infopulse

Part of TietoEVRY Group

EBOOK

Best Practices for Implementing Remote Work Solutions

Based on Microsoft Cloud Platform

infopulse
Part of TietoEVRY Group

Content

infopulse
Part of TietoEVRY Group

Introduction

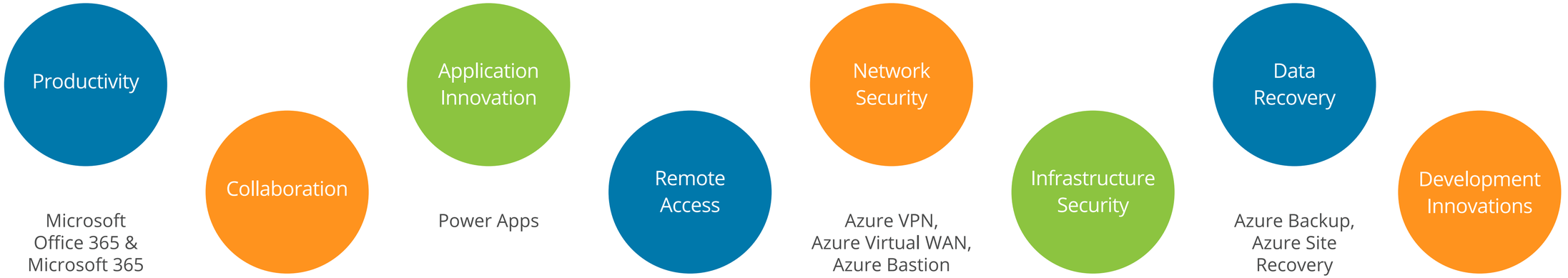
Remote work is entering the mainstream for the long-term. As strict lockdown measures have been lifted globally, most enterprises recognize that there's still no imminent need or benefit to returning the entire workforce back to the HQs. COVID-19 was an unexpected test in agility and remote readiness for companies and most scored a 'pass'. However, to remain remote in the long-term perspective, leaders need to look into broader and deeper technological changes that constant telecommuting requires.

In our new ebook, Infopulse team delivers a structured approach to scaling and securing remote operations on Microsoft Cloud and Microsoft Azure.

infopulse
Part of TietoEVRY Group

From Bottom-Up: Getting Your Front Office Operations on Microsoft Cloud

Your Journey to Remote Work



Source

infopulse
Part of TietoEVRY Group

Microsoft 365 Business & Enterprise – Your Productivity Cloud

“Darnitsa Pharmaceutical Company creates top-quality pharmaceutical solutions for solving complex healthcare problems. Aiming to deliver the best medicinal products on the Ukrainian market, Darnitsa is strongly committed to investing in own production and state-of-the-art technologies. Migration to the Microsoft cloud platform helped Darnitsa to leverage innovation and drive the rise of the internal corporate digital culture. New tools and solutions have already proven their efficiency, allowing for deeper engagement of all full-time and remote-working specialists.”

Andrey Romanenko, CIO at Darnitsa Pharmaceutical Company

Microsoft 365 is an integrated subscription-based cloud offering that allows your team to explore the best of Microsoft products – **Office 365, Windows 10 Enterprise, Intune, and Azure Active Directory Premium.**

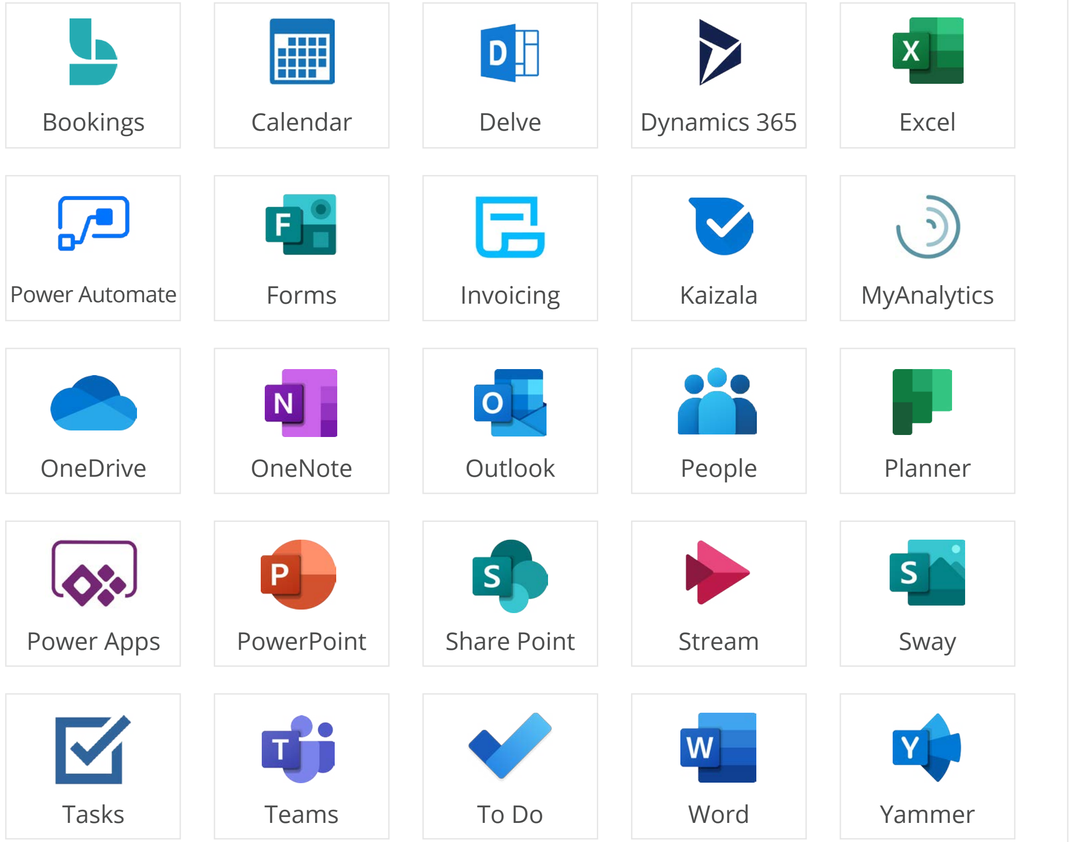
	Microsoft 365 Business Standard/ Premium	Microsoft 365 F3	Microsoft 365 E3	Microsoft 365 E5
Web and Mobile Microsoft 365 Apps	+	+	+	+
Desktop M365 apps (up to 5 PCs/Macs + 5 tablets + 5 smartphones per user)	+/–	–	+	+
Email and calendaring (Outlook, Exchange, Bookings)	+	+/– (Bookings not included)	+	+
File storage and sharing (OneDrive, Stream, and Sway)	+/– (Only OneDrive is included)	+	+	+
Communication and Intranet (Microsoft Teams, SharePoint, Yammer)	+/– (Teams and SharePoint included)	+/– (Audio calls and Phone System Connection not included)	+/– (Audio calls and Phone System Connection not included)	+
Task Management (Power Apps, Power Automate, To Do, Planner)	+	+	+	+
Advanced Security and Device Management	+/– (Only in Business Premium)	+	+	+
Analytics (Power BI Pro)	–	–	–	+
Identity Management with Azure Active Directory Premium plan	– (But Azure AD Premium P1 is coming soon for Premium Customers)	–	–	+ (Azure AD Premium P2 included)
More Details on the Offer	Learn more	Learn more	Learn more	Learn more
Monthly Pricing	**M365 Business Standard – $12.50 user/month** **M365 Business Premium – $20.00 user/month**	**$10.00 user/month**	**$32.00 user/month**	**$57.00 user/month**

infopulse
Part of TietoEVRY Group

Microsoft Office 365

Office 365 is a familiar set of Microsoft business apps, hosted and enhanced by the power of the cloud. Empower your team with the tools to create, collaborate, and contribute to important conversations remotely. Office 365 lets your workforce stay on top of every conversation, data exchange, and update by providing them with continuous access to essential business apps and communication tools.

Microsoft Office 365



Source

Key features:

- Always up-to-date web versions of Microsoft Word, Excel, PowerPoint, and SharePoint.
- Outlook email box and business address.
- Up to 1TB of storage space per user at OneDrive Business.
- Access to Microsoft Teams and Office 365 Groups – for collaboration.
- Always-on data security with Office 365 Threat Protection.
- Power Apps and Power Automate – the new tools for building simple workflow automations and more advanced business apps.
- Seamless, company-wide compliance management tools.

Get a 6-month free trial of Office 365 E1 for up to 3,000 users as a new customer or extra seats if you are an existing customer.

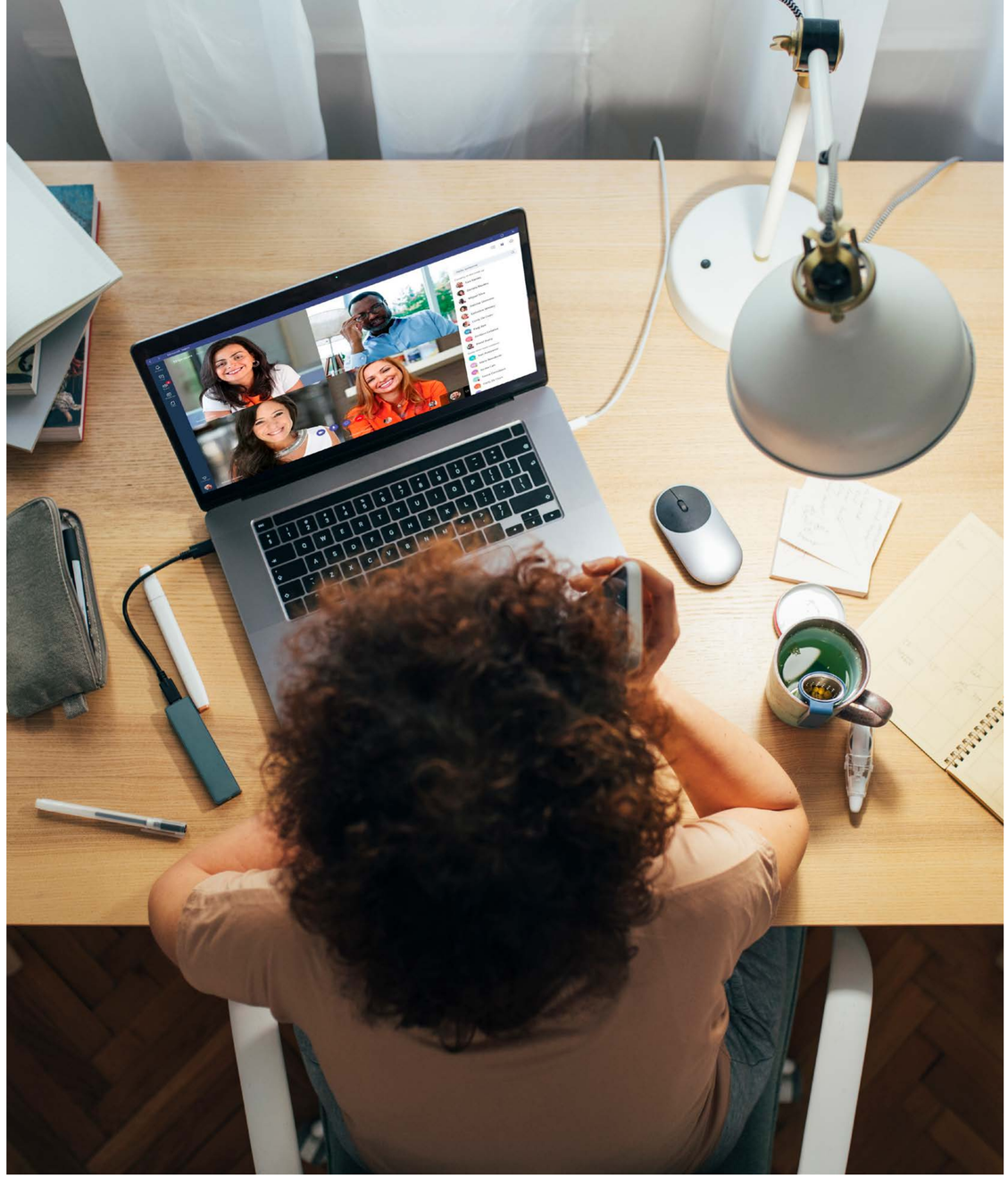
Contact us for more details.

CONTACT US >

infopulse
Part of TietoEVRY Group

Ramping Up Remote Work Productivity in Office 365

The biggest boon of Office 365 is its multi-app collaboration functionality. With apps such as Exchange Online, Outlook, and Microsoft Teams, your team members can collaborate in real-time, work on the same documents from favorite devices, thanks to auto-sync and OneDrive. They'll be able to remain a closely-knit, productive team despite being geographically apart.

