

Secure Intelligent Workplace

Secqur Assessments

Zero Trust Security Accelerators

Secqur Æther – Managed Security

Collaboration fuels innovation. Cloud services are continuously improving the tools that will define the future of work. By joining Infused Innovations' community of managed service customers, we will work together to build secure modern workflows for your organization.

- Dan Chemistruck, CISO



Infused Innovations
1130 Ten Rod Rd., Suite F-204
North Kingstown, RI 02852
401-267-4460

Secqur Assessments



Shadow IT Assessment

- Discover unsanctioned third-party SaaS platforms
- Review document sharing outside of your organization
- Review access attempts from foreign countries
- Review OAUTH approved applications



Microsoft 365 Cybersecurity Assessment

- Review Microsoft 365 Tenant
- Identify unconfigured & owned security tools
- Identify legacy protocols in use
- Identify regulatory control gaps
- Create a cybersecurity roadmap



Rapid Windows Cyberattack Assessment

- Two-day assessment of Windows infrastructure
- Identify legacy protocols, i.e., SMB1, NTLMv1
- Check for malware resistant backups
- Identify missing critical updates



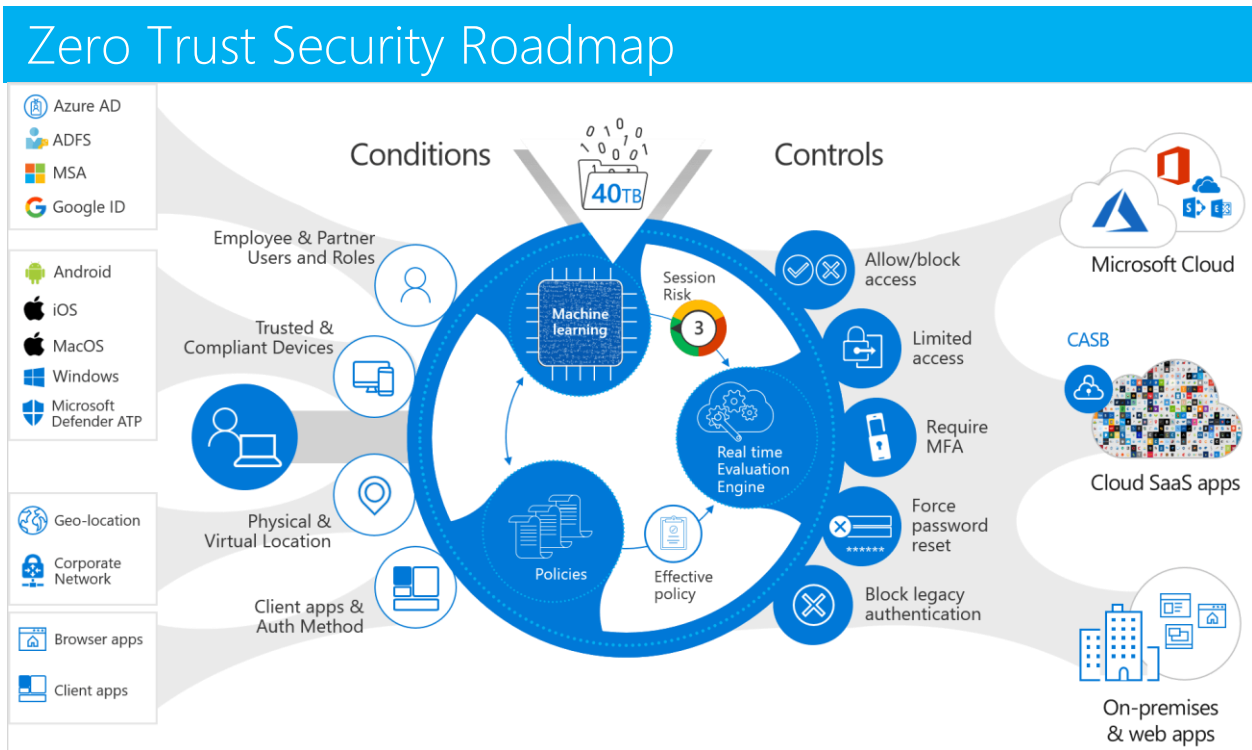
Azure Assessment

- Infrastructure diagrams & documentation
- Right-size VM recommendations
- Cybersecurity recommendations
- RBAC guidance



Vulnerability Scanning

- Scan against common frameworks such as PCI, HIPAA, NIST 800-171, NIST 800-53, ISO27001
- Credentialed CVE scanning
- Scan registry for exploits
- Identify misconfigurations



**Phase 1
Modern Authentication**

- Conditional Access & MFA
- Self Service Password Reset
- Banned Password List
- Company Branding
- Office 365 ATP
- Seamless SSO



**Phase 2
Data & Device Protection**

- Azure Information Protection
- OneDrive Folder Protection
- Intune for Mobile
- Intune for Windows 10
- Office 365 DLP








**Phase 3
Threat Protection**

- Azure ATP
- Advanced Threat Analytics
- Microsoft Cloud App Security
- Microsoft Defender ATP
- Office 365 Threat Intelligence
- Sentinel & Security Center

After implementing your zero trust security perimeter, keep it up to date with Secur Æther—a managed security orchestration, automation, and response service.



