

Effective March 25, 2026. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a separate Order including those Services.

DATA BACKUP AND DISASTER RECOVERY SERVICE

Local Backups - Using hardware and software (backup software), backups will be performed on the basis specified in the Order. Any Client provided hardware or software used for local backups must be acceptable to Provider. Client owns or rents the hardware and software agents (backup software) used to perform the backups. Provider will review the backups daily and notify Client of backup failures. Client upon request will perform simple on-site tasks (e.g., powering down and rebooting hardware).

Remote Backups - Provider, through its Third-Party Service Providers will make all commercially reasonable efforts, consistent with industry practices, to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at the Provider's or third-party vendor's data center facility. Data files can be restored from the cloud, but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. All data is backed up via a third-party client-side desktop/server software application (the "Application"). Provider will monitor the backups daily, notify Client of any failures, and work to resolve backup failures.

Cloud Backup - Provider, through its Third-Party Service Providers will make all commercially reasonable efforts, consistent with industry practice, to ensure the protection and recovery of Client's information. Data is backed up via a third-party application, encrypted, and sent to a third-party owned storage server at the Third-Party Services Provider's data center facility. Provider will monitor the status of all scheduled backup jobs, notify Client of failures and corrective actions. Provider will also provide remote administrative services of Data Backup Service as requested by Client.

Upon termination of these Services, Provider will request return of any Provider owned backup hardware and remove the Application from Client systems.

File Recovery

Provider will create, monitor, and modify up to the number of backup jobs as defined by the Client or per the Provider's best practice recommendations.

Upon request, Provider will remotely restore files.

Disaster Recovery

If Client experiences an event precipitating a major, multi-user loss of data, Client may notify Provider that a data loss event has occurred.

CLOUD AND HOSTING SERVICES

Private Cloud or Software Subscriptions - Provider will maintain all Client's data on premise at Provider's location, manage the cloud environment and software subscriptions for Client, provide unmanaged cloud environment and software subscriptions for Client, and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement as listed on the Order.

Third-Party Cloud & SaaS Vendors - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

Co-Location – Provider will provide required rack space as listed on the Order for the Client's hardware to be stored.

BUSINESS INTELLIGENCE

Provider will provide and support the Third-Party Cloud or software-as-a-service vendor per the Order, including but not limited to Microsoft. Unlimited remote "how-to" support is provided up to 1 (one) hour per unique request. Provider will test for functionality and manage Microsoft updates in addition to monitoring approved Integrations. The Service Fee does not include Consulting Services; if used, Client will pay Provider's then prevailing hourly rate.

Secure Managed Services

Centre Partnership Value Add Services

Specialized customer service you want, and cyber protection you need.

- ✓ Local 24x7 IT Support
- ✓ Layered Security Protection
- ✓ Personalized IT Innovation Recommendations and Consulting

- ✓ Detailed IT Environment Reporting (CMAC™ Dashboard)
- ✓ Quarterly Business Reviews Aligned to Your Business Goals
- ✓ Automatic End-to-End Threat Remediation and Verification*
Applies to devices running Endpoint Detection and Response (EDR).

Summary of Services

IT MANAGEMENT SERVICES

Personalized End User Support

24x7 Unlimited Technical Support

- Delivers Help Desk Support services via phone and email
- Supports both Windows and Apple/Mac operating systems
- Maintains and monitors operating system updates and security patching
- Monitors free disk/hard drive space availability
- Includes troubleshooting of Microsoft Office applications such as Microsoft Outlook, Excel, Word, etc.

Emergency On-Site Support*

- Delivers global on-site emergency desk-side support as deemed necessary by Centre technical consultants
- Includes access to Emergency Dispatch of Field Resources supporting desk-side, break-fix and troubleshooting
- Not included with Secure Co-Managed Services.*

Mobile and Tablet Support

- Includes Android and Apple/Mac iOS devices
- Configures account and email access
- Configures and optimizes Mobile Device Management (MDM) policies
- Installs operating system updates upon request
- Configures Multi-Factor Authentication (MFA) per Customer policy
- Supports and troubleshoots Customer-specific mobile applications to ensure functionality

Peripheral Hardware Support

- Includes troubleshooting of printers, monitors, keyboards, mice, etc.
- Monitors and manages available print queues

Public Cloud Support (Azure and Amazon Web Services)

- Strategizes workloads and applications
- Manages applications, availability and access permissions
- Troubleshoots connectivity
- Secures and optimizes private and public file storage systems
- Develops policies and procedures for private and public cloud storage access and permissions
- Support for Microsoft Azure and Amazon Web Services (AWS) requires additional services.

Proactive Systems Maintenance

Server Maintenance and Support

- Monitors general and critical server activity 24x7
- Monitors critical server services 24x7
- Installs minor server operating system updates and security patching
- Monitors Microsoft server operating system updates and security patching
- Strategizes policies for scheduled off-time server maintenance
- Manages Microsoft Active Directory (database) group policies and account access permissions
- Creates/deletes user accounts and groups upon Customer request
- Initiates server reboots as necessary
- Monitors and manages Microsoft Distributed File System Replication (DFS) configurations
- Monitors general system health and performance
- Reports memory constraints, predictive hard drive failure alerts, connectivity loss for storage controllers, and unusual collision activity for network cards
- Optimizes disk use via defrag and “chkdsk” utilities as necessary
- Monitors free disk/hard drive space availability
- Includes up to 4 hours of disk space activity management per month
- Additional disk space management services available separately through Centre Project Services*

Critical Service Monitoring

- Monitors and verifies critical application availability
- Monitors available server resources to deliver critical applications

Email Management

- Includes configuring and managing on-premise Microsoft Exchange and Microsoft Office 365 user accounts and mailboxes

Qualified Software Application Support

Software-as-a-Service (SaaS) and Third-Party Support

- Includes (but not limited to) providers such as Salesforce.com, QuickBooks Online, NetSuite, Microsoft Dynamics, etc.