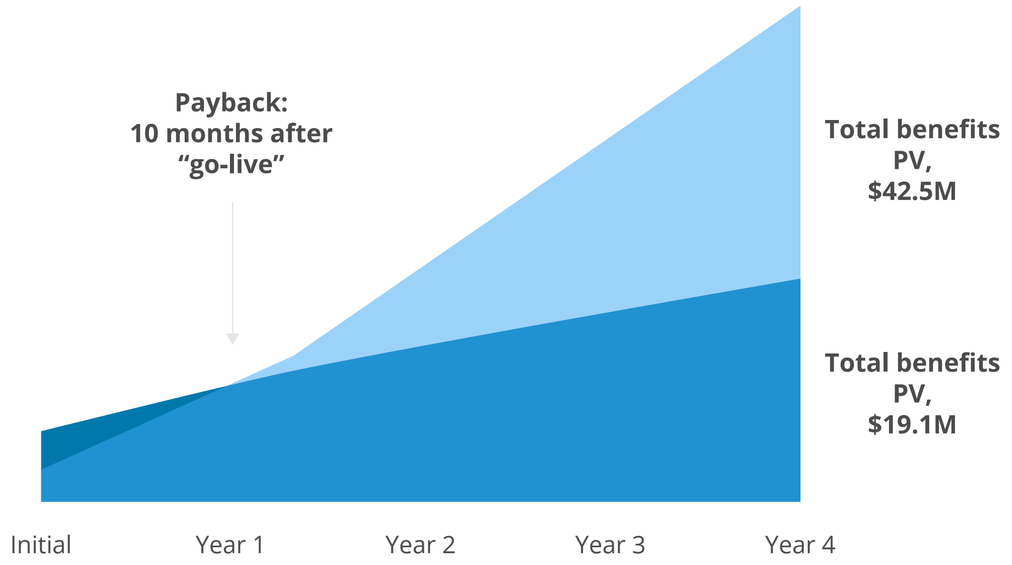


infopulse
Part of TietoEVRY Group

Benefits Post-Adoption

- **69%** of companies[1] report an increase in workforce productivity.
- Over **100 minutes** saved per week due to improved collaboration and information sharing, especially around co-authoring and document reviews.[2]
- Over **104 minutes** saved each week with better online meetings.
- Downtime reduced by **15.75 hours** annually for each Microsoft 365 user.
- Over **135 minutes** saved per request with automated application and resource provisioning.
- It takes **14.18 fewer days** to develop a new product thanks to streamlined business processes.

Total Value of Microsoft 365 Adoption



Source

[1] *The State of Office 365 Performance Survey 2019*

[2] *The Total Economic Impact™ Of The Microsoft 365 E5 Solutions*

Best Practices for Remote Collaboration in Office 365

Best Ways to Organize Your Workday

Co-author in real-time

Brainstorm a PowerPoint presentation, review Office documents, or contribute to Excel files – all in real time. Stay on the same page with your team and have all the key data auto-synced and backed up with the Auto-Save feature.

Use @mentions to tag others

Call on your collaborator in any app or communication channel by tagging them. Increase the pace of everyone's work by drawing attention of influencers to what truly matters.

Run a collective notebook

Share notes, ideas, and summaries in a virtual shared OneNote notebook, so that everyone on the project can easily find and review the key information.

Perform task management on the go

Stay up to date on the teams' progress and cross off items from your personal list from any device using the Planner app. Understand who's doing what at the moment and what overall progress is being made at a glance.

No more scattered copy versions

All the documents you create are automatically saved in different versions. You can easily switch between different versions to review changes or roll back to earlier iterations.

Chat in files

Stop switching gears all the time. You can now start a quick discussion straight in a word doc and @ask your colleagues to chip in as if you are sitting just across the office.

Meet and greet

Have instant access to everyone's calendar. Book and manage meeting time slots in several taps in the Calendar app. Seamlessly exchange your meeting notes, share your screen, and record footage. The Office 365 ecosystem makes it delightfully simple to have a productive online meeting.

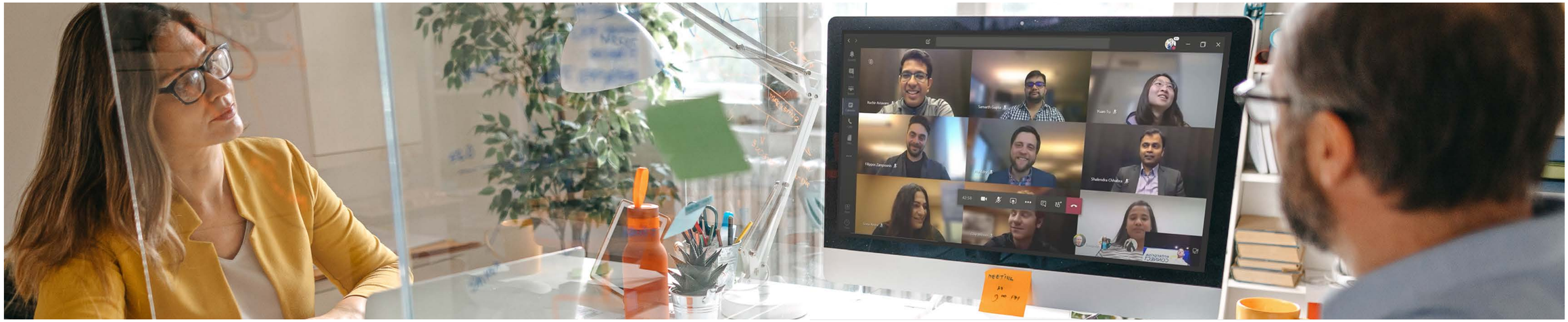
Microsoft Teams

Microsoft Teams can be the first, last, and single step in organizing your department's inner work. Fully integrated with most other business apps in the Microsoft ecosystem, Teams provides you with a single pane view into all communications and day-to-day tasks. Schedule video meetings, review multiple chat streams, assign tasks, monitor execution, and facilitate systematic knowledge sharing in your organization.

Key features:

- **Real-time user presence and information availability,** updated based on the Outlook Calendar appointments and participation in conference calls.
- **Personal chats and group chats (up to 100 users),** packed with advanced features for organizing, filtering, and prioritizing messages. Support of multiple chat formats (in-document conversations, code snippet exchanges, screen, and image sharing).
- **Audio-, video-, and web conferencing functionality** and a live events feature for streaming HD video for up to 10,000 participants.
- **Agile task management suite** for planning personal and group tasks, creating checklists, status reports, and prioritizing different task cards.
- **Strong, company-wide security,** ensured by two-factor authentication, single sign-on through Active Directory, and file/data encryption, powered by the latest security mechanisms.

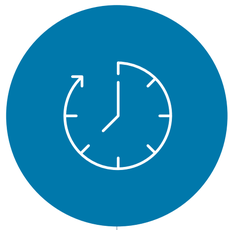
Learn more about [Microsoft Team key features from our blog post.]



infopulse
Part of TietoEVRY Group

Benefits Post-Adoption[3]

Benefits from the Solution Adoption in a Three-Year Period



Depending on the role, Teams users can **save between 1.1 to 8.0 hours per week** by having all tools in one place for better collaboration and information sharing.

By the third of its usage, online meetings in Microsoft Teams can **replace as many as 150 overnight trips** per enterprise.

With Teams, key decision-makers i**mprove their time-to-decision by 17.7%.**

350 users working closely with customers **save 24 minutes per day with Teams** that totals to $759,493 in operational savings within 3 years.

Infopulse can provide you with access to **a free Microsoft Teams license, valid through January 21, 2021.**

GET TO KNOW THE OFFER DETAILS >

[3] *The Total Economic Impact™ Of Microsoft Teams*

Maximizing Remote Work Productivity in Teams: Tips and Tricks

Take advantage of pre-made templates when setting up new teams (or create custom templates for your organization). Microsoft recently launched a collection of Templates for Teams, making it even easier to start a new group project in Teams.

The templates are created around common business scenarios such as crisis response or marketing management and also adapted for different industries – banking, healthcare, operations, and more.

Each Template for Teams features:

- Predefined channels.
- Suggested apps.
- Implementation guidance.

You can also templatize and standardize existing team setups to scale best practices across the organization.

Enhance your setup with custom apps and workflow automations. Use Power Automate business process templates to streamline repetitive actions using pre-built process templates. Admins can also distribute custom business apps, made in Power Apps, to individual teams or cross-organization.

Improve your scheduling and appointments via Bookings and Shifts apps. Both are directly integrated into Teams, allowing you to schedule, manage, and conduct virtual appointments with internal and external users. A set of new capabilities in the Shifts app now allows a greater degree of workflow automation, so that your team members and their managers can waste less time on approving shift requests and other low-value admin tasks.

Take advantage of the Immersive Reader – a robust text-to-speech tool that can read aloud key information from the screen, while you are on the go.

Augment your Teams with third-party app integrations that can enhance an array of regular tasks, meetings, and other work exchanges.

Recommended product combos:

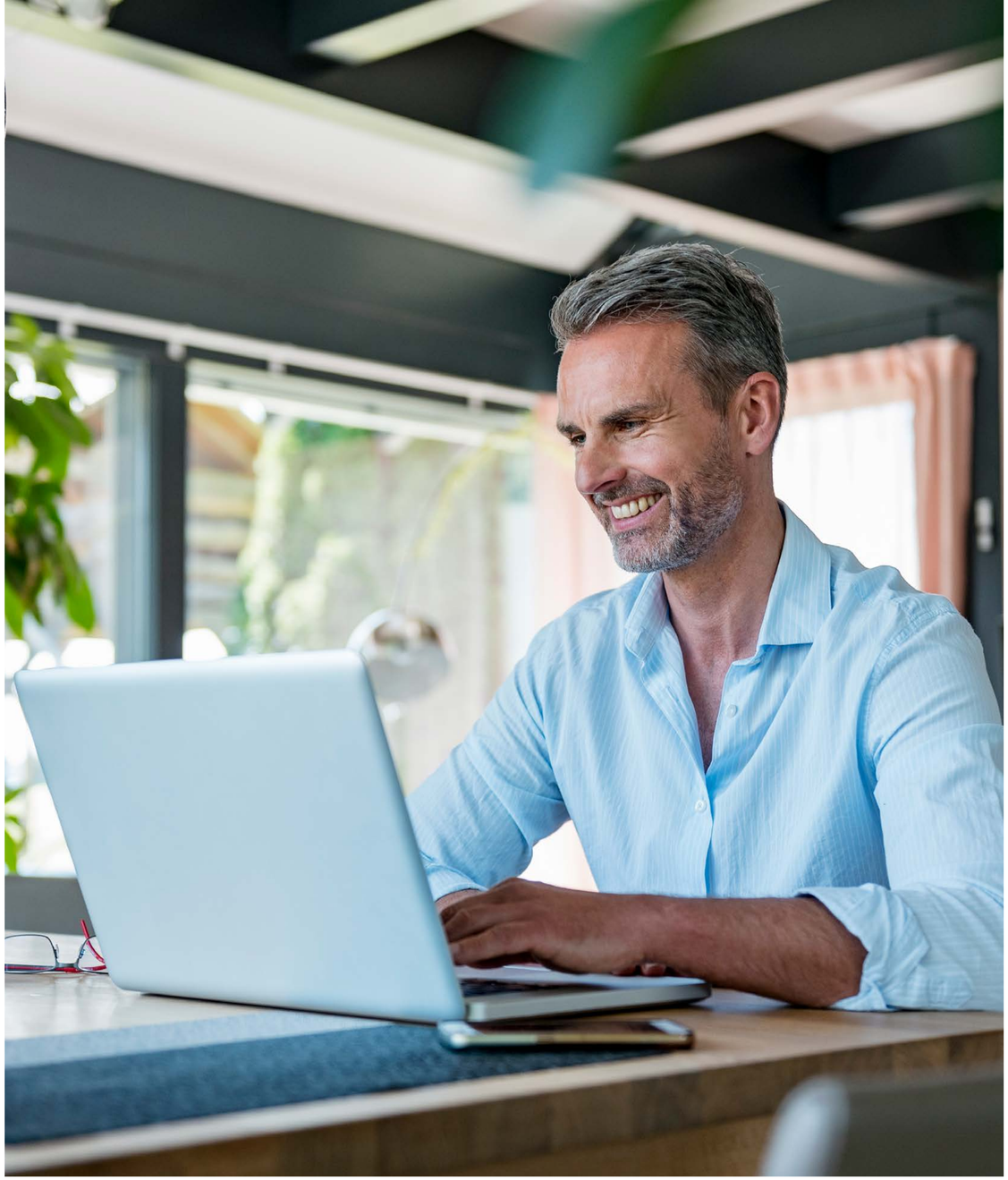
- **Microsoft teams + AgilePolly –** an efficient duo for hosting and documenting standups cross-organization. AgilePolly automatically collects standup data each day during the entire project span. When integrated with Teams, it allows you to review every team member's contribution to the project, plus promote better knowledge sharing and perform retrospective analysis, based on historical data.
- **Microsoft Teams + Workboard –** with a Workboard integration your team gains access to advanced project planning tools such as Kanban boards, status reports, and strategy alignment tools for monitoring key results (OKRs) and KPIs execution. On top of that, you can request updates on business objectives, KPIs, meetings agendas, and tasks in real time from WoBot – an AI-powered platform-built chatbot.
- **Microsoft Teams + InVision Freehand Board –** add everyone's favorite whiteboard to your Team streams. Use it for real-time charting and visual note exchanges.
- **Microsoft Teams + Trello, Asana or Wrike –** power up your project management by integrating one of these apps straight to your Teams space, so that no important tasks fall through the cracks.

infopulse
Part of TietoEVRY Group

Make Remote Employees the True Power Brokers in App Development with Power Apps

Power Apps is a PaaS (platform as a service) offering from Microsoft that allows anyone on your team to assemble new business apps for corporate usage based on reusable templates, pre-made integrations, and drag & drop UI development features.