Secur Æther

Train 	<ul style="list-style-type: none"> Web-based end-user training Phishing simulator Brute force simulation Password spray simulation
Protect 	<ul style="list-style-type: none"> Windows & Third-Party Patching OneDrive Known Folder Protection for Desktops BitLocker management in the cloud Vulnerability Hardening with Windows Defender Virtualization
Detect 	<ul style="list-style-type: none"> Microsoft Defender ATP Advanced Threat Analytics / Azure ATP Office 365 ATP Log Analytics Collection
Respond 	<ul style="list-style-type: none"> Microsoft Defender ATP Automated Response Azure AD Identity Protection Office 365 Detonation Chambers Threat Investigation
Report 	<ul style="list-style-type: none"> Azure Security Center Threat Intelligence Power BI Dashboards in Teams Compliance Controls Secure Score



Experience a managed holistic identity-based security platform that integrates beyond your network perimeter to allow your employees to work safely from anywhere on any device.

Maintain security hygiene on all your Windows, MacOS, iOS, and Android devices. Stop zero-day attacks from spreading with automated endpoint detection and response. Stay up to date to protect against new MITRE ATT&CKs with quarterly security briefing sessions.

Zero Trust Identity-Based Access Perimeter

- Monitor suspicious activity of SaaS applications accessed from anywhere in the world
- Continuously confirm device compliance and user identity before allowing access
- Block anomalous behavior

Manage Devices Globally From the Cloud

- Push updates to devices located anywhere in the world
- Continuous device health attestation
- Sandbox corporate information and prevent data loss
- Granular compliance reporting

Automated Breach Response

- The Microsoft Intelligent Security Graph responds to 6.5 Trillion signals daily
- Automatically quarantine and isolate suspicious behavior
- Use the speed of AI to automatically respond to alerts

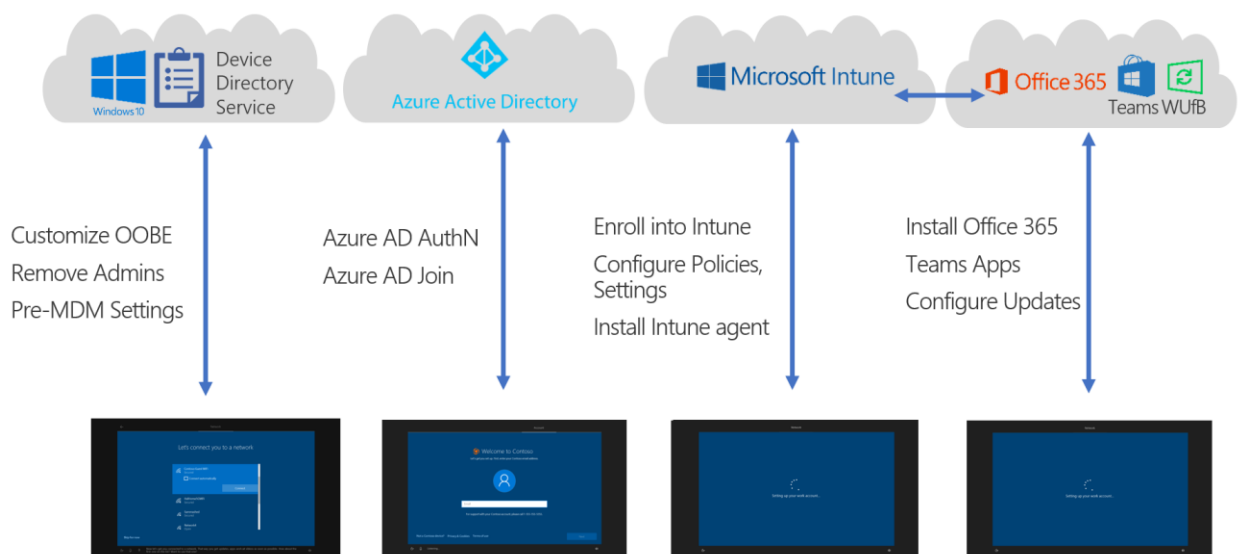


Our Vision for a Secure Intelligent Workplace

In a mobile-first, cloud-first world, users can access your organization's resources from anywhere using a variety of devices and apps. **Secure Intelligent Workplace** provides control, enabling your organization to create an identity-based perimeter to protect your sensitive data by leveraging the Microsoft 365 security stack.

