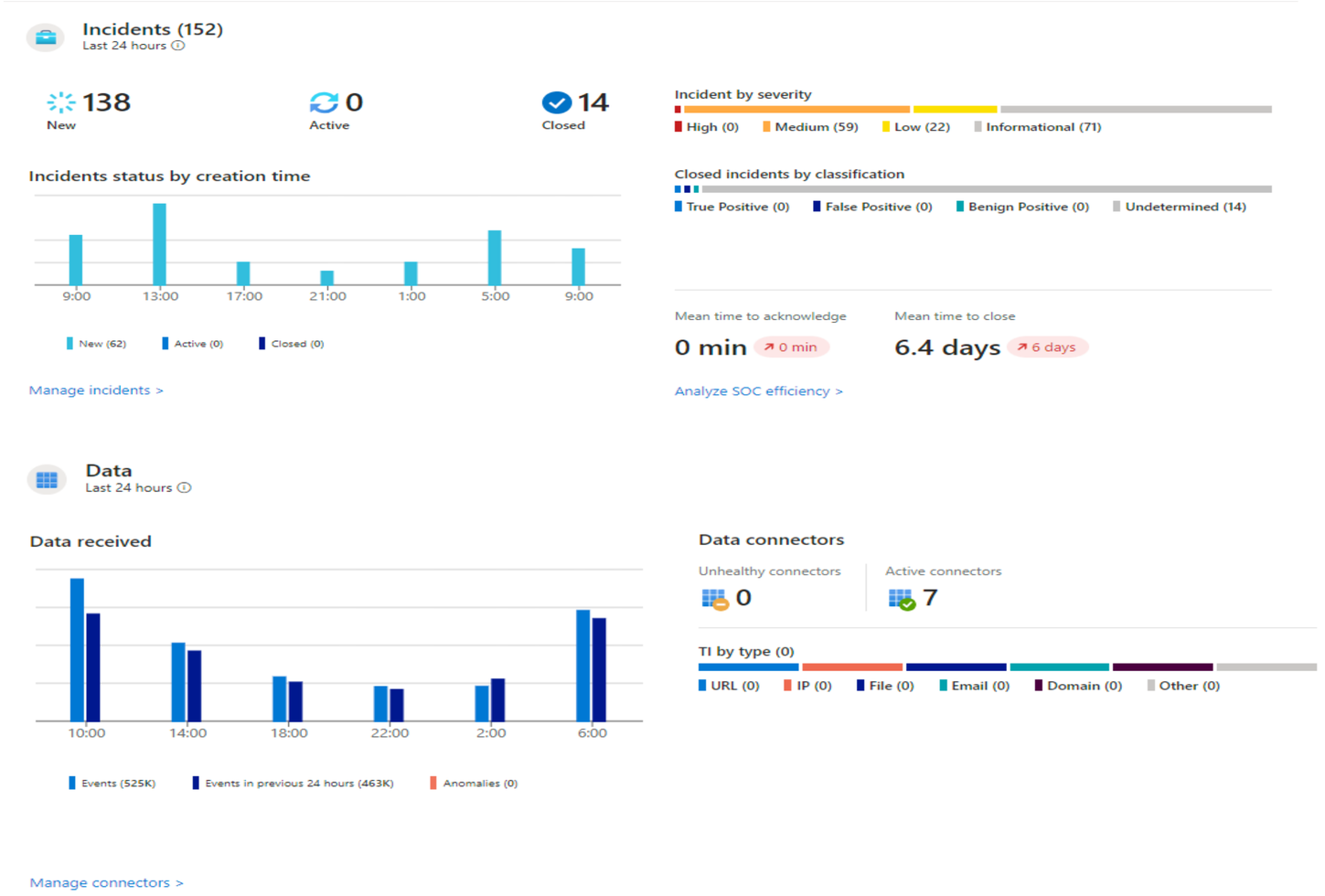
Automated Security Features

To further bolster your defenses, Azure Security Center offers a range of automated security features, such as just-in-time (JIT) access control for VMs and adaptive application controls.