Mobile-first, low-code, and robust, Power Apps is an efficient tool for speeding up your app development capabilities without placing additional pressure on senior IT department members. With the help of it, you can develop and deploy new business applications faster and at a lower cost to enhance other products within your Microsoft ecosystem, instead of investing in custom software development or more expensive off-the-shelf solutions.



Key features:

- **Access to a collection of sample web and mobile business apps** that can be rapidly adapted to your company's workflows.
- **Over 200 pre-made integrations (connectors)** to seamlessly integrate data and additional functionality into your app from across the Microsoft 365 ecosystem.
- **Securely connect external data via custom API integrations** or use the Gateway technology to connect on-prem data sources.
- **Select among multiple forms of data storage,** from SQL relational databases to unstructured blob storage.
- **Seamless integration with Microsoft Azure** that allows extending your Power Apps functionality to enterprise-grade solutions with advanced features such as AI services or Big Data analytics.

infopulse
Part of TietoEVRY Group

Benefits Post-Adoption[4]

- **70% reduction** in application development cost and effort.
- **38% decrease** in ongoing application management and maintenance effort.
- **122,850 worker hours** can be saved by Year Three of adoption within a large enterprise.
- **Up to $5.32 million** worth of increased process efficiencies can be achieved by Year Three.
- **$72,820** is the average internal and professional application development cost per Power App application.

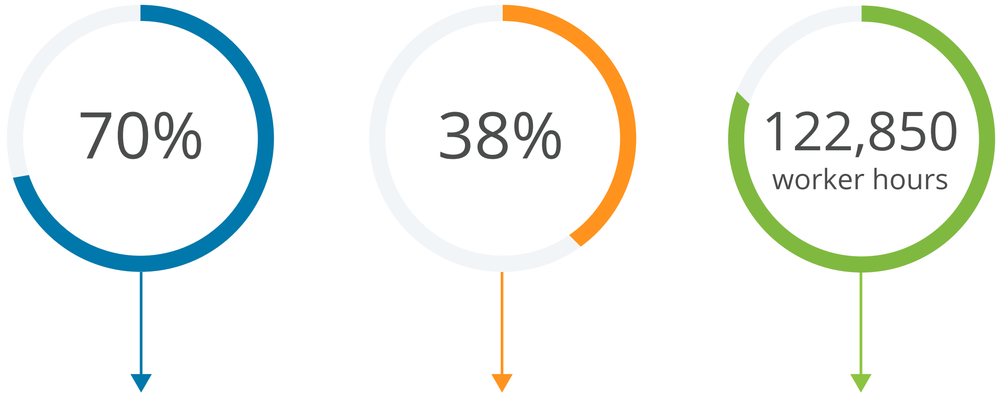
Infopulse offers rapid business application development services using Power Apps for a variety of use cases, ranging from sales to procuring, financial reporting, and supply chain management.

Learn more about our expertise.

LEARN MORE >

[4] *The Total Economic Impact™ Of Power Apps And Microsoft Flow*

Advantages of Power Apps Adoption



Reduced app development cost and effort

Decreased app management and maintenance effort

Saved by the third year of utilizing the solution

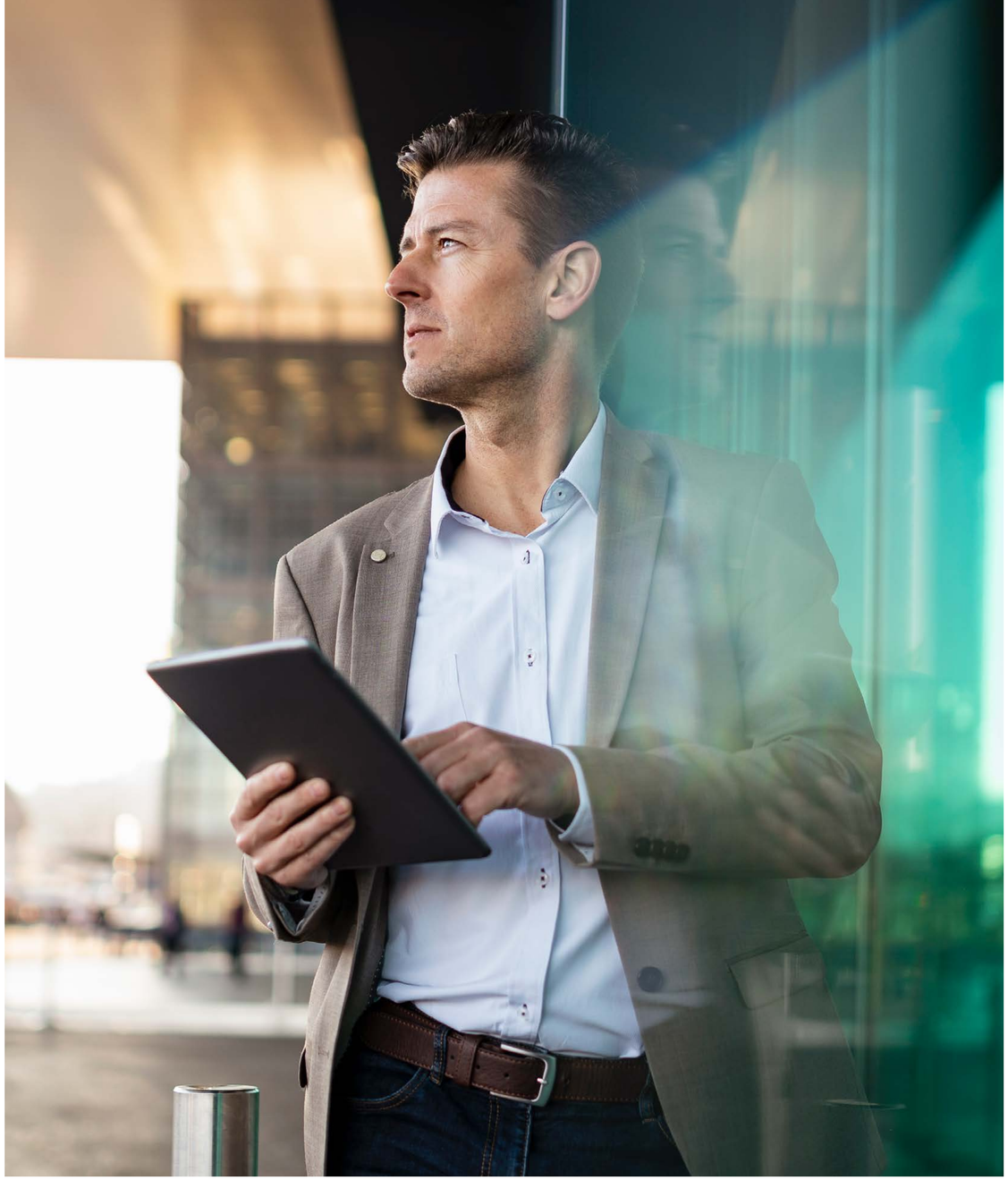
Source

infopulse
Part of TietoEVRY Group

Securing Your Remote Operations in Microsoft 365

Microsoft 365 cloud platform and all the connected services already come with state-of-the-art data encryption and in-built security mechanisms for protecting the most sensitive corporate data.

However, cybersecurity is a **joint responsibility**. As a customer, you'll have to ensure that your architecture, networks, and accesses are properly configured; all the necessary patches and updates get installed regularly. Educating your team members on basic security best practices is another key step to ensuring that your remote operations remain safe against external intruders. Clearly communicate the latest best practices and enforce stronger automated security measures in areas where user negligence can lead to security breaches.



Microsoft 365 Security Essentials Checklist

- **Enable multi-factor authentication for administrator accounts by default.** Consider doing the same for regular users working with sensitive information.
- **Keep the Outlook 365 mailbox logs auditing enabled by default for each user.** Perform regular log analysis. Educate users on common phishing and social engineering scams.
- **Verify that Azure Active Directory password sync is configured correctly before migrating users.** If you have password sync enabled in Azure AD Connect for on-premises apps, during the migration the passwords from on-premises software will overwrite the password in Azure AD. If the on-prem identity is compromised, the intruder can gain access to the cloud too.
- **Disable any legacy email protocols still in use** (unless absolutely necessary) and/or limit their usage to select users.
- **Enable anti-malware protection for all inboxes** and use the ATP Safe Attachments functionality to prevent malware distribution.
- **Find a good balance between Standard and Strict security measures** in EOP (Exchange Online Protection) and Office 365 ATP to balance security with user experience. You can review the recommended settings here.
- **Monitor for behavioral anomalies** such as excessive downloads of sensitive information per user, repeated logins from unusual locations, repeated non-permissioned access requests, and similar types of activities.
- **Continuously audit how corporate data is stored and shared.** In particular, scan unencrypted OneDrive and SharePoint documents for the presence of any personal customer/user information (email addresses, names, passwords, etc). Your IT team should know exactly where sensitive information is stored, who has access to it, and how it’s being shared.

infopulse
Part of TietoEVRY Group

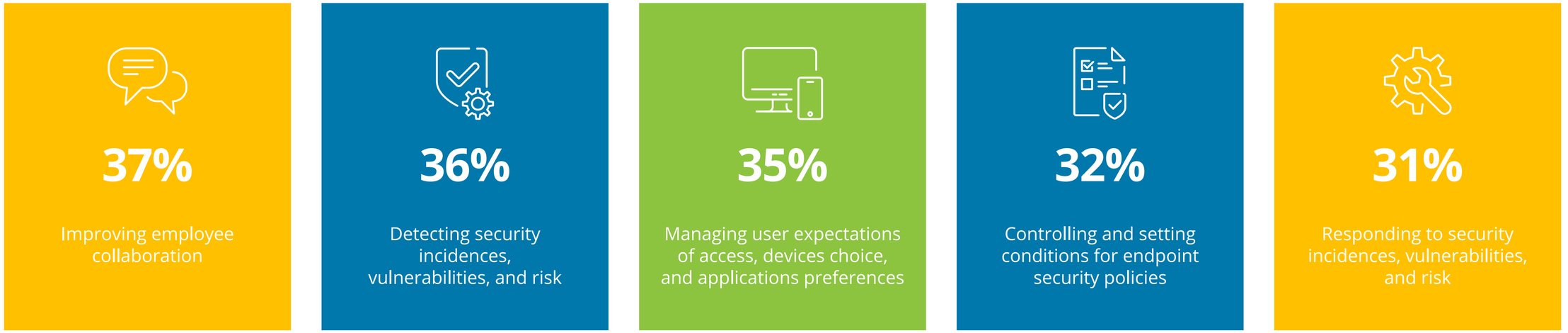
Azure VDI: Cloud Desktop Designed for Remote Work

Azure Virtual Desktop Infrastructure (VDI) is a native desktop and app virtualization service, designed specifically for Windows. Easy to implement and manage, Azure VDI can be instantaneously delivered and configured for a variety of remote machines, so that your team could have continuous access to multi-session Windows 10, desktop versions of Microsoft 365 apps for enterprises, along with your Remote Desktop Services (RDS) environment.

"Desktop virtualization slashes the costs of software licensing, updates, security, and compliance for the remote workforce."

Azure VDI lets you provision and scale access to a multitude of modern and legacy desktop apps in a matter of minutes through unified management in the Azure portal. Also, it allows improving your IT management without increasing the team size or operational costs.

Benefits of Azure VDI



Source

- Desktop virtualization environment without the need to run any extra gateway services results in minimized TCO.
- Instant scaling by adding new host pools in several clicks to accommodate higher workloads.
- Auto-scaling for individual users based on their activity.
- Support for hybrid workloads, running both on-premises and in the cloud.
- Fast troubleshooting of infrastructure issues and rapid response to end-user requests with a comprehensive Diagnostics service.
- Built-in delegated access to assign roles and collect insights on various errors.
- Increased efficiency: Azure VDI eliminates the need to manage infrastructure, as you manage only the image and virtual machines (VMs).
- Top security by using Azure AD for authenticating all end-users.

Best Practices for Azure VDI Adoption

“Four in ten organizations have deployed VDI, and current users have aggressive expansion plans.”

Enterprise Strategy Group[5]

Cloud-based VDIs have a clear advantage in terms of IT efficiency and security – they are **more secure than traditional desktop provisioning**. At the same time, cloud VDIs command a different approach to security responsibilities altogether.

Azure VDI practices **the ‘shared responsibility’ approach:** while most of the infrastructure already comes secured for your environment, certain facets will need to be configured manually to meet your company’s security needs:

Security need	Is the customer responsible for this?
Identity	Yes
User devices (mobile and PC)	Yes
App security	Yes
Session host OS	Yes
Deployment configuration	Yes
Network controls	Yes
Virtualization control plane	No
Physical hosts	No
Physical network	No
Physical datacenter	No

Source

[5] *Enterprise Strategy Group: Research Highlights: Are Desktops Doomed*

Essential security best practices:

- Enable Azure Security Center Standard for all VMs, subscriptions, key vaults, and storage accounts (learn more about ***Azure Security Center on page 45***).
- Set up multi-factor authentication for all users and admins in Windows Virtual Desktop.
- Collect audit logs to monitor all user activity on Windows Virtual Desktop.
- Rely on the Azure Monitor service to monitor service's usage and availability, and enable timely resource scaling when the need arises.
- Enable endpoint protection on all session hosts and consider using additional endpoint detection to strengthen security.
- Issue timely software patches. Base images should be patched monthly to ensure maximum security.
- Set maximum inactive time and disconnection policies for all users.