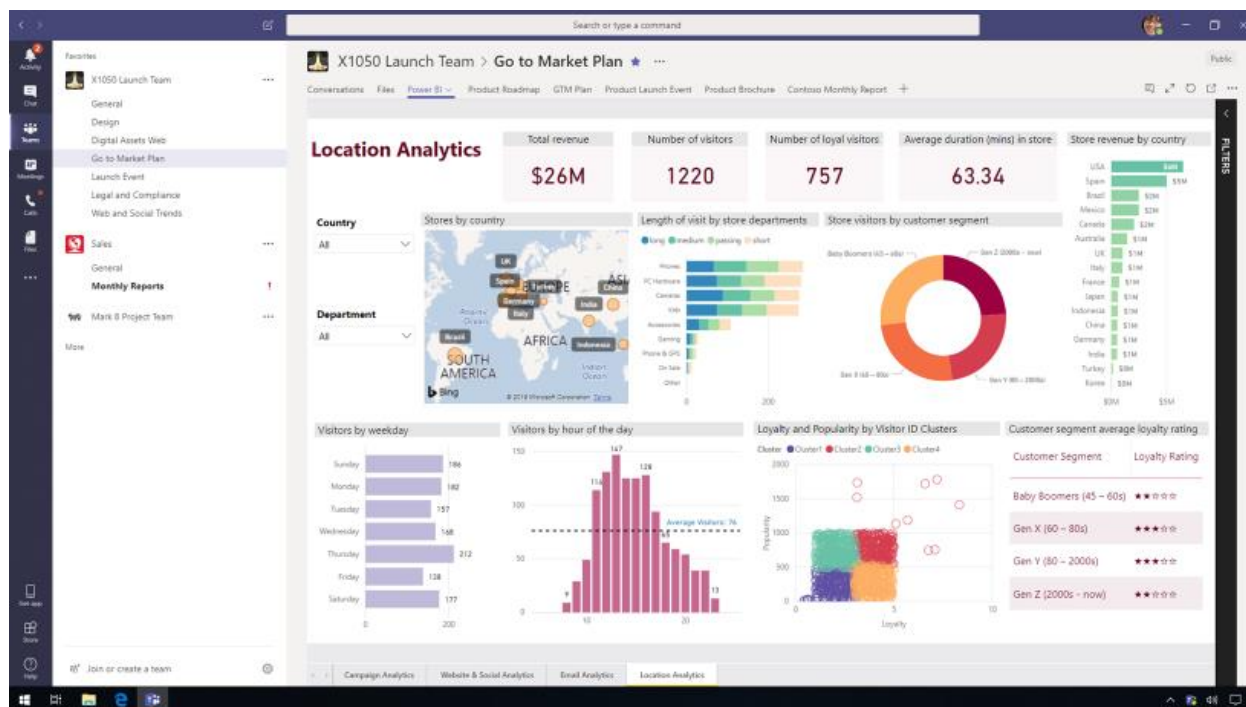
Ensure a consistent user experience that can be automatically deployed in less than an hour. User's files will travel with them across Windows, MacOS, Android, iOS, and VDI sessions. This same technology also maintains 1,000 versions of your documents, which enables a swift recovery from ransomware attacks. In most cases, AutoPilot with OneDrive folder protection can *restore a PC in under an hour*.

Using AI and machine learning models, telemetry is gathered from all devices and user actions to rapidly detect and respond to security breaches. Infused Innovations provides Secqur Æther as a managed service to keep your environment up to date, and your data secure.



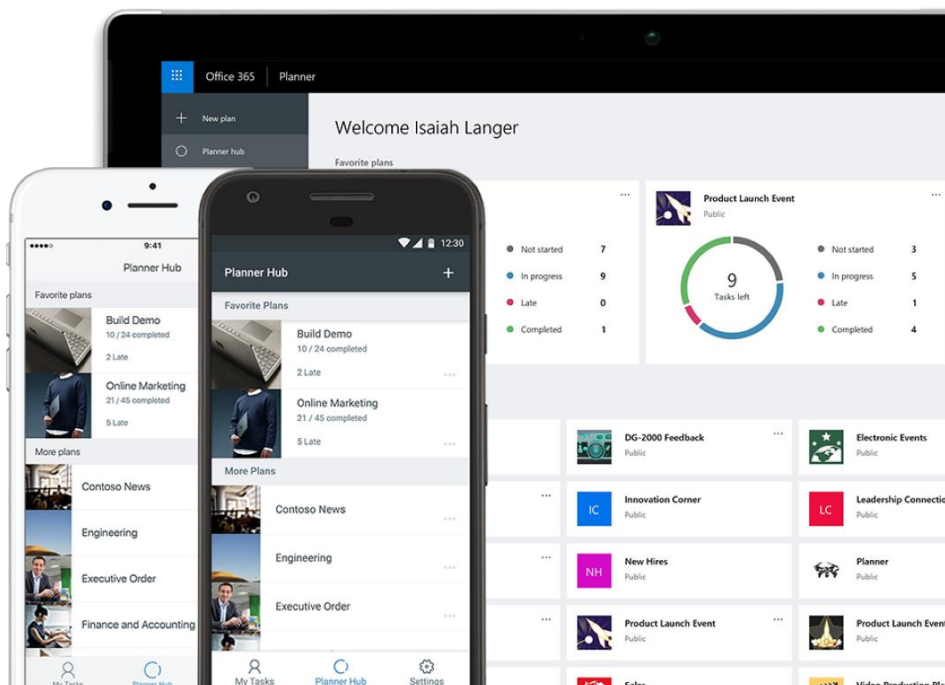
Microsoft Teams – A Digital Hub for Teamwork

Microsoft Teams is a rich collaboration platform that is included with your Office 365 subscription. Secure Intelligent Workplace uses Teams as a digital hub to aggregate data from multiple sources.