Specialty Applications Support

- Delivers support and troubleshooting of on-premise applications
- Excludes installing of application updates
- Available separately at an hourly rate through Centre Project Services.*

Microsoft Office Desktop Application Support

- Includes troubleshooting of Microsoft Outlook, Excel, Word, etc.

Microsoft Office 365 Management

- Support for Microsoft 365 tenant requires additional services*

Operating System (OS) Management and Support

Proven Network Protection

24x7 Network Monitoring and Maintenance

- Monitors and optimizes internet availability and bandwidth
- Monitors network switches and routers availability
- Ensures office network connectivity and performance
- Delivers capacity planning and strategy
- Installs available manufacturer Security and Emergency Updates for network devices such as routers and Wide-Area Network (WAN)
- Troubleshoots internal and external connectivity
- Analyzes router logs during troubleshooting

Firewall Management and Optimization

- Troubleshoots internal and external access
- Analyzes firewall logs during troubleshooting

Verified System Backups and Disaster Recovery

Customer owned or licensed solution(s).

Disaster Recovery Management

- Develops backup strategy
- Conducts monthly restore tests using C-Stack™ compliant tools
 - Applies to C-Stack™ compliant solutions.*
- Oversees data recovery policy compliance
- Performs remote restore operations to recover deleted files and corrupted files from backups upon Customer request

Backup Management and Optimization

- Creates and modifies backups as necessary or upon Customer request, including servers and network devices
- Monitors statuses of scheduled and on-demand backups
- Reports backup failures and recommends corrective actions via email
- Troubleshoots failed backups
- Provides remote administrative backup services upon Customer request
- Notifies when off/on-site action is required, such as cycling of drives

Transparent Service Performance

Documentation

- Reports IT environment data collected during scheduled system audits and hardware/software inventories provided through a secure online portal

Real-Time Business Intelligence (BI) Performance Analytics

- Centre Metrics Assurance and Compliance (CMAC™) Portal
- Provides monthly executive-level summary via email
- Reports service performance across service goals
 - Refer to Centre's Service Attachment (SA) for Secure Managed Services for details.*
- Summarizes latest asset inventory
- Displays real-time scoring for patching, backups and anti-virus compliance
- Logs End User support tickets
- Supports self-service ticket management
- Recaps billing history and trends across Centre services

Quarterly Business Reviews

Available upon request.

Comprehensive Security Protection

24x7 Layered Security

- Filters suspicious activity and connection attempts
- Improves overall security awareness and posture

Continuous Security Posture Assessment

Next Gen Anti-Virus Endpoint Protection

- Provides machine-learning and reputation scoring on global security threats to detect and prevent zero-day attacks
- Blocks identified malware and ransomware from internet sources
- Delivers visibility to internet activity across all endpoints and locations

Endpoint Detection and Response (EDR) Protection

- Monitors individual endpoints, including laptops and desktops
- Looks for data exfiltration (unauthorized data transfer) from device and applications
- Checks for activity from known malicious IP addresses
- Machine-learning and human-driven threat hunting
- Automatically contains threats by isolating verified endpoint threats
- Delivers rapid response and transparent remediation and verification
- Confirms anti-virus is installed and current for devices and local virtual machines (VM)
- Delivers personalized analysis from certified Security Analyst
- Provides remediation guidance and support for misconfigurations
- Delivers automatic and transparent remediation of misconfigurations
- Delivers personalized SOCaaS Security Incident Summary, including systems impacted, containment status, potential risks, incident details, remediation steps taken and long-term recommendations
- Delivers remediation guidance and support from both global security professionals and local experts
- Conducts secondary review by Centre security experts and analysts
- Checks for improper resource usage and changes to user and account privileges from operating system and applications
- Reports non-best practice configurations for endpoint security settings
- Provides additional evidence of compliance efforts

For detailed inclusions, see Endpoint Detection and Response (EDR) section of Centre Managed Detection and Response (MDR) with SOCaaS Features Summary.

Proactive End User Protection

Employee Security Awareness Training

- Conducts simulated phishing campaigns to test behaviors
- Provides best practices for password creation
- Educates employees using proven computer-based training platforms for cybersecurity awareness and visibility

Laptop Data Encryption

- Enforces Windows data encryption on company workstations and laptops
- Encrypts data stored on Windows workstations and laptops
- Integrates with Windows operating system
- Prevents data theft or exposure from lost, stolen, or inappropriately decommissioned computers
- Hardware and firmware requirements apply, including Trusted Platform Module (TPM) installed on device

Web Content Filtering and Secure Gateway

- Blocks known and requested website (URL) addresses

Geo Fencing

- Limits and optimizes network access from Customer-specified countries, regions and/or IP addresses
- Includes network firewall and Microsoft Office 365 configurations
- Monitors blocked or limited sources

Privilege Access Management

Dark Web Identity Scanning

Virtual Private Network (VPN)

- Configures and manages secure connections to shared network devices, servers and/or workstations
- Upon providing recommendations on enhanced and secured solutions.*

Secure Co-Managed Services

Centre Partnership Value Add Services

Specialized customer service you want, and cyber protection you need.

- ✓ Local 24x7 IT Support
- ✓ Layered Security Protection
- ✓ Personalized IT Innovation Recommendations and Consulting
- ✓ Detailed IT Environment Reporting (CMAC™ Dashboard)
- ✓ Quarterly Business Reviews Aligned to Your Business Goals
- ✓ Automatic End-to-End Threat Remediation and Verification*
Applies to devices running Endpoint Detection and Response (EDR).