A Few Tips for Migrating to Azure VDI:

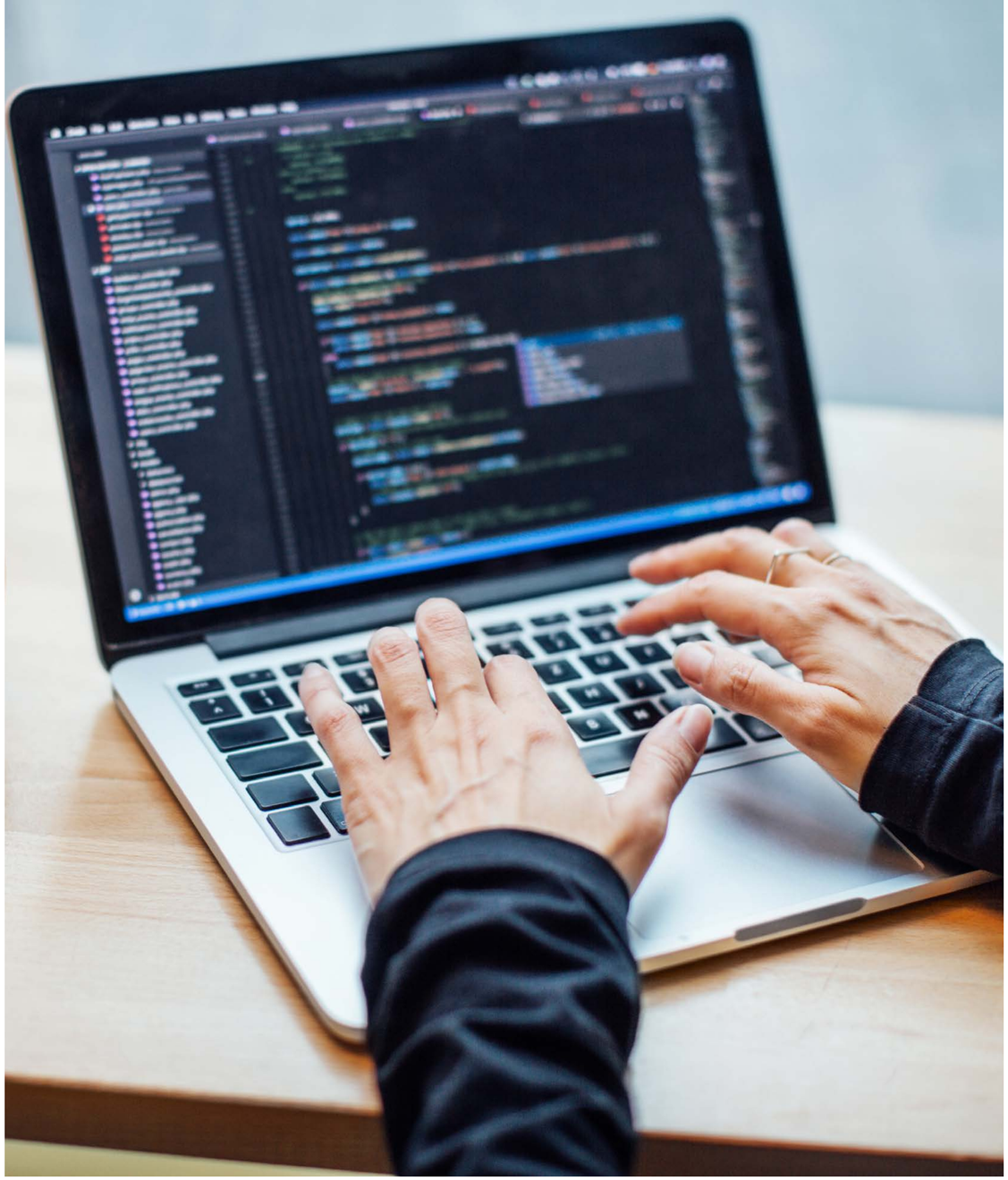
- Not every desktop app is a good candidate for cloud VDI. Conduct an inventory of your apps and prioritize a lineup for migration based on the needs of your end-users.
- Map out your target architecture in advance. Right-size your infrastructure to the workloads you are planning to send to the cloud.
- Establish formalized roles for different types of end-users and a set of supporting best practices for infrastructure configuration that will help ensure that the users' needs are fully met.

Operating in a regulated industry? Prior to VDI adoption, **create a detailed cloud governance framework** that would align your people, processes, and technology with adopted security, risk management, and operational practices to ensure full compliance.

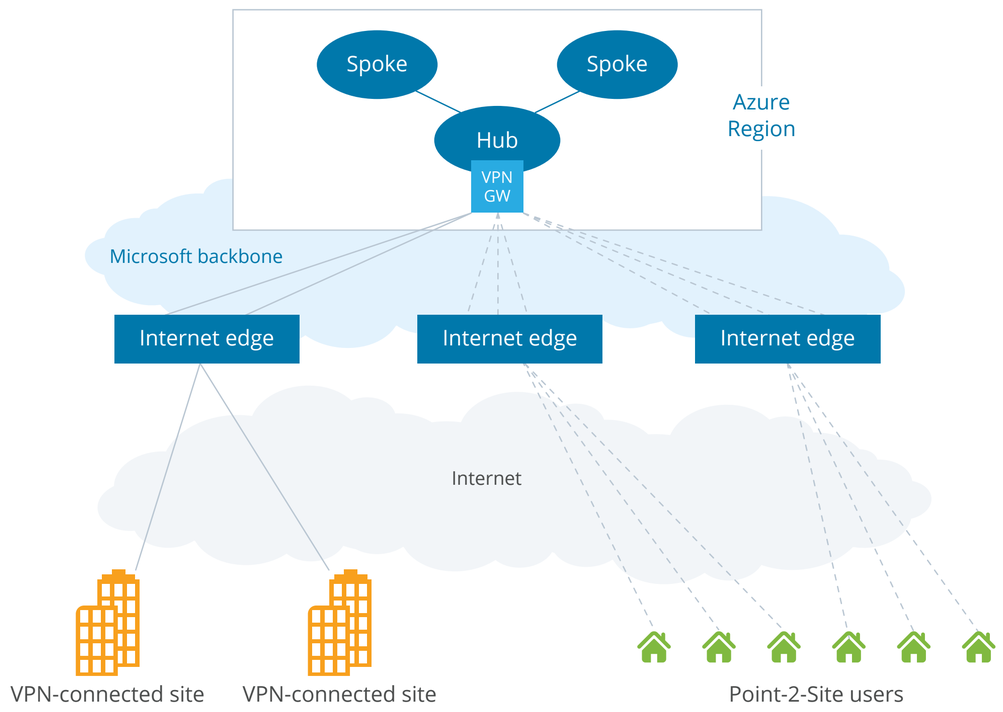
infopulse
Part of TietoEVRY Group

Essential Azure Network Solutions to Enable and Support Remote Work

Remote work leads to an increased volume of data exchanges between various remote sites. Securing every link in this newly assembled environment of burgeoning interactions between users, personal and business devices is mission-critical for enterprises. Microsoft Azure provides multi-faceted solutions for setting up different types of connectivity scenarios.



Sample Scenario for Provisioning Access to Both Azure and On-Premises Resources



Source

Azure VPN: Get the Workforce Connected

Azure VPN gateway securely links your on-premises networks to Azure, so that your team can have undisrupted access to in-house resources, as well as Azure-based apps. A VPN gateway supports both Point-to-Site (P2S) and Site-to-Site (S2S) VPN connections. Depending on your needs, you can configure different access scenarios and use different authentication methods.

Benefits of Azure VPN gateway:

- Secure, seamless access to on-premises resources.
- Streamlined connection to Azure virtual machines and apps from anywhere.
- Reduced risk exposure to cyber fraud, data leakage.
- Compatible with Windows 10/7, Windows servers, Mac OS, Android, iOS, and Linux.

Best suited for: Regular users

Azure ExpressRoute: More Private Connectivity

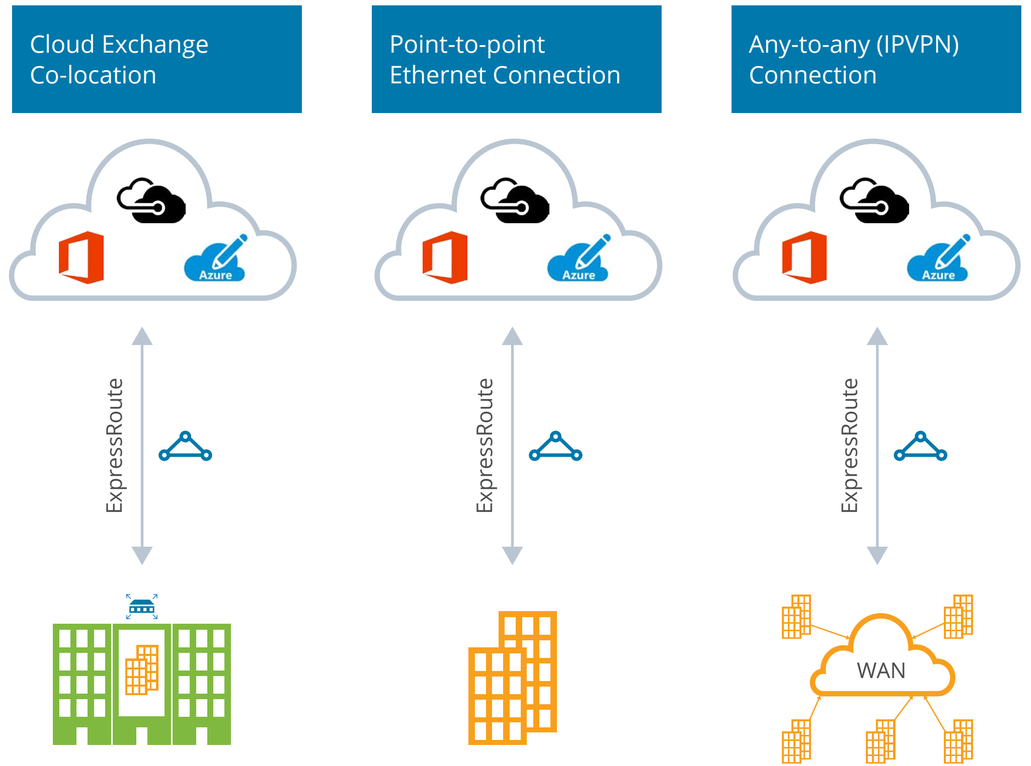
To exchange the most sensitive information, leverage **Azure ExpressRoute –** a private connector to Azure and Office 365. ExpressRoute can be linked directly to your WAN to establish a lower latency, secure connection that does not go over the public Internet.

Benefits of Azure ExpressRoute:

- Build a Layer 3 connectivity between your on-premises network and Azure solutions.
- Ensure uninterrupted, secure connection to Microsoft cloud services from any region.
- Connection uptime guaranteed by SLA.
- In-built redundancy to ensure higher service reliability.

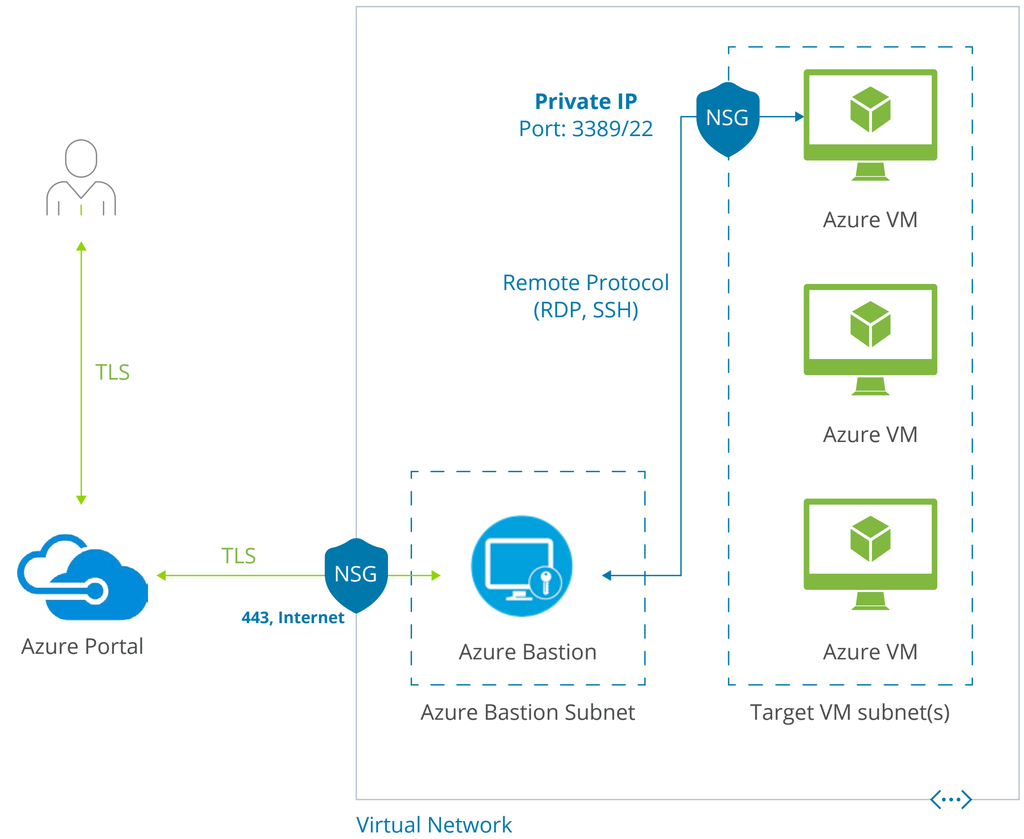
Best suited for: Users with high security privileges/access to sensitive data.