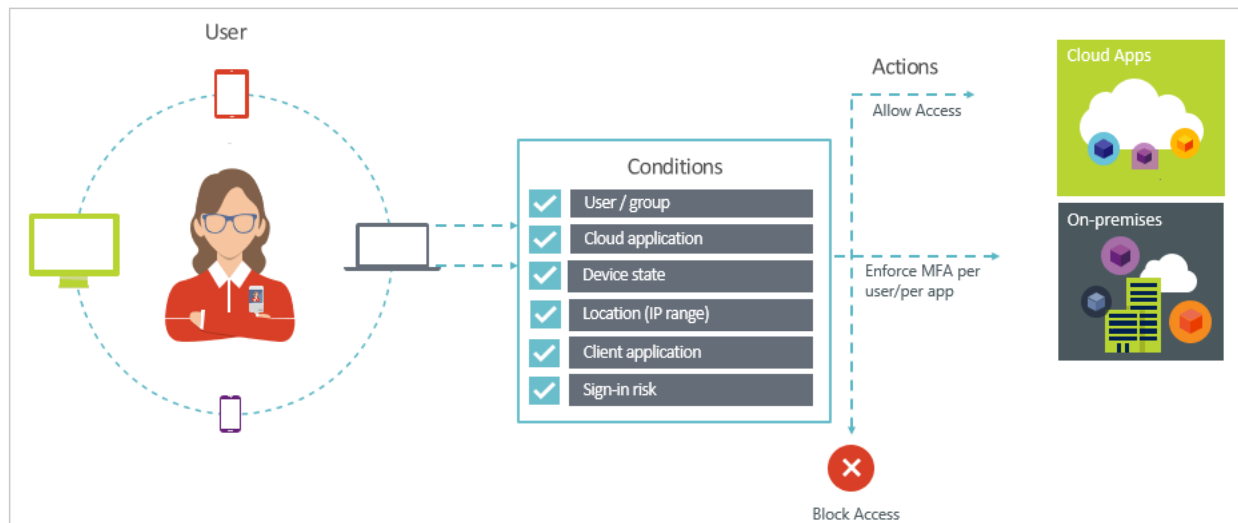


Some of the features that can be delivered with Microsoft Teams include:

- Conference Meetings
- PSTN Voice Calling
- Persistent team and individual chat
- Planner for task management
- Dedicated Team OneNote
- Collaboration from any device



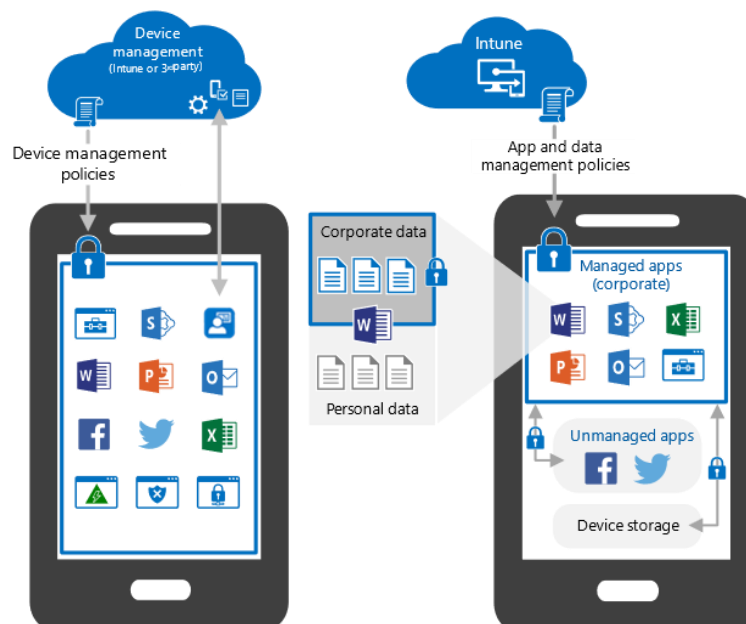
Zero Trust Security with an Identity-Based Perimeter



The traditional network perimeter is dead. Just because a device is on your network, doesn't mean it should automatically have access to your data. Use conditional access to create an identity-based perimeter around your organization's information. Require a device to be corporate owned, compliant, or under a specified risk profile before granting access. Otherwise, issue a multifactor authentication challenge, force a password reset, or block the user/device.

Mobile Device and Application Management

The modern workplace allows employees flexibility in their schedules with the ability to stay productive from anywhere. By leveraging conditional access, your employees can use personal devices while sandboxing access to the organization's data, isolating files from the rest of the device. This allows you to ensure your data is encrypted, password protected, and secure at all times.