Summary of Services

IT MANAGEMENT SERVICES

Personalized Internal IT Support

24x7 Unlimited Technical Support for IT Staff

- Delivers Help Desk Escalation Support for internal IT staff via phone and email
- Supports both Windows and Apple/Mac operating systems
- Maintains and monitors operating system updates and security patching
- Monitors free disk/hard drive space availability
- Includes troubleshooting of Microsoft Office applications such as Microsoft Outlook, Excel, Word, etc.
- Up to 15 business days of on-site IT staff augmentation for coverage during planned Paid Time Off (PTO) by internal IT staff per calendar year (no rollover)
- Requires request be submitted 14 business days prior to on-site date.*

Mobile and Tablet Support

- Includes Android and Apple/Mac iOS devices
- Configures account and email access
- Configures and optimizes Mobile Device Management (MDM) policies
- Installs operating system updates upon request
- Configures Multi-Factor Authentication (MFA) per Customer policy
- Supports and troubleshoots Customer-specific mobile applications to ensure functionality

Peripheral Hardware Support

- Includes troubleshooting of printers, monitors, keyboards, mice, etc.
- Monitors and manages available print queues

Public Cloud Support (Azure and Amazon Web Services)

- Strategizes workloads and applications
- Manages applications, availability and access permissions
- Troubleshoots connectivity
- Secures and optimizes private and public file storage systems
- Develops policies and procedures for private and public cloud storage access and permissions
- Support for Microsoft Azure and Amazon Web Services (AWS) requires additional services.

Proactive Systems Maintenance

Server Maintenance and Support

- Monitors general and critical server activity 24x7
- Monitors critical server services 24x7
- Installs minor server operating system updates and security patching
- Monitors Microsoft server operating system updates and security patching
- Strategizes policies for scheduled off-time server maintenance
- Manages Microsoft Active Directory (database) group policies and account access permissions
- Creates/deletes user accounts and groups upon Customer request
- Initiates server reboots as necessary

- Monitors and manages Microsoft Distributed File System Replication (DFS) configurations
- Monitors general system health and performance
- Reports memory constraints, predictive hard drive failure alerts, connectivity loss for storage controllers, and unusual collision activity for network cards
- Optimizes disk use via defrag and “chkdsk” utilities as necessary
- Monitors free disk/hard drive space availability
- Includes up to 4 hours of disk space activity management per month
- Additional disk space management services available separately through Centre Project Services*

Critical Service Monitoring

- Monitors and verifies critical application availability
- Monitors available server resources to deliver critical applications

Email Management

- Includes configuring and managing on-premise Microsoft Exchange and Microsoft Office 365 user accounts and mailboxes

Qualified Software Application Support

Software-as-a-Service (SaaS) and Third-Party Support

- Includes (but not limited to) providers such as Salesforce.com, QuickBooks Online, NetSuite, Microsoft Dynamics, etc.

Specialty Applications Support

- Delivers support and troubleshooting of on-premise applications
- Excludes installing of application updates
- Available separately at an hourly rate through Centre Project Services.*

Microsoft Office Desktop Application Support

- Includes troubleshooting of Microsoft Outlook, Excel, Word, etc.

Microsoft Office 365 Management

- Support for Microsoft 365 tenant requires additional services*

Operating System (OS) Management and Support

Proven Network Protection

24x7 Network Monitoring and Maintenance

- Monitors and optimizes internet availability and bandwidth
- Monitors network switches and routers availability
- Ensures office network connectivity and performance
- Delivers capacity planning and strategy
- Installs available manufacturer Security and Emergency Updates for network devices such as routers and Wide-Area Network (WAN)
- Troubleshoots internal and external connectivity
- Analyzes router logs during troubleshooting

Firewall Management and Optimization

- Troubleshoots internal and external access
- Analyzes firewall logs during troubleshooting

Verified System Backups and Disaster Recovery

Customer owned or licensed solution(s).

Disaster Recovery Management

- Develops backup strategy
- Conducts monthly restore tests using C-Stack™ compliant tools
 - Applies to C-Stack™ compliant solutions.*
- Oversees data recovery policy compliance
- Performs remote restore operations to recover deleted files and corrupted files from backups upon Customer request

Backup Management and Optimization

- Creates and modifies backups as necessary or upon Customer request, including servers and network devices
- Monitors statuses of scheduled and on-demand backups
- Reports backup failures and recommends corrective actions via email
- Troubleshoots failed backups
- Provides remote administrative backup services upon Customer request
- Notifies when off/on-site action is required, such as cycling of drives

Transparent Service Performance

Real-Time Business Intelligence (BI) Performance Analytics

- Centre Metrics Assurance and Compliance (CMAC™) Portal
- Provides monthly executive-level summary via email
- Reports service performance across service goals
 - Refer to Centre's Service Attachment (SA) for Secure Managed Services for details.*
- Summarizes latest asset inventory
- Displays real-time scoring for patching, backups and anti-virus compliance
- Logs End User support tickets
- Supports self-service ticket management
- Recaps billing history and trends across Centre services

Documentation

- Reports IT environment data collected during scheduled system audits and hardware/software inventories provided through a secure online portal

Quarterly Business Reviews

Available upon request.

SECURITY SERVICES

Comprehensive Security Protection

24x7 Layered Security

- Filters suspicious activity and connection attempts
- Improves overall security awareness and posture

Continuous Security Posture Assessment

Next Gen Anti-Virus Endpoint Protection

- Provides machine-learning and reputation scoring on global security threats to detected and prevent zero-day attacks
- Blocks identified malware and ransomware from internet sources
- Delivers visibility to internet activity across all endpoints and locations

Endpoint Detection and Response (EDR) Protection

- Monitors individual endpoints, including laptops and desktops
- Looks for data exfiltration (unauthorized data transfer) from device and applications
- Checks for activity from known malicious IP addresses
- Machine-learning and human-driven threat hunting
- Automatically contains threats by isolating verified endpoint threats
- Delivers rapid response and transparent remediation and verification
- Confirms anti-virus is installed and current for devices and local virtual machines (VM)
- Delivers personalized analysis from certified Security Analyst
- Provides remediation guidance and support for misconfigurations
- Delivers automatic and transparent remediation of misconfigurations
- Delivers personalized SOCaaS Security Incident Summary, including systems impacted, containment status, potential risks, incident details, remediation steps taken and long-term recommendations
- Delivers remediation guidance and support from both global security professionals and local experts
- Conducts secondary review by Centre security experts and analysts
- Checks for improper resource usage and changes to user and account privileges from operating system and applications
- Reports non-best practice configurations for endpoint security settings
- Provides additional evidence of compliance efforts

For detailed inclusions, see Endpoint Detection and Response (EDR) section of Centre Managed Detection and Response (MDR) with SOCaaS Features Summary.