Azure ExpressRoute Connectivity Models



Source

Azure Bastion Deployment Architecture



Source

Azure Bastion: Secure Shell Access

Azure Bastion is a robust alternative to VPN connections that we recommend implementing for secure access (RDP or SSH) to Azure-hosted VMs. Just like ExpressRoute, Bastion enables you to build private connections to your VMs over TLS, meaning that your machines do not need a public IP address and do not get exposed to outside threats.

Benefits of Azure Bastion:

- Platform-managed PaaS service that enables direct access to your VMs from the Azure portal.
- Eliminates the need for any additional ‘connector’ software.
- Robust protection against port scanning and zero-day exploits.
- Unified security due to Bastion’s position on the virtual network perimeter, you no longer need to harden individual VMs within the network.

Best suited for: Enterprises wishing to minimize VMs exposure to the outside world.

Azure Virtual WAN: Enterprise Solution for Global Teams

Azure Virtual WAN is the way to support an array of any-to-any connections between resources stored at different on-prem locations around the globe, e.g., different regional hubs and spoke virtual networks. A comprehensive solution best suited for larger enterprises, Azure Virtual WAN service consolidates a host of networking and security features within a single interface:

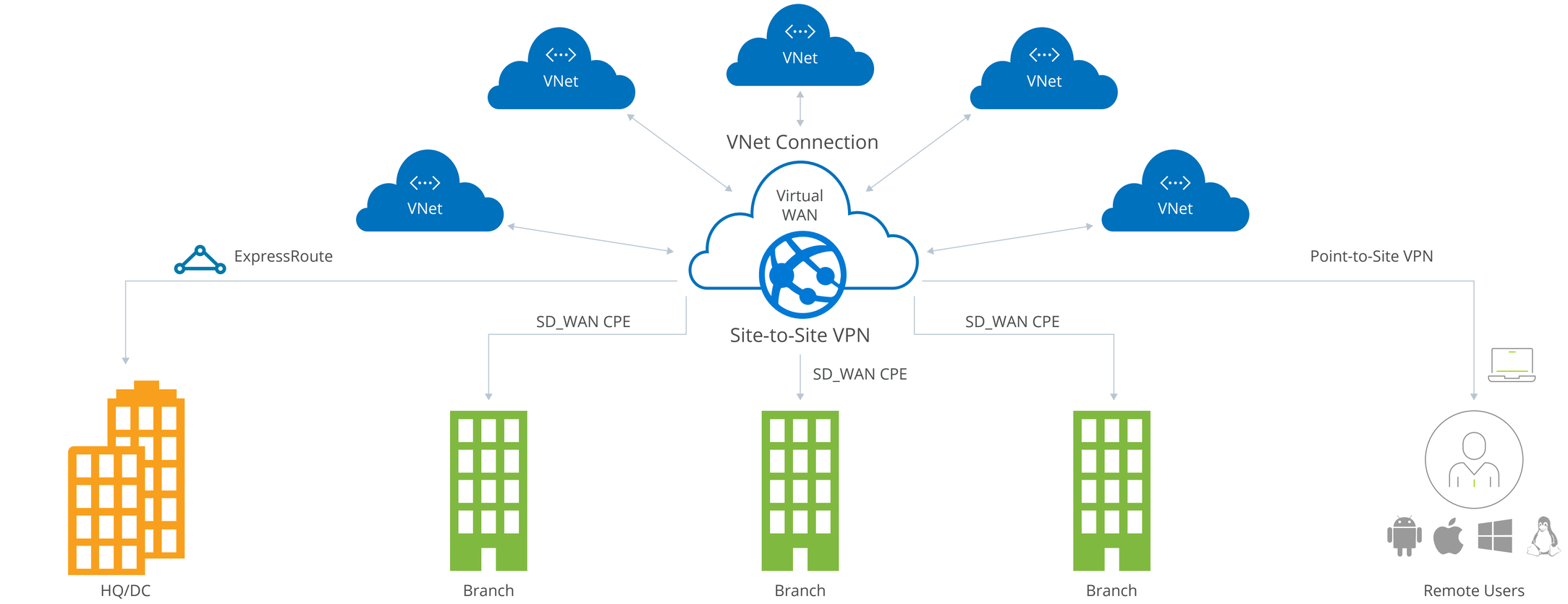
- Branch connectivity.
- Site-to-Site VPN connectivity.
- Remote User VPN (Point-to-Site) connectivity.
- Private (ExpressRoute) connectivity.
- Intra-cloud connectivity.
- VPN ExpressRoute Interconnectivity.
- Routing.
- Azure firewall.
- Encryption for private connectivity.

Benefits of Azure Virtual WAN:

- Automated and integrated Site-to-Site connectivity between on-premises locations and Azure.
- Point-to-Site, scalable VPN connectivity for a large number of remote users.
- Complete view of your network operations and end-to-end flows from Azure portal.
- Faster network setup and configuration thanks to automated Azure workflows.

Best suited for: Enterprises wishing to establish secure branch-to-branch, branch-to-branch cross-region and branch-to-remote users' connectivity.

Azure Bastion Deployment Architecture



Source

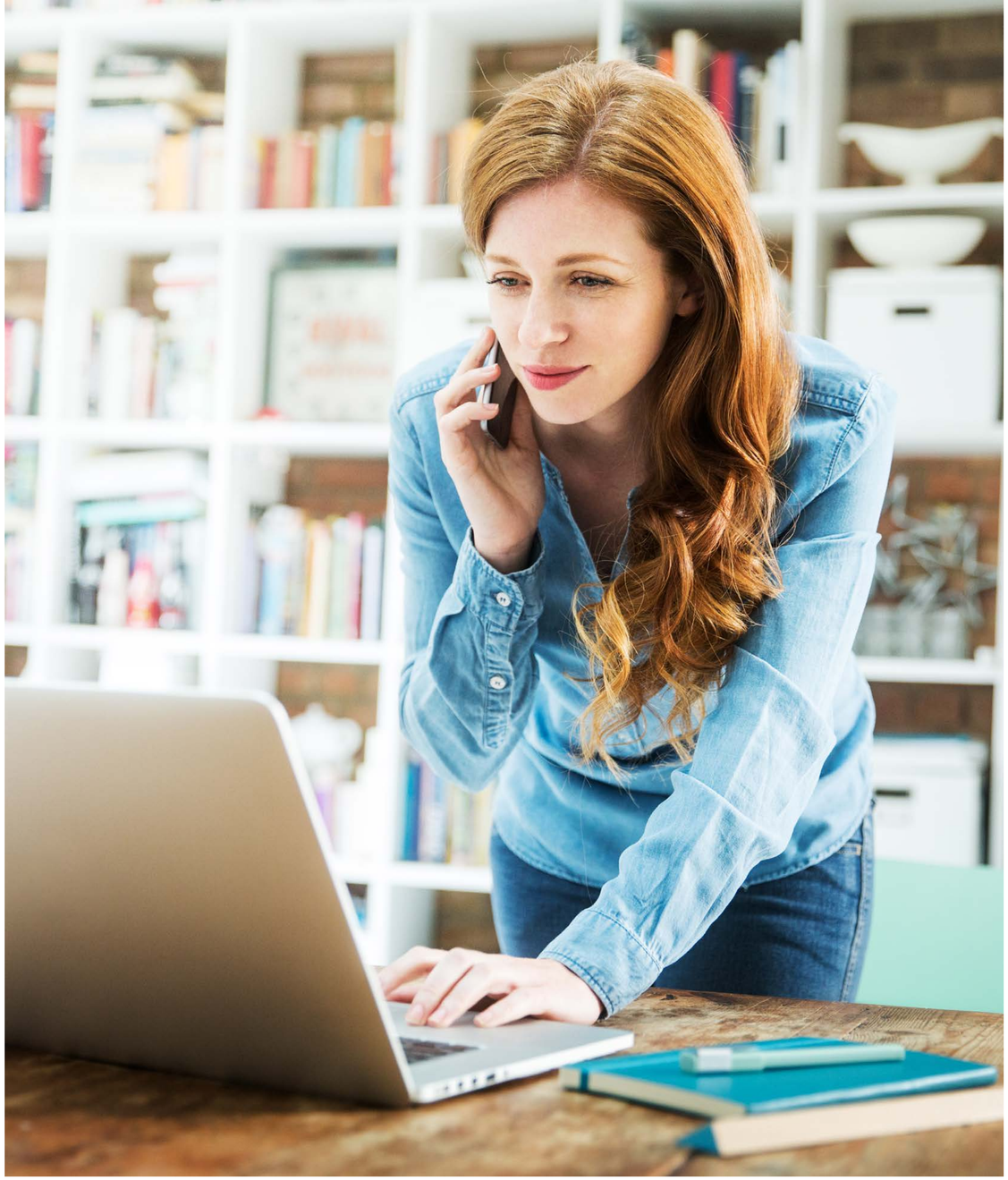
infopulse
Part of TietoEVRY Group

Overview of Different Network Configuration Scenarios on Azure

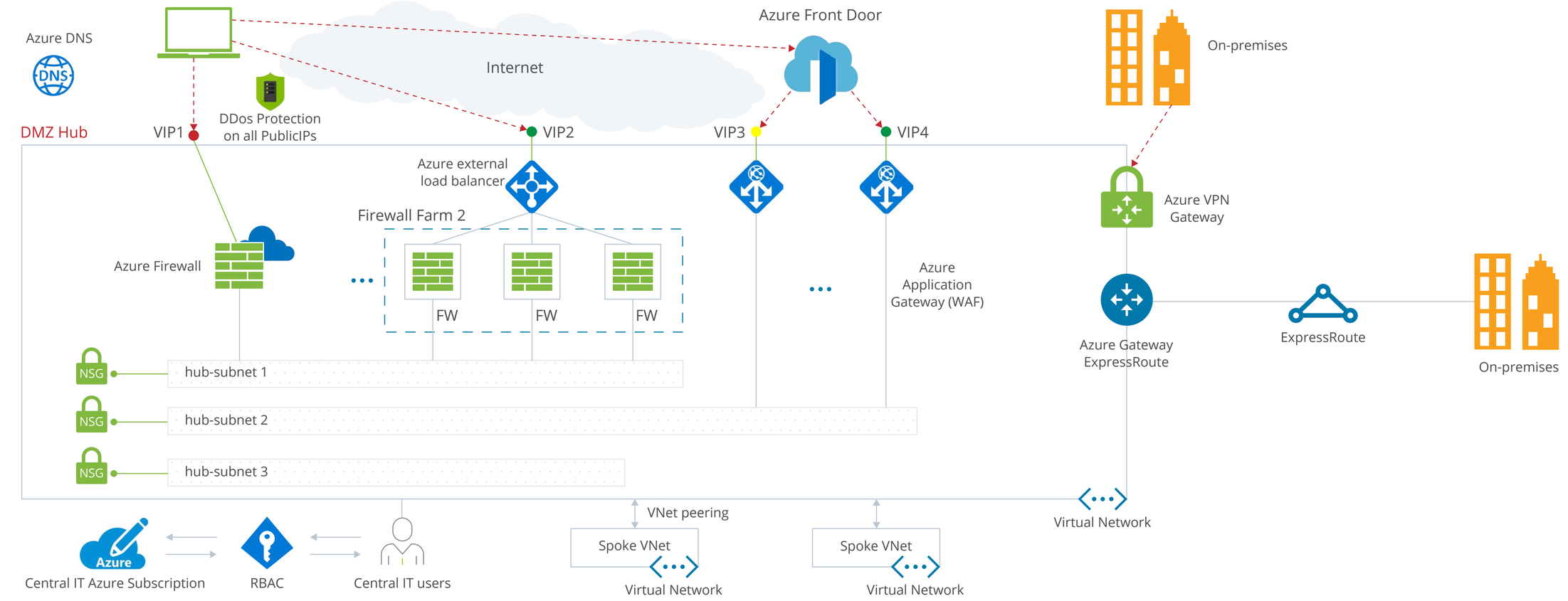
Application Protection Services

You can use the following combination of Azure networking services to secure your operations:

- Private Link.
- DDoS protection.
- Firewall, Network Security Groups.
- Web Application Firewall.
- Virtual Network Endpoints.