Azure Sentinel

- Comprehensive Data Aggregation
- AI-Driven Threat Detection
- Streamlined Investigation and Rapid Response
- Seamless Integration with Existing Tools



Automated Security Responses:

Rapid Threat Mitigation

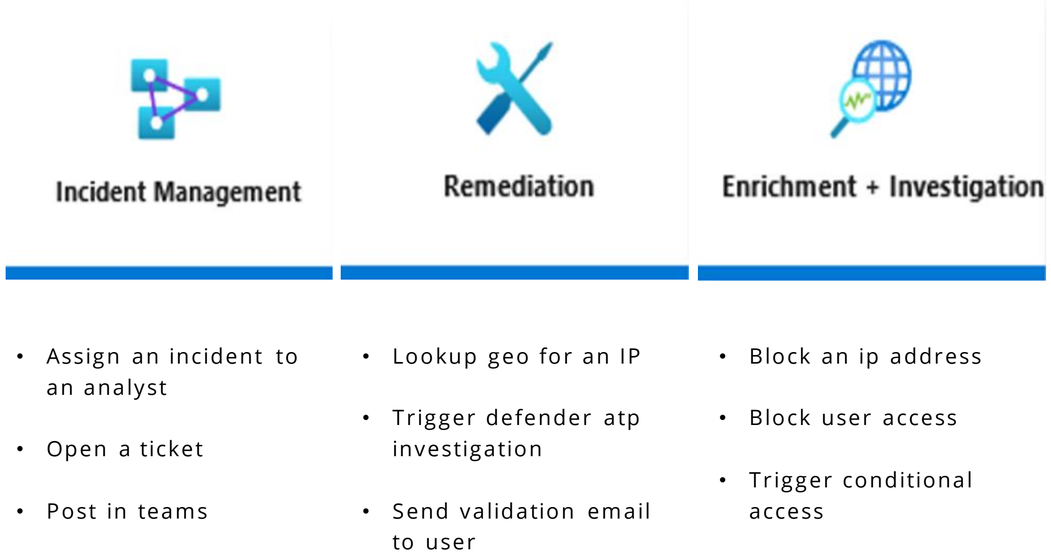
Azure's automated response capabilities significantly reduce the time it takes to address security threats. By automating the response process, organizations can swiftly mitigate threats, minimizing potential damage.

Customizable Playbooks for Tailored Responses

Azure Sentinel allows organizations to create and customize playbooks tailored to their specific security needs. These playbooks are automated workflows that can be configured to respond to various security alerts, from isolating affected systems to blocking suspicious IP addresses.

Integration with a Wide Range of Tools and Services

Azure Sentinel's playbooks can integrate with a vast ecosystem of tools and services, both within and outside the Azure platform. This flexibility allows for comprehensive automated responses that can leverage existing security tools, communication platforms, and even third-party services.



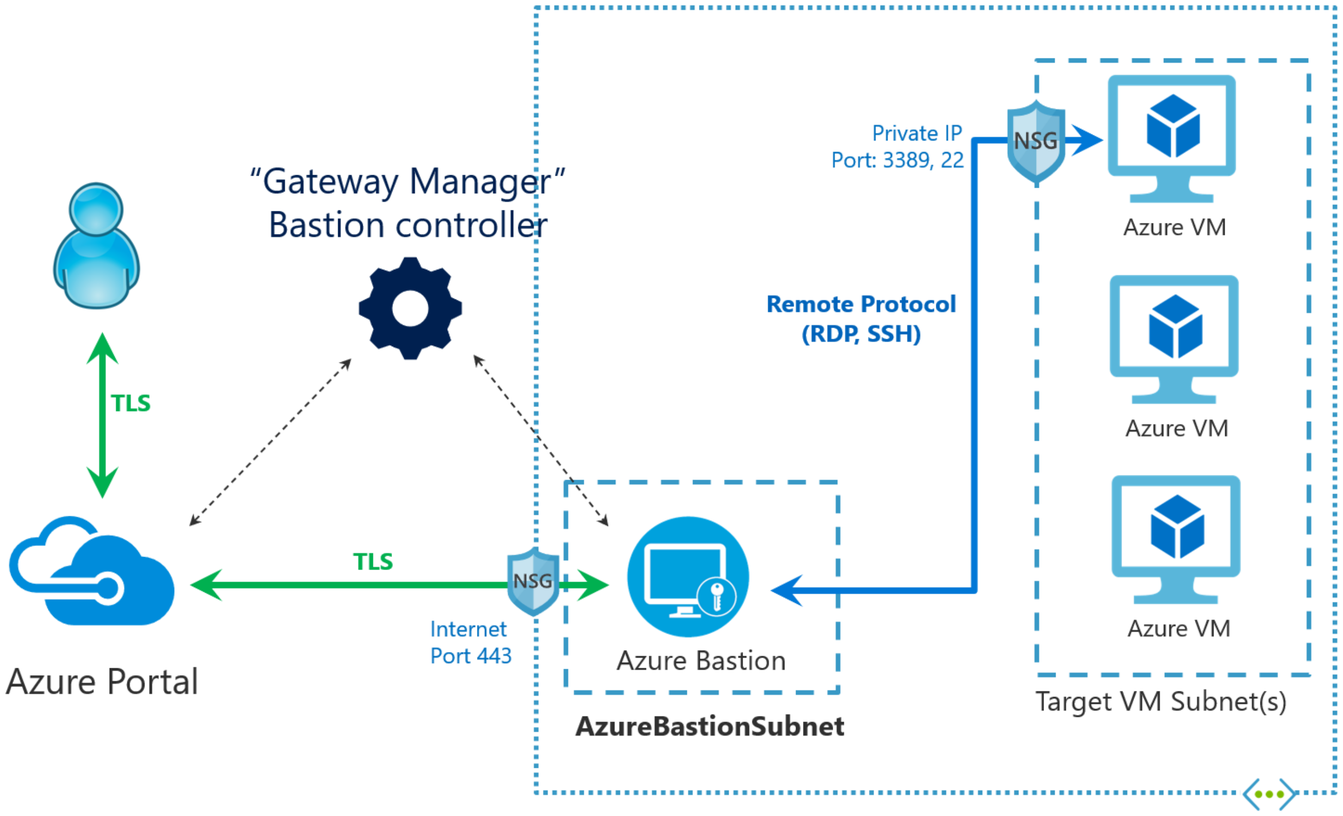
Integration with Microsoft Threat Intelligence