Proactive End User Protection

Employee Security Awareness Training

- Conducts simulated phishing campaigns to test behaviors
- Provides best practices for password creation
- Educates employees using proven computer-based training platforms for cybersecurity awareness and visibility

Laptop Data Encryption

- Enforces Windows data encryption on company workstations and laptops
- Encrypts data stored on Windows workstations and laptops
- Integrates with Windows operating system
- Prevents data theft or exposure from lost, stolen, or inappropriately decommissioned computers
- Hardware and firmware requirements apply, including Trusted Platform Module (TPM) installed on device

Web Content Filtering and Secure Gateway

- Blocks known and requested website (URL) addresses

Geo Fencing

- Limits and optimizes network access from Customer-specified countries, regions and/or IP addresses
- Includes network firewall and Microsoft Office 365 configurations
- Monitors blocked or limited sources

Privilege Access Management

Dark Web Identity Scanning

Virtual Private Network (VPN)

- Configures and manages secure connections to shared network devices, servers and/or workstations
- Upon providing recommendations on enhanced and secured solutions.*

Cybersecurity Leadership

Compliance Strategy (PCI, HIPPA, SOC, etc.)

Security Process and Policy Consulting

- Advises on internal processes to ensure optimal security posture
- Proactively enhances Centre tools for maximum protection

Enhanced Security Management

Account Access Maintenance

- Scans directory services for inactive user accounts
- Disables or deletes inactive useraccounts and devices (after 30 days of inactivity), directories, shares and/or security groups per security policies

Microsoft Security Patch Management

- Monitors and implements critical security patches on systems

Password Policy Enforcement and Management

- Centrally-manages all endpoint devices
- Includes individual licensing of password management software for each endpoint device

Microsoft Office 365 Security Management

- Assures all appropriate available security features are applied
- Leverages granular controls and security policies

Multi-Factor Authentication (MFA) Management

- Enforces and monitors end user enrollment and compliance

Centralized Anti-Virus Management

- Includes anti-virus software for all covered endpoint devices
- Conducts antivirus scans using C-Stack™ compliant services and utilities
- Installs available anti-virus engine and definition updates

Cybersecurity Leadership

Compliance Strategy (PCI, HIPPA, SOC, etc.)

Security Process and Policy Consulting

Advises on internal processes to ensure optimal security posture

Proactively enhances Centre tools for maximum protection

Enhanced Security Management

Account Access Maintenance

Scans directory services for inactive user accounts

Disables or deletes inactive useraccounts and devices (after 30 days of inactivity), directories, shares and/or security groups per security policies

Microsoft Security Patch Management

Monitors and implements critical security patches on systems

Password Policy Enforcement and Management

Centrally-manages all endpoint devices

Includes individual licensing of password management software for each endpoint device

Microsoft Office 365 Security Management

Assures all appropriate available security features are applied

Leverages granular controls and security policies

Multi-Factor Authentication (MFA) Management

Enforces and monitors end user enrollment and compliance

Centralized Anti-Virus Management

Includes anti-virus software for all covered endpoint devices

Conducts antivirus scans using C-Stack™ compliant services and utilities

Installs available anti-virus engine and definition updates

SMS Express

Centre Partnership Value Add Services

Specialized customer service you want, and cyber protection you need.

- ✓ Secure by Design Starter Microsoft Azure Virtual Servers and Cloud Desktops
- ✓ Local 24x7 IT Support
- ✓ Layered Security Protection
- ✓ Personalized IT Innovation Recommendations and Consulting
- ✓ Detailed IT Environment Reporting (CMAC™ Dashboard)
- ✓ Quarterly Business Reviews Aligned to Your Business Goals
- ✓ Automatic End-to-End Threat Remediation and Verification*
Applies to devices running Endpoint Detection and Response (EDR).

Summary of Services

IT MANAGEMENT SERVICES

Personalized End User Support

24x7 Unlimited Technical Support

- Delivers Help Desk Support services via phone and email
- Supports both Windows and Apple/Mac operating systems
- Maintains and monitors operating system updates and security patching
- Monitors free disk/hard drive space availability
- Includes troubleshooting of Microsoft Office applications such as Microsoft Outlook, Excel, Word, etc. on Virtual Desktops
- Excludes any software or applications not hosted in Microsoft Azure
- Excludes workstation moves (available separately at an hourly rate)

Emergency On-Site Support

- Delivers global on-site emergency desk-side support as deemed necessary by Centre technical consultants
- Includes access to Emergency Dispatch of Field Resources supporting desk-side, break-fix and troubleshooting

Peripheral Hardware Support

- Includes troubleshooting of printers, monitors, keyboards, mice, etc.
- Monitors and manages available print queues

Public Cloud Support (Microsoft Azure Only)

- Strategizes workloads and applications
- Manages applications, availability and access permissions
- Troubleshoots connectivity
- Secures and optimizes private and public file storage systems
- Develops policies and procedures for private and public cloud storage access and permissions

Proactive Systems Maintenance

Server Maintenance and Support

- Monitors general and critical server activity 24x7
- Monitors critical server services 24x7
- Installs minor server operating system updates and security patching
- Monitors Microsoft server operating system updates and security patching
- Strategizes policies for scheduled off-time server maintenance
- Manages Microsoft Active Directory (database) group policies and account access permissions
- Creates/deletes user accounts and groups upon Customer request
- Initiates server reboots as necessary
- Monitors and manages Microsoft Distributed File System Replication (DFS) configurations

- Monitors general system health and performance
- Reports memory constraints, predictive hard drive failure alerts, connectivity loss for storage controllers, and unusual collision activity for network cards
- Optimizes disk use via defrag and “chkdsk” utilities as necessary
- Monitors free disk/hard drive space availability
- Includes up to 4 hours of disk space activity management per month
Additional disk space management services available separately through Centre Project Services

Critical Service Monitoring

- Monitors and verifies critical application availability
- Monitors available server resources to deliver critical applications

Email Management

- Includes configuring Microsoft Office 365 user accounts and mailboxes

Qualified Software Application Support on Virtual Desktops

Software-as-a-Service (SaaS) and Third-Party Support

- Includes (but not limited to) providers such as Salesforce.com, QuickBooks Online, NetSuite, Microsoft Dynamics, etc.
- Excludes any software or applications not hosted in Microsoft Azure

Specialty Applications Support

- Delivers support and troubleshooting of applications hosted in Microsoft Azure
- Excludes installing of application updates
Available separately at an hourly rate through Centre Project Services.