Perimeter Network Acrhitecture



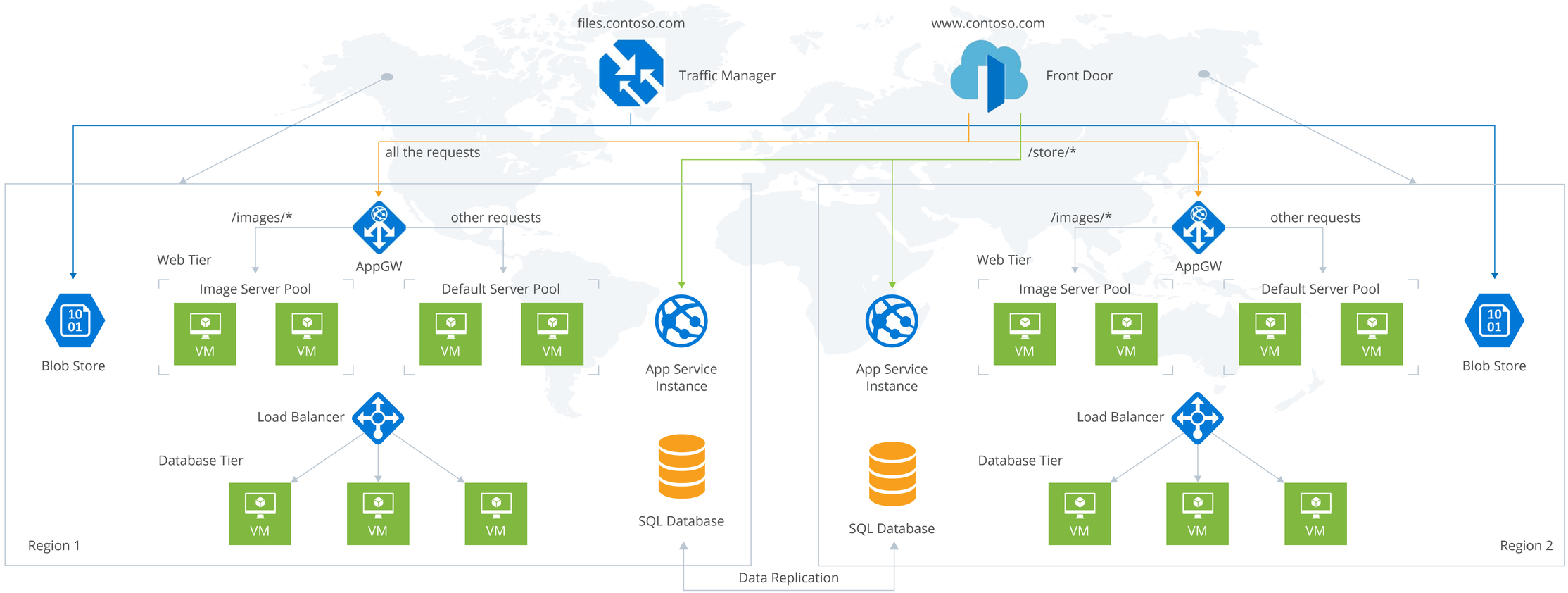
Source

Application Delivery Services

To ensure smooth application delivery in the Azure network, leverage one or a combination of the following networking services:

- Content Delivery Network (CDN).
- Azure Front Door Service.
- Azure Traffic Manager.
- Application Gateway.
- Internet Analyzer.
- Load Balancer.

Sample Network Configuration for a Web Application



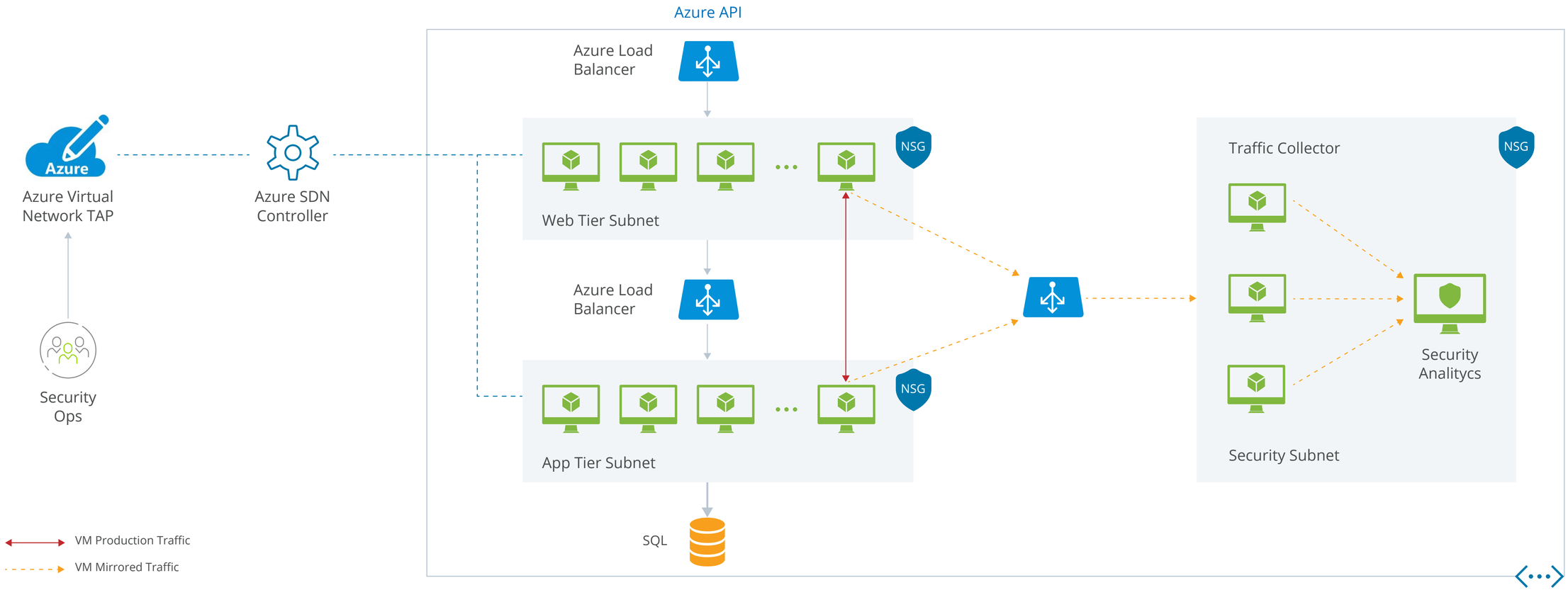
Source

Network Monitoring

To implement comprehensive network resources monitoring, take advantage of the following networking services:

- Network Watcher.
- Azure ExpressRoute Monitor.
- Azure Monitor.
- VNet Terminal Access Point (TAP).

Sample Network Architecture Featuring a Collector Solution for Virtual Network TAP



Source

infopulse
Part of TietoEVRY Group

Azure Load Balancing Services Overview

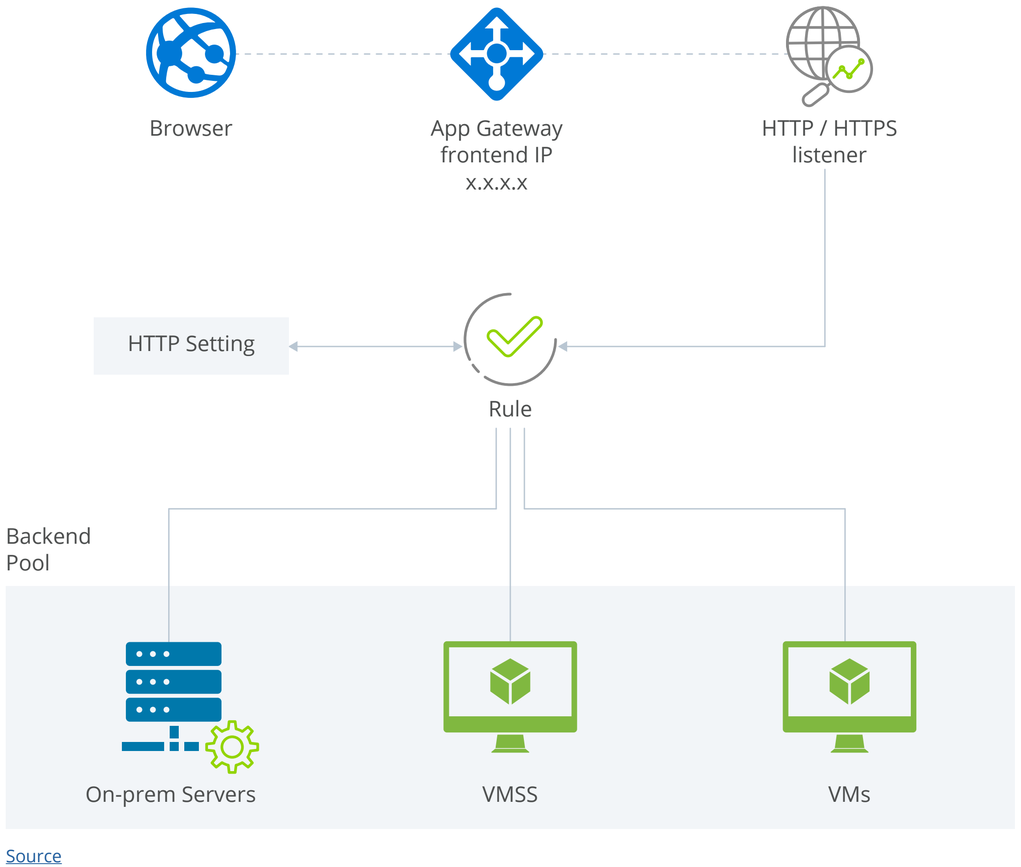
To maintain undisrupted remote operations, you have to attain the optimal distribution of all workloads across multiple resources and networks. The goal of load balancing solutions is to help you achieve equilibrium across all sites. Azure offers several load balancing services, suited for different traffic types, that can help you increase throughput, enhance resource usage, and boost availability.

Azure load balancing services by categories:

Service	Global/regional	Recommended traffic
Azure Front Door	Global	HTTP(S)
Traffic Manager	Global	non-HTTP(S)
Application Gateway	Regional	HTTP(S)
Azure Load Balancer	Regional	non-HTTP(S)

Source

How Azure Application Gateway Works



Source

Azure Application Gateway

Rapidly respond to spikes in usage and effectively balance the incoming traffic to your web and cloud applications to ensure undisrupted access for your teams. **Azure Application Gateway** enables seamless autoscaling to respond to changes in traffic load patterns allowing you to maximize your applications' performance and optimizing your cloud bill at the same time. Web Application Firewall (WAF) comes as a handy add-on of this solution, so that you can set custom security measures and monitoring for all the web applications within your ecosystem.

Benefits of Azure Application Gateway:

- Seamless connectivity with other Azure services – Azure Traffic Manager, Azure VMs, Azure App Service, Azure Monitor, and Azure Security Center.
- End-to-end SSL encryption of all the traffic to bolster cybersecurity.
- Multiple-site hosting – configure more than one website on the same application gateway instance.
- Native support for the WebSocket and HTTP/2 protocols.

Azure Load Balancer

Remote work quadruples the traffic load on your infrastructure and can majorly eschew the load across different sites. **Azure Load Balancer** was designed specifically to enhance regional performance and availability of all your web applications, VMs, and virtual networks, by helping you distribute all the incoming network traffic evenly.

Load Balancer is an excellent zone-redundant solution for all UDP and TCP protocols. What's more, **with Load Balancer you can also add another layer of security to your private networks by using built-in network address translation (NAT)** to control inbound and outbound network traffic.

Benefits of Azure Load Balancer:

- Improve performance of your Azure VMs by balancing the load of internal and external traffic.
- Ensure up-to-date network configuration with native IPv6 protocol support.
- Enhance resources availability by distributing resources across different zones.
- Enable continuous monitoring of your networks' performance and gain access to further suggestions on improvements.
- Collect current and historic insights into the performance and health of your networks.

Azure Traffic Manager

Traffic Manager is the optimal solution for **balancing global DNS-based traffic.** Reroute all the incoming and outgoing traffic across global Azure regions to ensure a higher availability of your applications. Leverage various traffic routing methods and end-point health monitoring services to **set up custom traffic-routing scenarios and automated failover models.** The best part? Traffic manager is immune to failure, including the failure of an entire Azure region.

Benefits of Azure Traffic Monitoring:

- High, undisrupted uptime for critical applications and endpoints.
- Stable performance of cloud and distributed data centers.
- Low network latency for end-users.
- Unbeatable business continuity thanks to the ability of directing traffic to alternative sites during planned maintenance.
- Compatible with hybrid clouds and on-premises deployments.