Data Classification and Protection



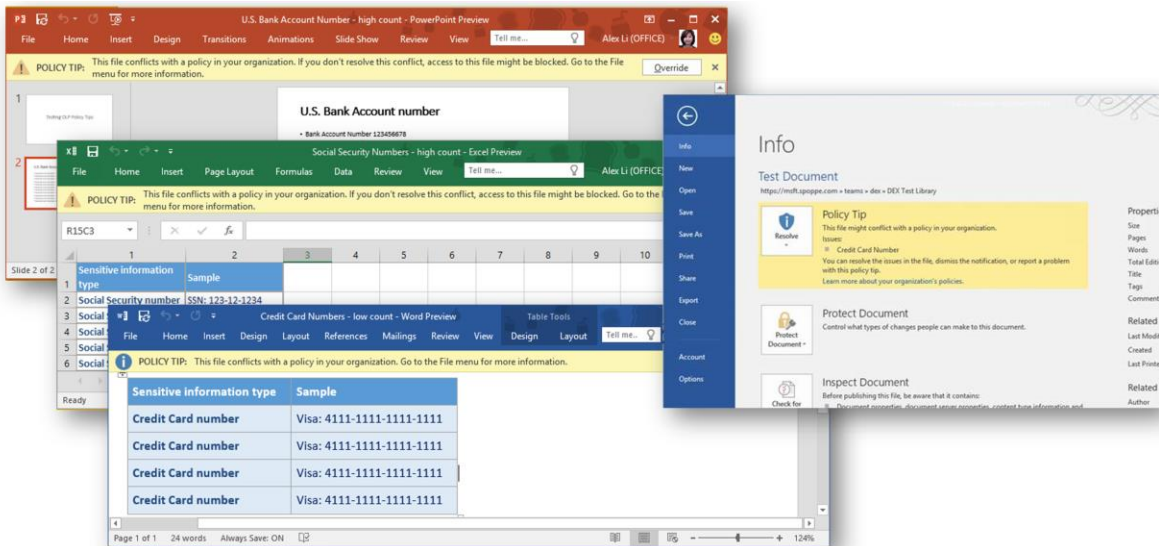
Classification

Protect

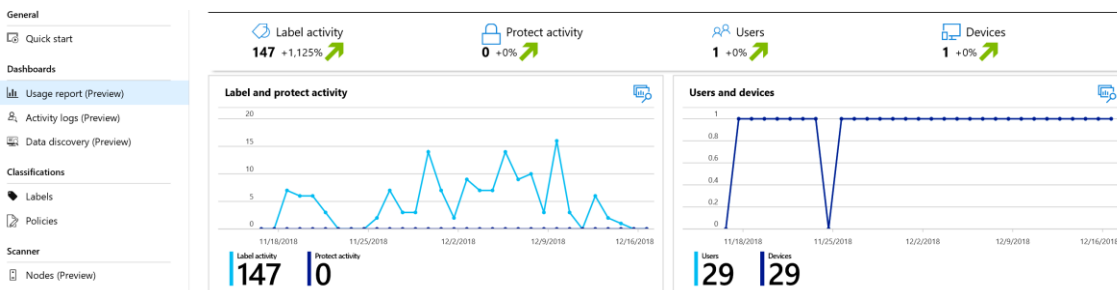
Monitor

To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Microsoft 365 comes with over 80 DLP templates for identifying common sensitive information types from around the world.

The new unified labeling experience allows you to create a single set of rules to classify and encrypt data across the entire Microsoft ecosystem, from any device. These labels can be used to train your users with policy tips if a document contains sensitive data:



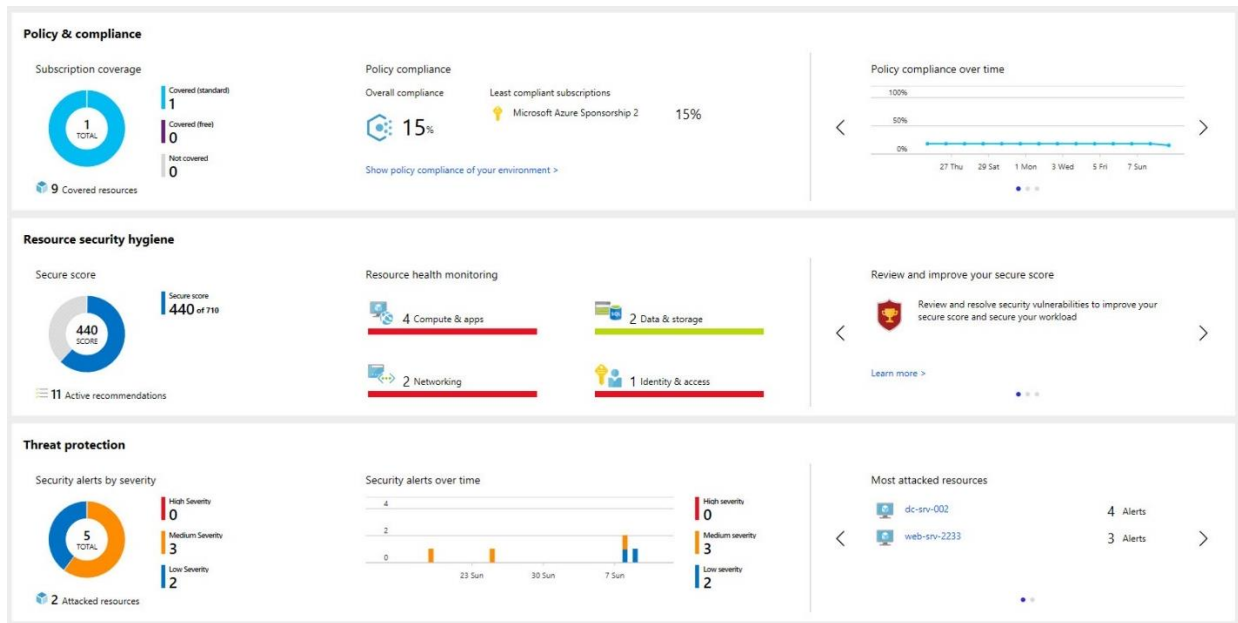
Built-in reporting on label usage allows you to monitor, track, and revoke access to documents even after the document has left the borders of your organization.