Microsoft Office Desktop Application Support

- Includes troubleshooting of Microsoft Outlook, Excel, Word, etc. on Virtual Desktops
- Excludes any software or applications not hosted in Microsoft Azure

Microsoft Office 365 Management

- Includes licensing modifications, additions, or removals
- Includes troubleshooting of Microsoft 365 tenant
- Advanced Microsoft 365 Business Intelligence (BI) and security protections sold separately

Operating System (OS) Management and Support

Proven Network Protection

24x7 Network Monitoring and Maintenance (Meraki Only)

- Monitors and optimizes internet availability and bandwidth
- Monitors network switches and routers availability
- Ensures office network connectivity and performance
- Delivers capacity planning and strategy
- Installs available manufacturer Security and Emergency Updates for network devices such as routers and Wide-Area Network (WAN)
- Troubleshoots internal and external connectivity
- Analyzes router logs during troubleshooting

Firewall Management and Optimization (Meraki Only)

- Troubleshoots internal and external access
- Analyzes firewall logs during troubleshooting

Verified System Backups and Disaster Recovery

Customer owned or licensed solution(s).

Disaster Recovery Management

- Develops backup strategy
- Conducts monthly restore tests using C-Stack™ compliant tools
 - Applies to C-Stack™ compliant solutions.*
- Oversees data recovery policy compliance
- Performs remote restore operations to recover deleted files and corrupted files from backups upon Customer request

Backup Management and Optimization

- Creates and modifies backups as necessary or upon Customer request, including servers and network devices
- Monitors statuses of scheduled and on-demand backups
- Reports backup failures and recommends corrective actions via email
- Troubleshoots failed backups
- Provides remote administrative backup services upon Customer request
- Notifies when off/on-site action is required, such as cycling of drives

Transparent Service Performance

Documentation

- Reports IT environment data collected during scheduled system audits and hardware/software inventories provided through a secure online portal

Real-Time Business Intelligence (BI) Performance Analytics

- Centre Metrics Assurance and Compliance (CMAC™) Portal
- Provides monthly executive-level summary via email
- Reports service performance across service goals
 - Refer to Centre's Service Attachment (SA) for Secure Managed Services for details.*
- Summarizes latest asset inventory
- Displays real-time scoring for patching, backups and anti-virus compliance
- Logs End User support tickets
- Supports self-service ticket management
- Recaps billing history and trends across Centre services

Quarterly Business Reviews

Available upon request.

Comprehensive Security Protection

24x7 Layered Security

- Filters suspicious activity and connection attempts
- Improves overall security awareness and posture

Continuous Security Posture Assessment

Next Gen Anti-Virus Endpoint Protection

- Provides machine-learning and reputation scoring on global security threats to detected and prevent zero-day attacks
- Blocks identified malware and ransomware from internet sources
- Delivers visibility to internet activity across all endpoints and locations

Endpoint Detection and Response (EDR) Protection

- Monitors individual endpoints, including laptops and desktops
 - Looks for data exfiltration (unauthorized data transfer) from device and applications
 - Checks for activity from known malicious IP addresses
 - Machine-learning and human-driven threat hunting
 - Automatically contains threats by isolating verified endpoint threats
 - Delivers rapid response and transparent remediation and verification
 - Confirms anti-virus is installed and current for devices and local virtual machines (VM)
 - Delivers personalized analysis from certified Security Analyst
 - Provides remediation guidance and support for misconfigurations
 - Delivers automatic and transparent remediation of misconfigurations
 - Delivers personalized SOCaaS Security Incident Summary, including systems impacted, containment status, potential risks, incident details, remediation steps taken and long-term recommendations
 - Delivers remediation guidance and support from both global security professionals and local experts
 - Conducts secondary review by Centre security experts and analysts
 - Checks for improper resource usage and changes to user and account privileges from operating system and applications
 - Reports non-best practice configurations for endpoint security settings
 - Provides additional evidence of compliance efforts
- For detailed inclusions, see Endpoint Detection and Response (EDR) section of Centre Managed Detection and Response (MDR) with SOCaaS Features Summary.*

Proactive End User Protection

Employee Security Awareness Training

- Conducts simulated phishing campaigns to test behaviors
- Provides best practices for password creation
- Educates employees using proven computer-based training platforms for cybersecurity awareness and visibility

Laptop Data Encryption

- Enforces Windows data encryption on company workstations and laptops
- Encrypts data stored on Windows workstations and laptops
- Integrates with Windows operating system
- Prevents data theft or exposure from lost, stolen, or inappropriately decommissioned computers
- Hardware and firmware requirements apply, including Trusted Platform Module (TPM) installed on device

Web Content Filtering and Secure Gateway

- Blocks known and requested website (URL) addresses

Geo Fencing

- Limits and optimizes network access from Customer-specified countries, regions and/or IP addresses
- Includes network firewall and Microsoft Office 365 configurations
- Monitors blocked or limited sources

Privilege Access Management

Dark Web Identity Scanning

Virtual Private Network (VPN)

- Configures and manages secure connections to shared network devices, servers and/or workstations
- Upon providing recommendations on enhanced and secured solutions.*

Cybersecurity Leadership

Compliance Strategy (PCI, HIPPA, SOC, etc.)