Azure Front Door

Azure Front Door is a robust application delivery network designed for global load balancing. It comes with **a host of features for defining, managing, and monitoring all applications on your network.** The solution works at Layer 7 (HTTP/HTTPS layer), meaning that you also gain access to the following application capabilities:

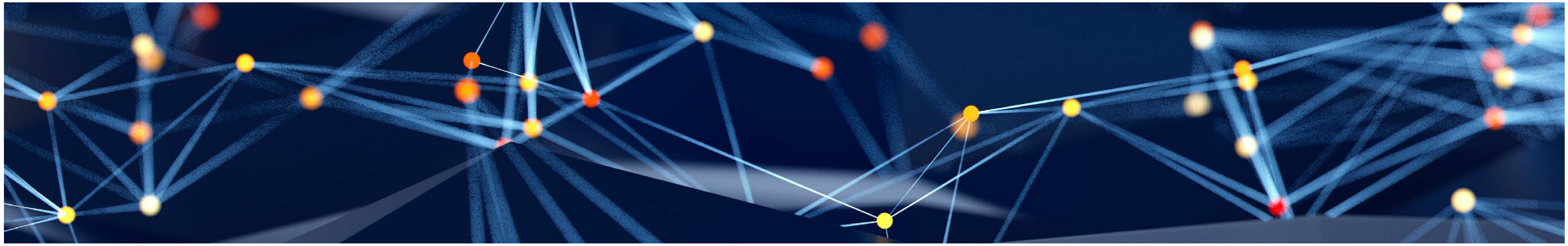
- Path-based routing.
- SSL offload.
- Rapid failover.
- Application caching.

On top of that, Azure Front Door uses Anycast protocol with split TCP and Microsoft's global network for improving global connectivity.

Benefits of Azure Front Door:

- Provide multi-region end-users with fast and effective access to all your applications.
- Leverage smart health probes to monitor your backend for latency.
- Use URL Path Based to direct traffic to backend pools based on URL paths of the request.
- Configure more than one website on the same Front Door configuration to create a more effective topology for all your deployments.
- Create custom Web Application Firewall (WAF) rules for access control to protect your HTTP/HTTPS workloads.

Note: Azure Front Door does not support web sockets.



infopulse
Part of TietoEVRY Group

Azure Security Solutions

Remote work dramatically extends the defense perimeter your CIO needs to set up. The surged volume of data exchanges, frequent remote access, the growing range of cyber-attacks and insider threats place greater pressure on security management. **Azure Sentinel** and **Azure Security Center** can help you set up and scale more advanced security operations time- and cost-efficiently.

Azure Sentinel

Azure Sentinel is a cloud-based security information and event management (SIEM) platform standing at the vanguard of your remote operations cyber defense. Incorporating advanced AI-driven functionality and state-of-the-art monitoring features, Sentinel scans your entire ecosystem of apps, VMs, and databases hosted on Azure for anomalies or signs of security breaches.

Invisible, yet robust Sentinel can identify the tiniest disturbances in your operations, helping your security teams stay ahead of potential threats before they morph into major catastrophes.

How Azure Sentinel Works

Collect

Microsoft Services

Apps, users, infrastructure

Public clouds

Security solutions

Visibility

Dashboard

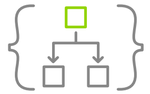
Analize and Detect

Machine Learning

Investigate & Hunt

Pre-defined Queries, Azure Notebook

Automate & Orchestrate Response



Playbooks

Enrichment

Data Ingestion

Data Repository

Data Search

Azure Monitor

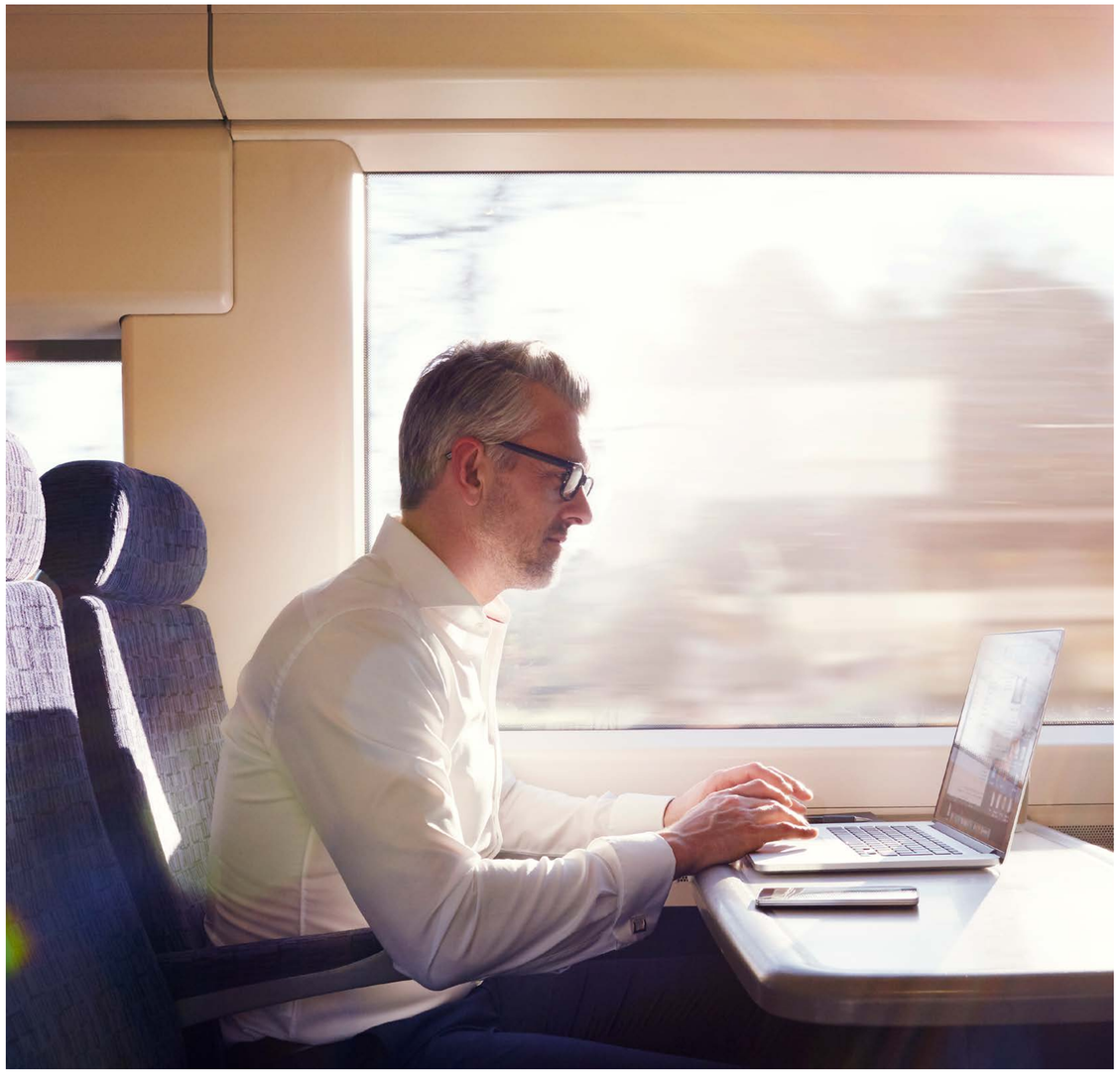
Integrate

ServiceNow

Other tools

Community

Source



Key features:

- Azure-native solution, offering a fast, streamlined, greenfield approach to deploying SIEM.
- Comprehensive monitoring for all Azure offerings as well as imported data from third-party software solutions and other custom data streams.
- Auto-scaling along with your infrastructure to minimize the costs of re-orchestration.
- Built-in AI functionality for threat detection and analytics.

Benefits of Azure Sentinel:

- Automate and orchestrate **up to 80% of security-related tasks.**
- Reduce the rate of false positives and minimize alert fatigue **by up to 90%.**
- Stay protected against emerging, complex threats and multi-vector attacks.
- Pay-as-you-go **pricing starting at $2.46 per gigabyte** of analyzed data.
- Free storage and analysis of Office 365 data.

Azure Security Center

Another native Azure solution, the Security Center monitoring and security management solutions extend through all Azure PaaS offerings, including Service Fabric, SQL databases, and storage accounts without any extra deployments. What's more, Azure Security Center can be configured to enforce security protection across hybrid workloads, running in the cloud and on-premises. The solution adds additional security tools to your chain for hardening your networks and safeguarding service workloads.

Key features:

- Advanced security health monitoring for cloud and on-prem workloads.
- Customizable security policies, aligned with the regulatory and standards compliance.
- Single-pane control over access management and app controls.
- Comprehensive threat detection, powered by analytics and real-time alerts.
- Advanced cloud-defense toolkit for VM-related security.
- Extra protection for the Azure IoT solution and connected devices.
- Embedded integration with other popular security solutions, including Check Point, Tenable, and CyberArk.

Benefits of Azure Security Center:

- Adaptive, automated protection for rapidly changing workloads across complex environments.
- Immediate view into your environment and security statuses of key assets.
- Deep assessment of servers and service workloads with insights for further threat prevention.
- More efficient cross-company security management thanks to auto-provisioning and tight integration with other Azure solutions.

The Main Difference Between Azure Sentinel and Azure Security Center

Azure Security Center's primary role is to protect your servers and service workloads. Azure Sentinel is a more proactive service that analyzes real-time data and scans for attacks. The Security Center has similar features to Sentinel, but they do not overlap.

Learn more about adopting innovative approaches to cybersecurity from our dedicated ebook.

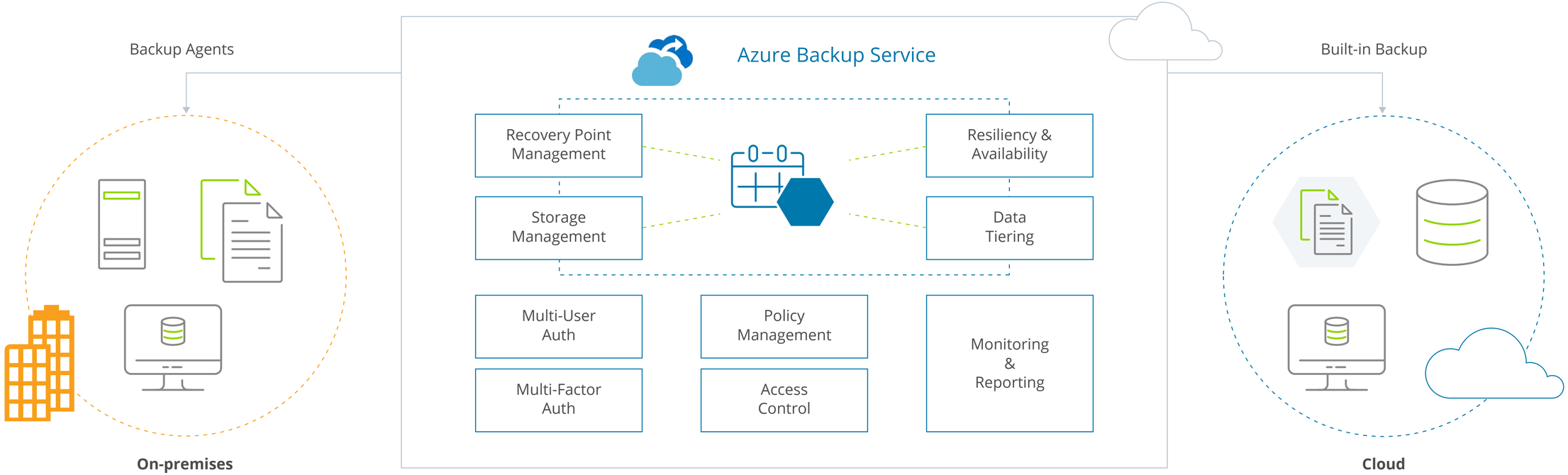
LEARN MORE >

infopulse
Part of TietoEVRY Group

Setting Up Backup and Data Recovery on Microsoft Azure

Automated data sync and streamlined recovery is among the strongest attractors of the cloud technologies. Learn how to configure an automated systems/data backup process and streamline recovery with the help of **Azure Backup** and **Azure Site Recovery.**

Azure Backup



Source

Azure Backup Service simplifies and streamlines data recovery. The service allows you to set up one-click backups of Azure SQL Database, individual files, folders, and entire VMs to the Azure cloud, and exercise precise control through the centralized management panel.

What can be backed up on Azure?