Real-time threat insights - azure security center and azure sentinel harness the power of Microsoft's extensive threat intelligence network, delivering real-time alerts and actionable insights.

Enhanced detection and response - the integration with Microsoft's threat intelligence empowers azure security center and sentinel with advanced analytics to detect anomalies and potential threats more effectively.

Global intelligence network - benefit from Microsoft's unparalleled threat intelligence, derived from billions of data points collected across its vast range of devices, services, and applications worldwide.

Continuous learning and adaptation - Microsoft's threat intelligence is continuously updated, ensuring that azure's security services evolve in tandem with the changing threat landscape.



Network Security in Azure

- Comprehensive Network Protection
- Advanced Threat Protection
- Secure Connectivity
- Network Security Monitoring and Management

Ensuring Compliance and Governance in Azure

- Leverage Azure Policy - Implement Azure Policy to enforce organizational standards and to assess compliance at scale across your resources. Utilize built-in policies for common regulatory standards or create custom policies to meet specific compliance needs of your organization.

- Manage Risk with Azure Compliance Manager - Azure Compliance Manager helps you manage your compliance posture with a centralized dashboard, providing insights into your compliance score and actionable guidance to improve it.

- Stay Informed with Azure Trust Center - Regularly visit the Azure Trust Center to stay updated on compliance certifications, service trust details, and security best practices. compliance with global standards.

BUSINESS TECHNOLOGY SUMMIT 2024

The Future of Cloud Security in Azure

The Evolution of Cloud Security in Azure

- **Innovative Security Technologies**

Azure is at the forefront of integrating cutting-edge security technologies, including AI and machine learning for anomaly detection, quantum-resistant cryptography to safeguard against future threats, and advanced network security solutions.

- **Enhanced Automation and AI-driven Security**

- The future of Azure security lies in further automation and the use of AI to predict, detect, and respond to threats in real time. By harnessing the power of AI, Azure aims to provide even more proactive security measures, reducing the need for manual intervention and enabling more sophisticated threat intelligence and response strategies.

- **Focus on Zero Trust Architecture**

- Azure is moving towards a comprehensive Zero Trust security model, which assumes breach and verifies each request as though it originates from an open network. This model emphasizes strict user verification, minimal access rights, and micro-segmentation to secure the network and data, reflecting a shift in how security boundaries are defined in the cloud era.

BUSINESS TECHNOLOGY SUMMIT 2024

Actionable Next Steps:

- Review your current Azure security configurations against today's insights.
- Leverage Azure Security Center and Azure Sentinel for comprehensive security management and threat detection.
- Consider a security assessment or consultation to identify and mitigate potential vulnerabilities within your Azure environment.
- Stay informed about the latest Azure security features and best practices through the Azure updates and community forums.

We love feedback!

Please complete the session survey **for an extra giveaway raffle ticket!**

BUSINESS TECHNOLOGY SUMMIT 2024

BUSINESS TECHNOLOGY SUMMIT 2024

Thank You!

Let’s Connect:

Alex Ryan

info@journeyteam.com