Security Process and Policy Consulting

- Advises on internal processes to ensure optimal security posture
- Proactively enhances Centre tools for maximum protection

Enhanced Security Management

Account Access Maintenance

- Scans directory services for inactive user accounts
- Disables or deletes inactive useraccounts and devices (after 30 days of inactivity), directories, shares and/or security groups per security policies

Microsoft Security Patch Management

- Monitors and implements critical security patches on systems

Microsoft Office 365 Security Management

- Assures all appropriate available security features are applied
- Leverages granular controls and security policies

Password Policy Enforcement and Management

- Centrally-manages all endpoint devices
- Includes individual licensing of password management software for each endpoint device

Multi-Factor Authentication (MFA) Management

- Enforces and monitors end user enrollment and compliance

Centralized Anti-Virus Management

- Includes anti-virus software for all covered endpoint devices
 - Conducts antivirus scans using C-Stack™ compliant services and utilities
- Installs available anti-virus engine and definition updates

Managed Detection and Response (MDR) with SOCaaS

Centre Partnership Value Add Services

Force multiplying threat detection and remediation guidance with enhanced tracking, visibility, and consulting.

- ✓ Local Security Analysts Supporting Co-Managed IT Environments
- ✓ Threat and Vulnerability Remediation Guidance and Consulting
- ✓ Tailored SOCaaS Threat Detection and Remediation Reporting (CMAC™ Security Dashboard)
- ✓ Weekly and Monthly SOCaaS Reports
- ✓ Personalized Security Innovation Recommendations and Consulting
- ✓ Automatic End-to-End Threat Remediation and Verification*
Requires Centre Secure Managed Services agreement.

Summary of Services

MANAGED DETECTION AND RESPONSE (MDR)

24x7 network monitoring, threat containment and remediation guidance across your entire local environment of networked devices.

Threat Monitoring

- ✓ 24x7 Detection and Response
 - Monitors networks and connected devices and local virtual machines (VM)
 - Looks for suspicious network use and spikes
 - Checks for activity from known malicious IP addresses
- ✓ Proactive Threat Hunting
 - Machine-learning threat hunting
 - Human-driven threat hunting
- ✓ Perimeter Assessments
 - Monitors for local network threats
 - Searches for threats and provides remediation guidance

Threat Containment and Remediation

- ✓ Automatic Threat Containment
 - Automatically contains threats by isolating verified network threats
 - Provides remediation guidance and support
 - Delivers rapid response and transparent remediation*
Requires Centre Secure Managed Services agreement.
 - Provides remediation verification
- ✓ Misconfiguration Analysis and Remediation
 - Confirms anti-virus is installed and current
 - Delivers personalized analysis from certified Security Analyst
 - Provides remediation guidance and support for misconfigurations
 - Delivers automatic and transparent remediation of misconfigurations*
Requires Centre Secure Managed Services agreement.
- ✓ Triage and Remediation
 - Delivers personalized SOCaaS Security Incident Summary, including systems impacted, containment status, potential risks, incident details, remediation steps taken and long-term recommendations
 - Delivers remediation guidance and support from both global security professionals and local experts
 - Conducts secondary review by Centre security experts and analysts

Security Management

- ✓ Identity Management
 - Checks for improper resource network usage and connections
 - Checks for unusual changes to network privileges
- ✓ Log Management
 - Supports SIEM integration
 - Configures SIEM tools

Reporting

- ✓ Security Reporting
 - CMAC™ Security Dashboard*
Access to additional Managed Detection and Response (MDR) management tools available upon request.
 - Weekly SOCaaS Report
 - Monthly SOCaaS Summary
 - Categorizes alerts by raw signals, filtered, incidents and escalations
- ✓ Audit Reporting
 - Fulfills compliance requirements like PCI DSS, HIPAA, CMMC, SEC, ISO, etc.
 - Provides additional evidence of compliance efforts
- ✓ Security Innovation Recommendations
 - Provides security hardening recommendations and consulting*
Additional support requires Centre Secure Managed Services or available separately at an hourly rate.
 - Provides insights on both global and industry threat landscape
 - Reports security advisory news and exploit briefs

ENDPOINT DETECTION AND RESPONSE (EDR)

24x7 device monitoring, threat containment and remediation guidance for desktops, laptops, on-prem servers and local virtual machines.

Threat Monitoring

- ✓ **24x7 Endpoint Detection and Response**
 - Monitors individual endpoints, including laptops and desktops
 - Looks for data exfiltration (unauthorized data transfer) from endpoint device and installed applications
 - Checks for activity from known malicious IP addresses
- ✓ **Proactive Threat Hunting**
 - Machine-learning threat hunting
 - Human-driven threat hunting
- ✓ **Perimeter Assessments**
 - Monitors for local device threats
 - Searches for threats and provides remediation guidance

Threat Containment and Remediation

- ✓ **Automatic Threat Containment**
 - Automatically contains threats by isolating verified endpoint threats
 - Provides remediation guidance and support
 - Delivers rapid response and transparent remediation*
Requires Centre Secure Managed Services.
 - Provides remediation verification
- ✓ **Misconfiguration Analysis and Remediation**
 - Confirms anti-virus is installed and current for devices and local virtual machines (VM)
 - Delivers personalized analysis from certified Security Analyst
 - Provides remediation guidance and support for misconfigurations
 - Delivers automatic and transparent remediation of misconfigurations*
Requires Centre Secure Managed Services.
- ✓ **Triage and Remediation**
 - Delivers personalized SOCaaS Security Incident Summary, including systems impacted, containment status, potential risks, incident details, remediation steps taken and long-term recommendations
 - Delivers remediation guidance and support from both global security professionals and local experts
 - Conducts secondary review by Centre security experts and analysts

Security Management

- ✓ **Identity Management**
 - Checks for improper resource usage from operating system and applications
 - Checks for unusual changes to user and account privileges
- ✓ **Log Management**
 - Supports SIEM integration
 - Configures SIEM tools

Reporting

- ✓ **Security Reporting**
 - CMAC™ Security Dashboard*
Access to additional Managed Detection and Response (MDR) management tools available upon request.
 - Weekly SOCaaS Report
 - Monthly SOCaaS Summary
 - Categorizes alerts by raw signals, filtered, incidents and escalations
- ✓ **Audit Reporting**
 - Fulfills compliance requirements like PCI DSS, HIPAA, CMMC, SEC, ISO, etc.
 - Provides additional evidence of compliance efforts
- ✓ **Misconfiguration Reporting**
 - Reports non-best practice configurations for individual endpoint security settings
- ✓ **Security Innovation Recommendations**
 - Provides security hardening recommendations and consulting*
Additional support requires Centre Secure Managed Services or available separately at an hourly rate.
 - Provides insights on both global and industry threat landscape
 - Reports security advisory news and exploit briefs

CLOUD DETECTION AND RESPONSE (CDR)

24x7 monitoring and containment across your entire cloud ecosystem, including hosted virtual machines, Microsoft 365, Amazon Web Services, Microsoft Azure, and Google Cloud.