Vulnerability Management & Cloud App Security

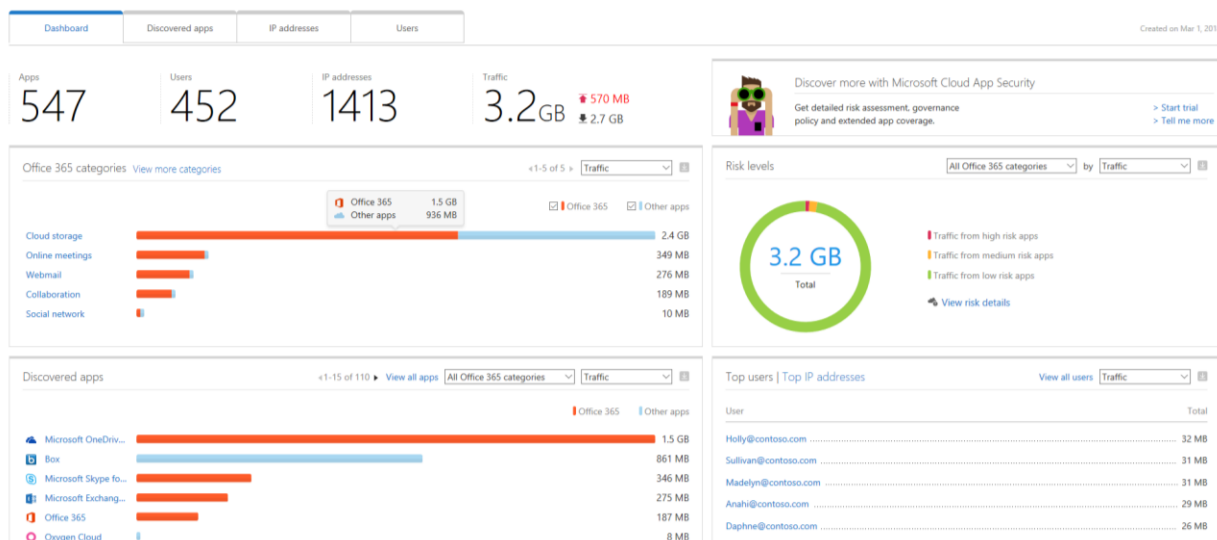
CVE & Compliance Scanning

Do you know where you are most likely to be hacked? Scanning for known vulnerabilities and misconfigurations gives you visibility into the areas of your environment that require immediate remediation. Infused Innovations uses compliance management tools to scan against common frameworks including NIST CSF / 800-171 / 800-53, ISO27001, PCI-DSS, CIS, GDPR.



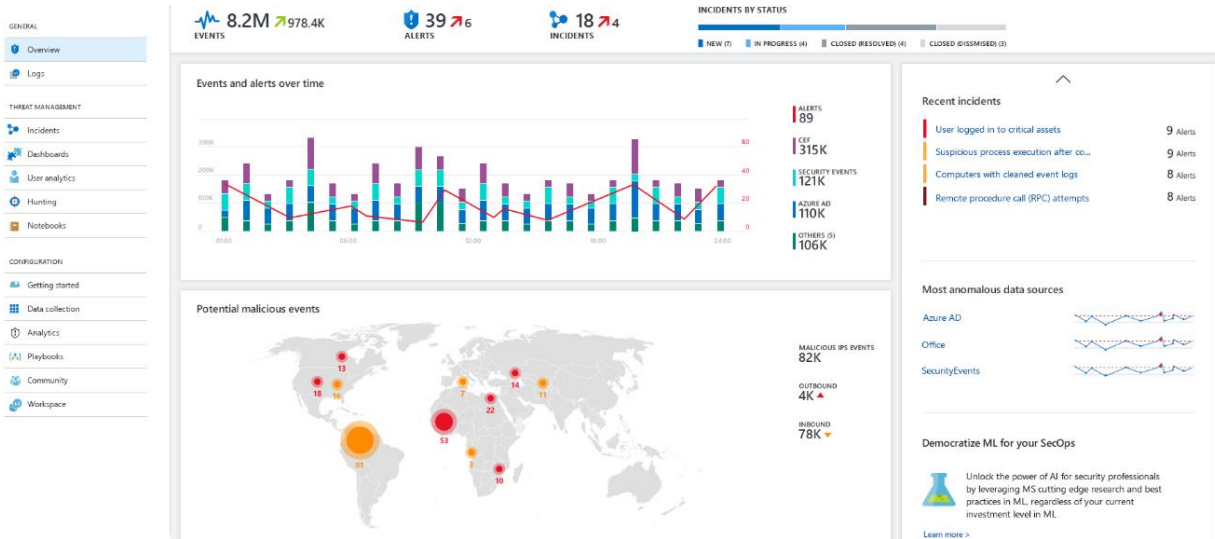
Cloud App Security Broker

Once your data is in the cloud, how do you track who it is shared with and how do you limit access from personal devices, vendors, or competitors? Microsoft Cloud App Security provides full visibility and policy management for data stored in OneDrive, SharePoint, and Teams. Native integration with Windows 10 also provides insight into “Shadow IT” usage with unsanctioned third-party vendors.

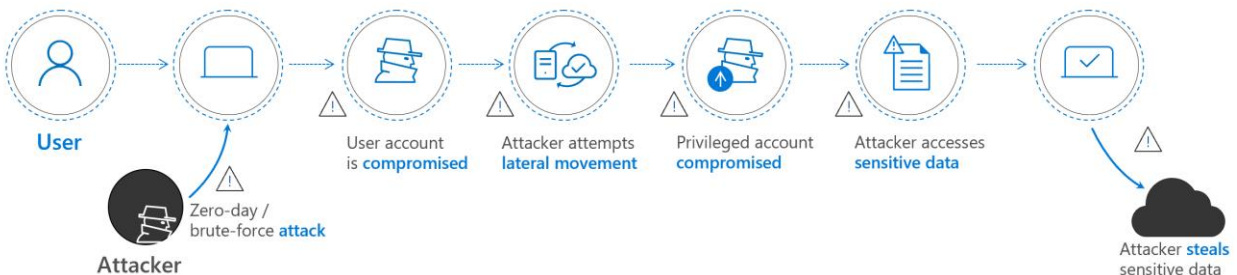


Security Information Event Management (SIEM)