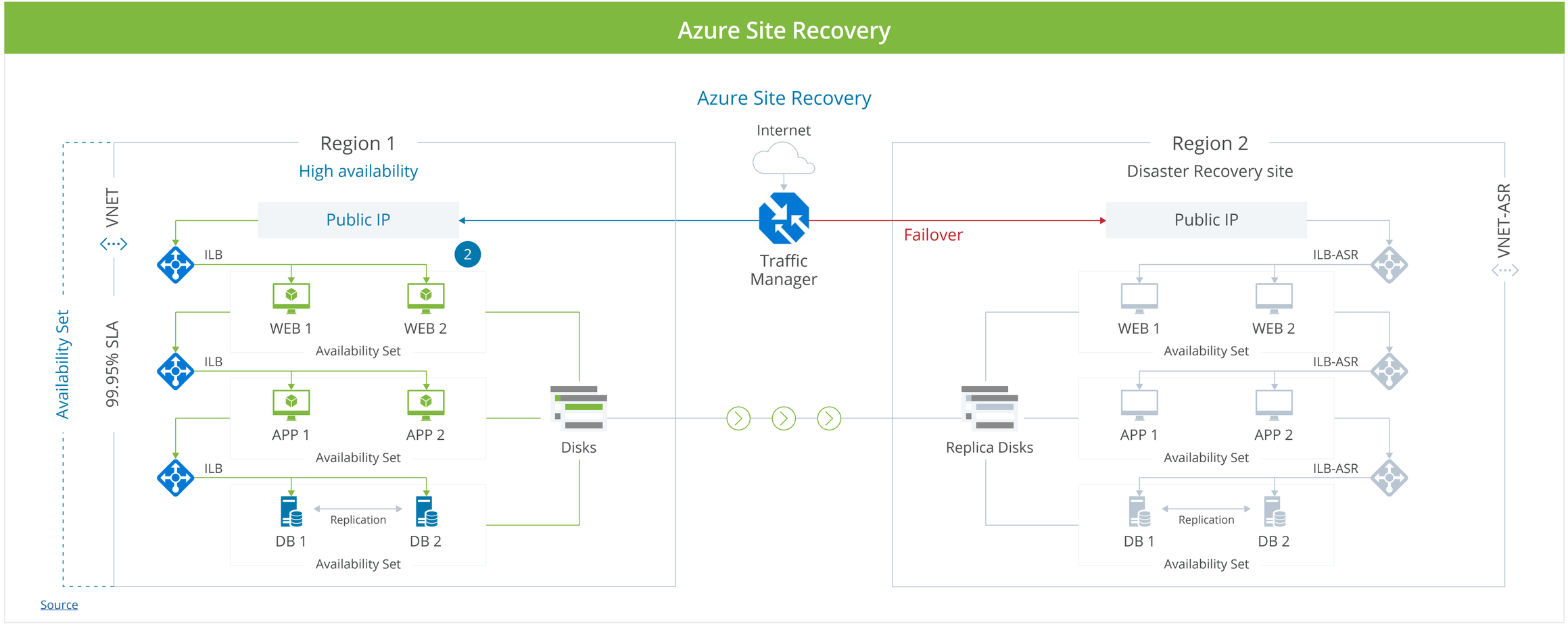
- On-premises files, folders, and system states.
- Entire Azure VMs or individual files, folders.
- SQL databases running on Azure VMs.
- SAP HANA databases hosted on Azure VMs.
- All the corporate Azure Fileshares.

Key benefits:

- **Curb on-premises storage spending.** More backups and archival data to optimize your bill. Create a portfolio of hot, cold, and archival cloud storage to match your current needs.
- **Easy scaling.** Ramp up your backup requirements any time without any hardware, maintenance, or monitoring overheads.
- **Flexible backup storage options.** To ensure high availability, Microsoft Azure provides two types of replication:
  - **Locally redundant storage (LRS)** enables you to create 3 copies of your data in one storage scale unit in a data center. LRS is an affordable option for keeping all data copies within the same region to offset the impact of local hardware failures.
  - **Geo-redundant storage (GRS)** is a recommended replication option that copies your data to the secondary region, meaning that you are also protected against regional outages.
- **Unlimited data transfer.** Azure Backup comes with no limits on inbound/outbound data transfers or extra charges for backing up larger instances.
- **Secure, uninterrupted operations.** Microsoft uses the latest security measures for protecting all data stored on Azure, as well as securing it during transmission. Migrating your backups to the cloud also improves your response time to disaster recovery (DR) events, as most DR plans can be automated. This way your teams will always have undisrupted access to important data, even if their local equipment fails.

In March 2020, Azure also launched Backup Reports in preview. Backup Reports are a new analytical solution that you can use to forecast your backup needs, review backup trends over time, and pull together all the information you need for reporting or audits. The tool collects insights across all your virtual machines, including SQL databases and SAP HANA, and on-premises workloads, using data from Azure Backup Server, Azure Backup Agent, and System Center Data Protection Manager. Gain complete visibility into your current backup properties and drill-down to the smallest details to understand where and how your data is stored.

Azure Site Recovery



Source

Azure Site Recovery is Microsoft's built-in disaster recovery as a service (DRaaS) offering that facilitates the rapid recovery of applications and data across your cloud and on-premises ecosystem. It allows achieving business continuity and mitigating downtime by automating multiple replications, failover, and recovery processes. Also, ASR reduces costly downtime with a near-constant data replication process then ensures instant syncronization cross-site. All the applications and workloads can be automatically recovered from on-premises to Azure or Azure to another Azure region in a matter of minutes.

What can be replicated with Azure Site Recovery?

- Azure VMs from one Azure region to another (multiple regions available across the US and Canada).
- On-premises VMs (VMware and Hyper-V) and physical servers (Windows and Linux) – from on-premises to Azure or from Azure primary to secondary site.
- AWS Windows instances to Microsoft Azure.
- Any workloads on a machine supported for replication.

Key benefits:

- **Improved data resilience.** Site Recovery automatically orchestrates replication without intercepting application data. Furthermore, during a disaster event, Azure VMs are created directly based on the latest replicated data, meaning there are no gaps in sync or missing information.
- **Boost your recovery time objectives (RTOs).** Over the last 3 years, one in ten companies experienced 10 or more outages and 10 or more brownouts[6]. With a replication frequency of 30 seconds for Hyper-V VMs and similar metrics for other hardware, Site Recovery can help you minimize downtime during such events and significantly raise your RTO scores.
- **Precise replication.** Azure solution allows you to set up replication using application-consistent snapshots that contain all the disk data, in-memory data, and all transactions in process. During sudden outages, your end-users won't experience drastic disruptions or irreversible data losses.
- **Embedded testing.** Modify and simulate various DR scenarios without any impact on the ongoing replication.
- **Zero-data loss during expected outages.** By setting up planned failovers you can protect your company from data losses. Even if an unexpected disaster strikes, Site Recovery helps you attain minimal data loss with the help of high-frequency replication.
- **Robust automation.** Azure provides access to a library of production-ready, application-specific scripts for automating common DR scenarios on Azure.

[6] *LogicMonitor: 2019 IT Outage Impact Survey*

infopulse
Part of TietoEVRY Group

DevOps on Microsoft Azure: Fully Integrated Experience

“59% of DevOps companies deploy multiple times per day, every day or once in a few days. That’s up from 45% last year. In other words, DevOps brings truly continuous deployment.”

GitLab DevSecOps Survey 2020

It’s certain: DevOps drives continuous improvements in software development. However, switching gears and breaking away from the tested-and-tried approaches requires more than just strong change management – you need a core technological backbone to support your DevOps operations.

Microsoft Azure Services is a recognized leader in the DevOps space, offering an integrated, cloud-based set of tools, solutions, and technological innovations to support and scale continuous development and integrated security.

With a robust DevOps toolchain for developing, testing, securing, and deploying software, Azure acts as an optimal launchpad for new DevOps operations. Seamless integration with GitHub (and other Gits), packages and containers, automated testing and security tools, adds up to the appeal and relative simplicity of doing DevOps. Being based in the cloud, Azure also removes the geographical constraints of running cross-company or even cross-continent remote DevOps operations at scale.

Azure DevOps Main Tools Overview

Azure Boards: plan, track, and manage tasks using Kanban boards, dashboards, backlog trackers, and custom reporting tools. Azure Boards enable better sprint planning and help ensure that everyone on your remote team stays on the same track.

Azure Pipelines: a set of pre-made and customizable workflows to support your CI/CD. Deploy continuously across platforms, cloud vendors, and languages.

Azure Repos: Securely host your code in cloud-based private Git repos and add custom integrations with other Gits that your teams use.

Azure Test Plans: Incorporate automated testing to your pipeline or add manual test plans whenever needed with end-to-end traceability.

Azure Artifacts: Automate and streamline the usage of your favorite packages (Maven, npm, NuGet, Python, etc.) across all CI/CD pipelines.

Azure DevOps – a Cloud C-Panel to Manage Remote Work

The world's prime technological products are backed by mature DevOps practices. Microsoft Azure offers a strong technological core and all-encompassing collection of tools to place DevOps on remote rails.

- Azure Boards and Pipelines support better remote task planning, tracking, and management.
- Azure Repos and Artifacts boost knowledge sharing and improve collaboration on shared code bases.
- Advanced Analytics functionality lets you set and track custom KPIs and DevOps success metrics cross-company to foster improvements.
- Access Management and Distribution of Roles features ensure that the right people always have the optimal access to the work tools they need.
- Azure cloud storage, on-demand databases, and VMs allow you to scale your deployments en masse within minutes, not days.
- In-built security services and state-of-the-art data encryption safeguards your operations from external intruders.
- All your networks and end-points can be configured for security from a single control point.
- Every virtual network you create is protected by 2FA and additional measures, set up to match your security needs.
- With an array of application and user security mechanisms, your proprietary data remains safe cross-device and cross-location.

Co-located or not, your DevOps people enjoy the same level of security, access rights, and knowledge sharing.

"Through this process, DevOps people learn to become experts at collaboration and flexibility."

Hina Popal, senior agile practitioner and Scrum Master at Red Hat.

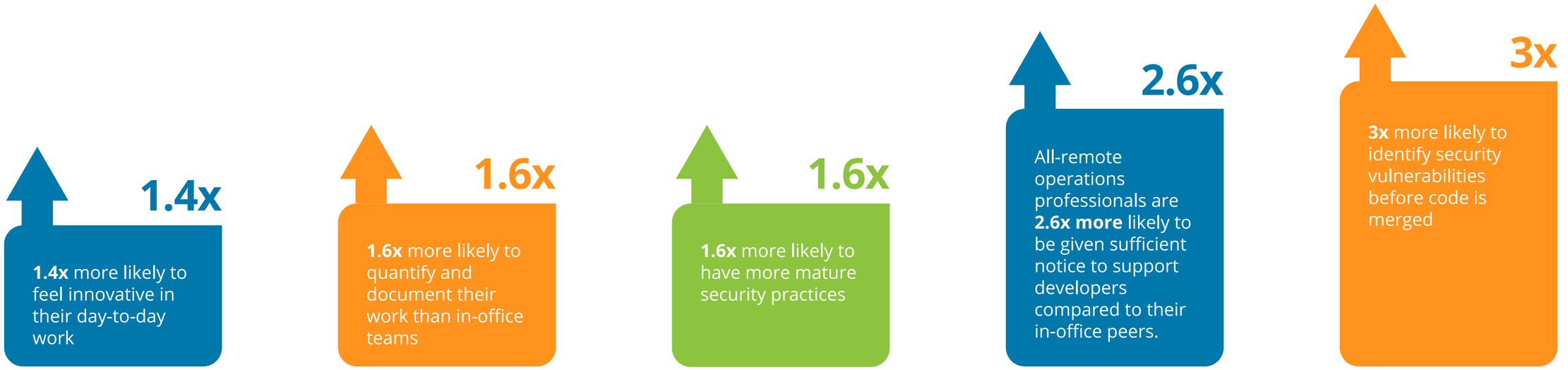
An effective DevOps culture rests on three pillars – collaboration, efficiency, and visibility. Achieving high rankings in these three categories isn't always possible within co-located teams. Impromptu Slack chats, frequent face-to-face meetings, and micromanagement can hinder your teams' ability to take ownership and communicate effectively with one another within the same room or cross-border.

"Teams with a well-developed DevOps model are 58% more likely to have good insight into what colleagues on other teams are working on."

GitLab DevOps Survey 2019

DevOps culture prompts to break away from the rigid, ineffective workflows and routines and adopt a more streamlined, agile, and targeted approach to software development. Once the framework is properly set up and adopted by the core majority, the results of DevOps are not long in coming:

Mature Remote DevOps Teams are:



Source

Learn more about how Infopulse can help you build a strong remote DevOps culture at our dedicated DevOps portal.

LEARN MORE >

infopulse
Part of TietoEVRY Group

Connecting the Dots on Your Microsoft Cloud Journey

With uncertainty lying ahead, one may assume that playing the “wait and see” game when it comes to technology investments may be the preferred option.

However, it is now certain that remote work is here to stay for the long-term. Recognizing the need to adapt and secure your operations for the long-term is a strategic imperative for businesses cross-domain. Microsoft has long been a leader in delivering office management solutions and recently has become the top cloud computing choice of global Fortune 500 companies[7].

Foraying into the ever-expanding universe of Microsoft products today translates into a competitive advantage in the short-term perspective. Companies investing in Azure IaaS solutions will have a payback in less than 3 months with a positive ROI of up to 478%[8].

Whether you prefer to start with transforming your front-end or right-sizing your backend operations and supporting infrastructure to reinforce and scale your current processes, Infopulse is here to advise you further on your journey.

CONTACT US >

[7] *CNBC: Microsoft Azure has an edge over Amazon Web Services at big companies, Goldman Sachs survey says*
[8] *The Total Economic Impact™ Of Microsoft Azure IaaS*

infopulse
Part of TietoEVRY Group

Contact us:

Ivan Musiienko
Head of Cloud Managed Services and Solutions

+380 44 585 25 00

i.musiienko@infopulse.com

UA: +380 44 585 25 00

DE: +49 3222 109 52 35

UK: +44 8455 280 080

USA: +1 888 339 75 56

info@infopulse.com

Follow us:

www.infopulse.com

About Infopulse

Infopulse, part of the leading Nordic digital services company TietoEVRY, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,000 professionals and is represented in 7 countries across Europe and North America. Infopulse is a Global Outsourcing 100® company recognized by IAOP®.