Threat Monitoring

- ✓ **24x7 Cloud Detection and Response**
 - Monitors exposed services and data in cloud infrastructure
 - Looks for data exfiltration (unauthorized data transfer) for both cloud infrastructure and cloud applications
 - Checks for activity from known malicious IP addresses for both cloud infrastructure and cloud applications
- ✓ **Proactive Threat Hunting**
 - Machine-learning threat hunting
 - Human-driven threat hunting
- ✓ **Perimeter Assessments**
 - Monitors for vulnerabilities in integrated cloud environments
 - Searches for vulnerabilities and provides remediation guidance

Threat Containment and Remediation

- ✓ **Automatic Threat Containment**
 - Automatically contains threats by isolating verified cloud threats
 - Provides remediation guidance and support
 - Delivers rapid response and transparent remediation*
Requires Centre Secure Managed Services.
 - Provides remediation verification

- ✓ **Misconfiguration Analysis and Remediation**
 - Confirms anti-virus are installed for Azure virtual machines (VM)
 - Notifies when virtual machines are deployed incorrectly
 - Delivers personalized Security Analyst analysis
 - Provides remediation guidance and support for misconfigurations
 - Delivers automatic and transparent remediation of misconfigurations*
Requires Centre Secure Managed Services.
- ✓ **Triage and Remediation**
 - Delivers personalized SOCaaS Security Incident Summary, including systems impacted, containment status, potential risks, incident details, remediation steps taken and long-term recommendations
 - Delivers remediation guidance and support from both global security professionals and local experts
 - Conducts secondary review by Centre security experts and analysts

Security Management

- ✓ **Identity Management**
 - Monitors Identity Access Management (IAM) policy violations within both cloud infrastructure and cloud applications
 - Checks for improper resource usage in cloud infrastructure
 - Checks for unusual privilege changes within both cloud infrastructure and cloud applications
 - Monitors suspicious email policy changes within cloud applications

- ✓ **Log Management**
 - Supports SIEM integration to public cloud platform
 - Configures SIEM tools in cloud environments

Reporting

- ✓ **Security Reporting**
 - CMAC™ Security Dashboard*
Access to additional Managed Detection and Response (MDR) management tools available upon request.
 - Weekly SOCaaS Report
 - Monthly SOCaaS Summary
 - Categorizes alerts by raw signals, filtered, incidents and escalations

- ✓ **Audit Reporting**
 - Fulfills compliance requirements like PCI DSS, HIPAA, CMMC, SEC, ISO, etc.
 - Provides additional evidence of compliance efforts
- ✓ **Misconfiguration Reporting**
 - Identifies misconfigurations for all cloud workloads (current and new)
 - Reports non-best practice configurations for SQL, firewalls, and TCP ports
- ✓ **Security Innovation Recommendations**
 - Provides security hardening recommendations and consulting*
Additional support requires Centre Azure Operational Care and Optimization or Centre Secure Managed Services.
 - Provides insights on both global and industry threat landscape
 - Reports security advisory news and exploit briefs

LOG MANAGEMENT (SIEM)

Fully aggregated critical threat visibility and log management that prioritizes security gap remediation guidance across your entire technology ecosystem.

Comprehensive Threat Alerts

- ✓ Phishing Attacks
- ✓ Suspicious and/or Unusual User Behavior
- ✓ Data Loss Prevention
- ✓ Privilege Escalations and Alterations
- ✓ Insider Threats
- ✓ Cloud Service Misconfigurations
- ✓ Modular Malware
- ✓ Crypto-Jacking and Crypto-Mining
- ✓ Email Security
- ✓ Brute-Force Attacks

Robust Cloud Integrations

- ✓ **Cloud Infrastructures**
 - Microsoft Azure
 - Amazon Web Services (AWS)
 - Google Cloud
- ✓ **Cloud Applications***
 - Microsoft 365
 - GSuite*Additional applications may be supported.*
- ✓ **Agnostic Log Source Ingestion***
 - Endpoint Detection and Response (EDR)
 - Endpoint Protection Platform (EPP)
 - Network Security
 - VPN Provider Support*Additional log sources may be supported.*
- ✓ **Email Security Platforms***
 - Microsoft Outlook
 - Gmail
 - Proofpoint*Additional platforms may be supported.*
- ✓ **Web Gateway Solutions**

Extended Detection and Response (XDR) Platform

- ✓ Purpose-Built for Cloud
- ✓ Ingests and Enriches Signals
 - SIEM
 - Other MDR solutions
- ✓ Eliminates Noise
- ✓ Enables Real-Time Detection and Response
- ✓ Automatically Blocks Known and Unknown Threats

MITRE ATT&CK Mapping

- ✓ Broad Tactic Categories
- ✓ Individual Technique IDs
- ✓ Detectors and Runbooks

Compliance Assurance

- ✓ **Audit Reporting**
 - Fulfills compliance requirements like PCI DSS, HIPAA, CMMC, SEC, ISO, etc.
 - Provides additional evidence of compliance efforts
- ✓ **Security Innovation Recommendations**
 - Provides security hardening recommendations and consulting*
Additional support requires Centre Secure Managed Services or available separately at an hourly rate.
 - Provides insights on both global and industry threat landscape

Managed Vulnerability Scanning (MVS) Premier + SOCaaS

Centre Partnership Value Add Services

Force multiplying risk management and remediation guidance with enhanced tracking, visibility, and consulting.