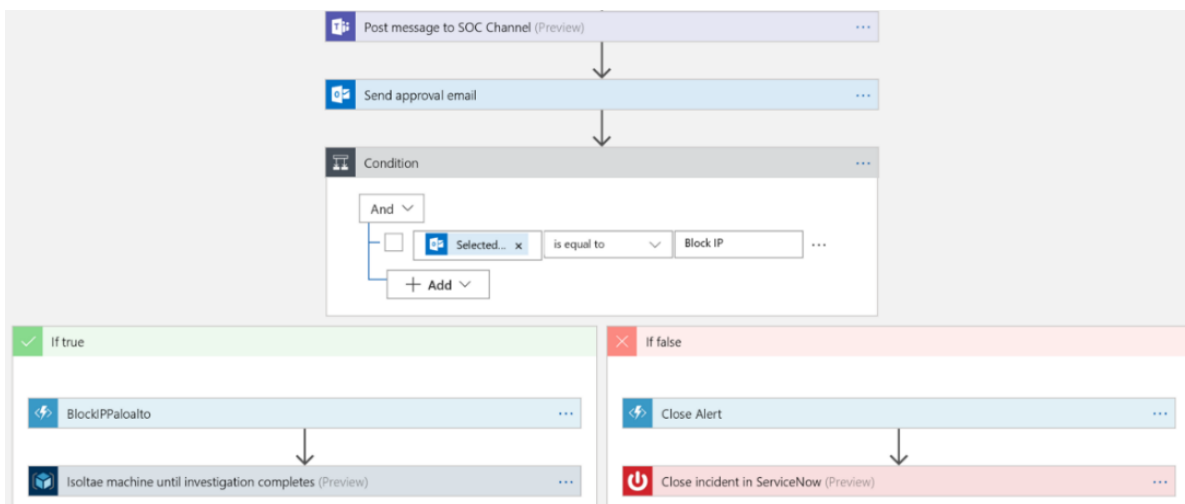
How long does it currently take you to identify that you've been breached? Can you tell exactly what data or systems have been compromised? Most organizations take 80+ days to detect a breach and digital forensics expenses can start at \$25,000 for the smallest breaches.



Infused Innovations recommends deploying a cloud-native SIEM solution for most organizations. SIEM allows you to collect syslogs and telemetry from your entire environment, then uses AI and machine learning to correlate anomalous signals to visualize the entire attack-chain of a breach.



Using the data collected from your SIEM tool, Infused Innovations offers security orchestration services via our **Secur Ether** platform to automate responses at the speed of the attacker.



Project Methodology

Projects can often be differentiators of one business from its competition. Infused Innovations uses the following steps and principals to modernize and secure your IT infrastructure.



1
Plan



2
Design



3
Build



4
Pilot



5
Operationalize



INCREASE PRODUCTIVITY

Microsoft 365 allows you to control when users are prompted for MFA, when access is blocked, or when they are required to use a trusted device. This keeps users more productive than a policy requiring MFA every single time.



MANAGE RISK

Enabling Microsoft 365 policies can provide you with cloud-scale identity protection, risk-based access control capabilities, and native multi-factor authentication support.



ADDRESS COMPLIANCE AND GOVERNANCE

Auditing access requests and approvals for the application, as well as understanding overall application usage becomes easier with Azure Active Directory, which supports native audit logs for every application access request performed. Auditing includes requester identity, requested date, business justification, approval status, and approver identity. This data is also available from an API, which will enable importation of this data into a Security Incident and Event Monitoring (SIEM) system of choice, such as Azure Sentinel.



MANAGE COST

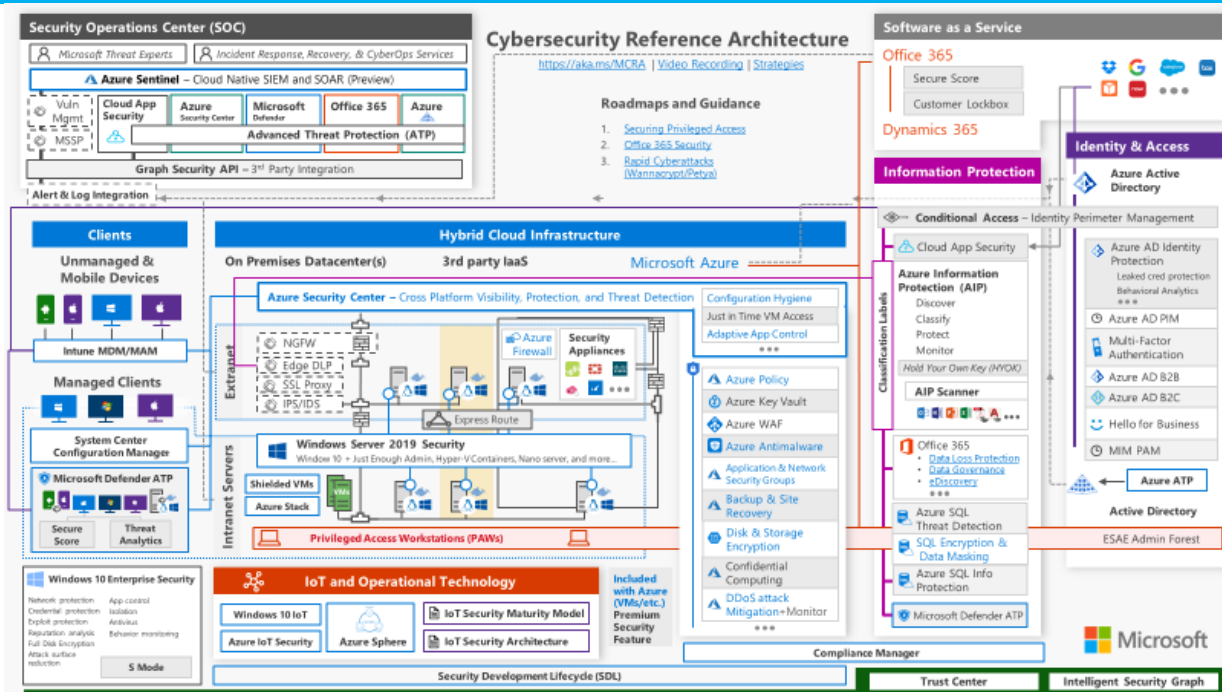
Moving access policies to Microsoft 365 allows you to standardize on a single integrated security stack that allows you to reduce the reliance on custom or on-premises solutions such as ADFS for CA, Okta for SSO, Duo for MFA, or Cylance for APT detection.



ADOPTION AND SUCCESS

Minimizing business interruption and providing clear communication are the keys to a successful project. We provide a series of workshops and pilot programs to gather feedback from your organization's stakeholders to ensure we're delivering the solution that your business wants and needs.

Zero Trust Security Accelerators



Network perimeters no longer exist in the modern workplace. Zero Trust Security Accelerators focus on protecting the three key aspects of your organization from anywhere that your users work: identity, data, and devices.

ZTS Accelerator for Modern Authentication

Passwords are obsolete. Work towards a password-less environment by integrating third-party services with Azure SSO and enabling biometric authentication on known devices. Don't wait for your users to change their password every 90 days—force a password reset as soon as a breach is detected.

Infused Innovations will perform the following tasks as part of this accelerator:

- Identity & Access Management
 - Deploy or validate Azure AD Connect for a single Active Directory Domain
 - Enable modern authentication for a single Office 365 tenant
 - License and provision users in a single Office 365 tenant
 - Configure AAD P1 and EM+S licensed users for Self Service Password Reset
 - Configure sync of all supported modern workstations in a single AD Domain
 - Enable seamless SSO via Group Policy or Intune
 - Create a custom banned password list
 - Configure Company Branding
 - Create Azure AD groups to use for targeting policy configurations
 - Create a Cybersecurity Microsoft Teams site for dynamic Power BI reports
- Conditional Access and MFA
 - Provide a one-hour workshop to review suggested baseline configurations
 - Enforce MFA for current global admins

- Configure automated risk-based policies for Azure AD P2 users
 - Create a break glass policy
 - Provide a two-week pilot
- Office 365 ATP
 - Configure Anti-Phishing Policies
 - Configure Anti-Spoofing Policies
 - Configure Safe Links baseline
 - Configure Safe Attachments baseline
 - Configure Malware detection baseline
- Configure DKIM records
- Configure DMARC records with Valimail for DMARC monitoring

ZTS Accelerator for Data & Device Protection

Protect against ransomware and accidental data leakage with modern device management. Use Cloud App Security to monitor data access and sharing across your organization and automatically block access for unapproved scenarios.

Infused Innovations will perform the following tasks as part of this accelerator:

- Mobile Device Management
 - Provide a two-hour workshop to review baseline MDM/MAM configurations in Intune
 - Create a baseline MDM Device Compliance Policy to include device encryption, data containerization, and device PIN lock
 - Create a baseline Mobile Application Management (MAM) Intune App Policy to include data encryption, data containerization, and app PIN lock
 - Provide a two-week pilot for up to five Android Enterprise or iOS devices
- Workstation Management (Windows 10 1809 or newer)
 - Provide a one-hour workshop to review baseline configurations
 - Create a baseline Windows 10 Device Compliance Policy
 - Create a baseline MacOS Device Compliance Policy
 - Create a Windows 10 Security Baseline profile (previously EMET)
 - Create a Microsoft Defender ATP Baseline profile
 - Configure OneDrive Known Folder Protection for Windows 10
 - Remove Windows 10 Consumer Experience and uninstall bloatware
 - Provide a two-week pilot for up to five Windows 10 devices
- Data Loss Prevention
 - Provide a one-hour workshop to review baseline configurations
 - Enable global Office 365 DLP Policies for Exchange Online for the following information types:
 - Credit Card Number
 - U.S. Bank Account Number
 - U.S. Individual Taxpayer ID Number (ITIN)
 - U.S. Social Security Number (SSN)
 - Configure baseline Office Message Encryption templates for end-users
 - Configure up to two retention policies
 - Enable Unified Labeling Experience
 - Configure Azure Information Protection Agent deployment via Intune

ZTS Accelerator for Threat Protection

By standardizing on the Microsoft 365 security platform, you can integrate threat analytics from over 60+ security products to create risk profiles for users and devices in real-time. Conditional Access policies that are configured in the ZTS accelerator for Modern Authentication will be enriched with this data, providing fewer false positives and identifying breaches faster.

Infused Innovations will perform the following tasks as part of this accelerator:

- Azure ATP
 - Deploy the Azure ATP Workspace in your Azure subscription
 - Deploy the ATA lightweight gateway on up to five domain controllers
 - Configure monitoring alerts
 - Integrate with Microsoft Defender ATP
 - Review of configured environment
- Microsoft Defender ATP
 - Configure the Windows Defender Security Portal
 - Configure Microsoft Defender ATP Onboarding via Intune
 - Enable integration with Microsoft Cloud App Security
- Shadow IT Discovery
 - Enable the Microsoft Cloud App Security Portal
 - Provide a two-hour workshop to review baseline policies and how to use the portal
 - Integrate MCAS with Microsoft Defender ATP
- Configure Log Analytics and Azure Security Center for infrastructure monitoring via agent
- Configure baseline Azure Sentinel collection with native Microsoft cloud services

vCISO Services

The biggest threat facing a modern business is in the realm of security—and the biggest threat facing a secure business is complexity. Our reference architecture for a Secure Intelligent Workplace can take years for a new team to comprehend and implement. With the shortage of cybersecurity professionals, you must also worry about employee turnover after a team is established.

Infused Innovation's vCISO services ensure that all processes and policies have security as an underpinning—projecting confidence and trust in customer, vendor, and partner relations. Using a fractional model of a vCISO is of high importance to customers that take these roles and responsibilities seriously in understanding the risk models of the current threat landscape.

Our vCISO services use metrics collected from our monthly Security-as-a-Service platform, SecurÆther, to provide ongoing guidance and recommendations to protect against new cyber threats.