- ✓ Extended Local Security Operations Center-as-a-Service (SOCaaS)
- ✓ Rigorous Vulnerability Prioritization
- ✓ Risk Remediation Guidance and Consulting
- ✓ Personalized Security Innovation Recommendations and Consulting
- ✓ Tailored SOCaaS Vulnerability and Remediation Reporting (CMAC™ Security Dashboard)
- ✓ Weekly Internal Vulnerability Reports
- ✓ Monthly External Vulnerability Reports
- ✓ Automatic End-to-End Threat Remediation and Verification*
Requires Centre Secure Managed Services agreement.

Summary of Services

MANAGED VULNERABILITY SCANNING (MVS)

Recurring security scanning of Individual workstations, servers, and network devices.

Enterprise-Grade Security Scanning

- ✓ Tailored Configurations
 - Builds virtual server (VM) in your environment
 - Configures Vulnerability Scanning application, including internal and external IP addresses
 - Performs pre-launch scanning tests across all connected endpoints, workstations, servers, and network devices
 - Schedules monthly scanning of all connected endpoints, workstations, servers, and network devices
- ✓ Process Automation
 - Monthly scheduled external scans
 - Continuous scheduled internal scans
 - On-demand scans as required or upon request

Risk Prioritization

- ✓ Prioritize Vulnerability Risks
 - Prioritized by greatest risk
 - Assets grouped and tracked

Vulnerability Reporting

- ✓ Comprehensive Threat Vulnerability Report
 - Analyzes weekly external vulnerability scanning results
 - Analyzes monthly internal vulnerability scanning results

Consulting and Remediation

- ✓ Personalized Security Vulnerability Posture Consultation
 - Prepares monthly external vulnerability recommendations report
 - Prepares weekly internal vulnerability recommendations report
- ✓ Cloud Security Posture Management (CSPM)*
 - Inventories and maps cloud assets
 - Detects cloud misconfigurations
 - Analyzes cloud security policies
 - Prioritizes remediation steps

Supports public cloud including, Microsoft Azure, AWS, and Google Cloud
- ✓ Holistic Threat Vulnerability Remediation Strategy
 - Drafts and adjusts IT strategy based on monthly external vulnerability scanning results
 - Drafts and adjusts IT strategy based on weekly internal vulnerability scanning results
 - Collaborates monthly on IT strategy for remediating external and internal vulnerabilities
 - Prioritizes remediation steps
- ✓ Prompt Remediation of Threat Vulnerabilities
 - Includes automatic vulnerability remediation* *Requires Centre Secure Managed Services agreement or billed separately at an hourly rate.*

Managed Vulnerability Scanning (MVS) Premier

Centre Partnership Value Add Services

Force multiplying risk management and remediation guidance with enhanced tracking, visibility, and consulting.

- ✓ Rigorous Vulnerability Prioritization
- ✓ Risk Remediation Guidance and Consulting
- ✓ Direct Access to Vulnerability Management Platform
- ✓ Tailored Vulnerability and Remediation Reporting (CMAC™ Security Dashboard)
- ✓ Quarterly Internal Vulnerability Reports
- ✓ Automatic End-to-End Threat Remediation and Verification*
Requires Centre Secure Managed Services agreement.

Summary of Services

MANAGED VULNERABILITY SCANNING (MVS)

Recurring security scanning of Individual workstations, servers, and network devices.

Enterprise-Grade Security Scanning

- ✓ Tailored Configurations
 - Builds virtual server (VM) in your environment
 - Configures Vulnerability Scanning application, including internal and external IP addresses
 - Performs pre-launch scanning tests across all connected endpoints, workstations, servers, and network devices
 - Schedules monthly scanning of all connected endpoints, workstations, servers, and network devices
- ✓ Process Automation
 - Monthly scheduled external scans
 - Continuous scheduled internal scans
 - On-demand scans as required or upon request

Risk Prioritization

- ✓ Prioritize Vulnerability Risks
 - Prioritized by greatest risk
 - Assets grouped and tracked

Vulnerability Reporting

- ✓ Comprehensive Threat Vulnerability Report
 - Access to Vulnerability Management Platform
 - Analyzes monthly internal vulnerability scanning results
 - Prepares internal vulnerability recommendations report

Managed Vulnerability Scanning (MVS) Basic

Centre Partnership Value Add Services

Force multiplying risk management and remediation guidance with enhanced tracking, visibility, and consulting.

- ✓ Rigorous Vulnerability Prioritization
- ✓ Risk Remediation Guidance and Consulting
- ✓ Tailored Vulnerability and Remediation Reporting (CMAC™ Security Dashboard)
- ✓ Quarterly Internal Vulnerability Reports
- ✓ Automatic End-to-End Threat Remediation and Verification*
Requires Centre Secure Managed Services agreement.

MANAGED VULNERABILITY SCANNING (MVS)

Recurring security scanning of Individual workstations, servers, and network devices.

Enterprise-Grade Security Scanning

- ✓ **Tailored Configurations**
 - Builds virtual server (VM) in your environment
 - Configures Vulnerability Scanning application, including internal and external IP addresses
 - Performs pre-launch scanning tests across all connected endpoints, workstations, servers, and network devices
 - Continuous scanning of all connected endpoints, workstations, servers, and network devices
- ✓ **Process Automation**
 - Continuous scheduled internal scans

Risk Prioritization

- ✓ **Prioritize Vulnerability Risks**
 - Prioritized by greatest risk
 - Assets grouped and tracked

Vulnerability Reporting

- ✓ **Comprehensive Threat Vulnerability Report**
 - Analyzes quarterly internal vulnerability scanning results
 - Prepares internal vulnerability recommendations report

Consulting and Remediation

- ✓ **Holistic Threat Vulnerability Remediation Strategy**
 - Drafts and adjusts IT strategy based on internal vulnerability scanning results
 - Collaborates quarterly on IT strategy for remediating external and internal vulnerabilities
 - Prioritizes remediation steps
- ✓ **Prompt Remediation of Threat Vulnerabilities**
 - Includes automatic vulnerability remediation* *Requires Centre Secure Managed Services agreement or billed separately at an hourly rate.*

**THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY
TIME WITHOUT NOTICE.**