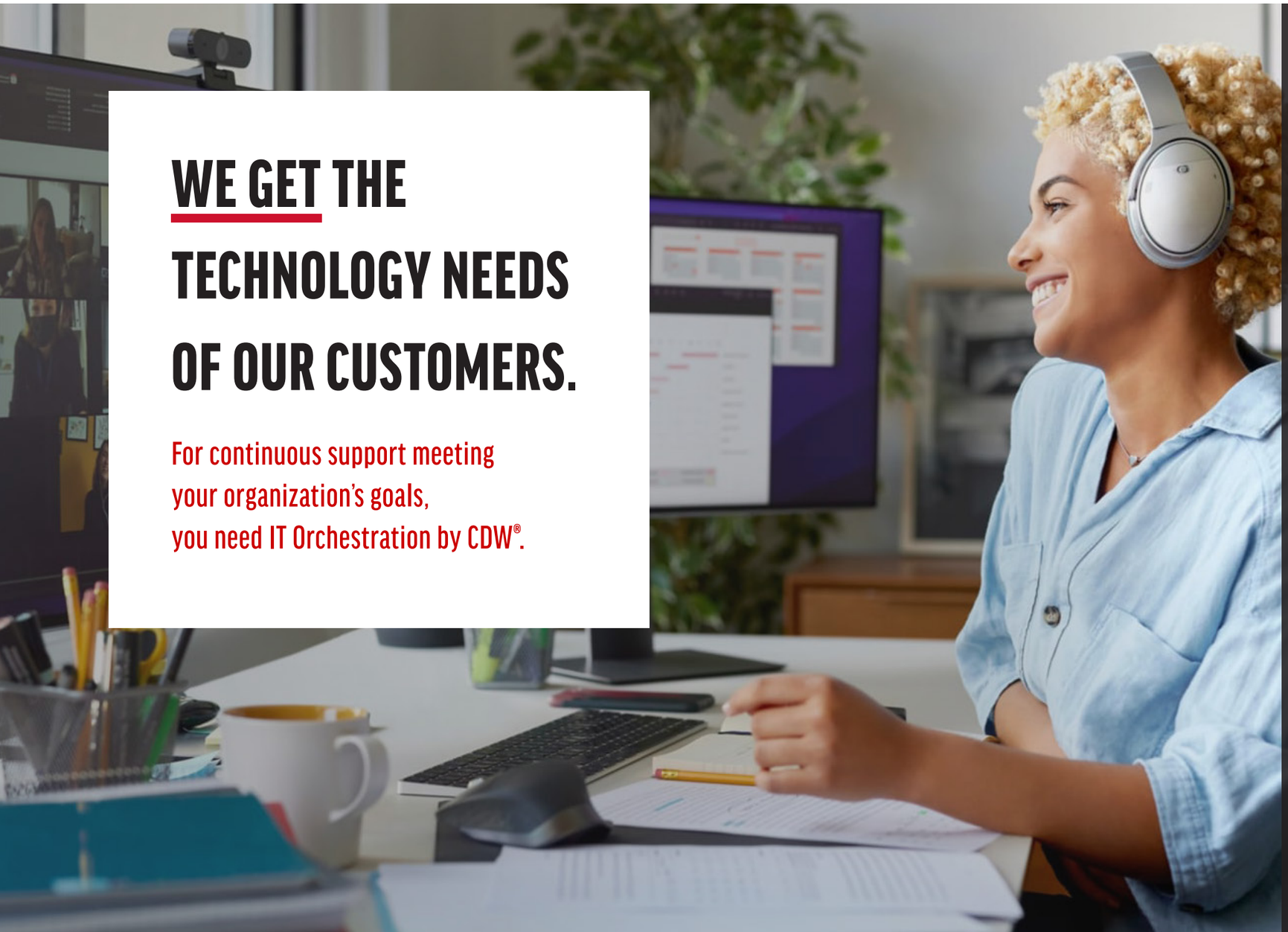


WE GET THE TECHNOLOGY NEEDS OF OUR CUSTOMERS.

For continuous support meeting your organization's goals, you need IT Orchestration by CDW®.

Modern organizations across all industries struggle to keep pace with the demands of a technology-focused, innovation-driven, digitally connected landscape.

IT teams grapple with legacy infrastructures and disparate platforms while being torn between handling day-to-day technology maintenance and driving company innovation.

Today's organizations need all the support they can get — by way of services that take the burden off IT staff, bolster growth and help organizations achieve their desired outcomes.

Technology Drives Organizational Outcomes

In today's competitive market, the speed of digital priorities is critical to success. Yet, technical complexities can slow progress. CDW's full-stack engineering services team focuses on digital transformation — from code and applications to cloud, data and security — to help you accelerate innovation, enhance customer experiences and optimize collaboration, all while delivering agility and cost efficiencies to your business.

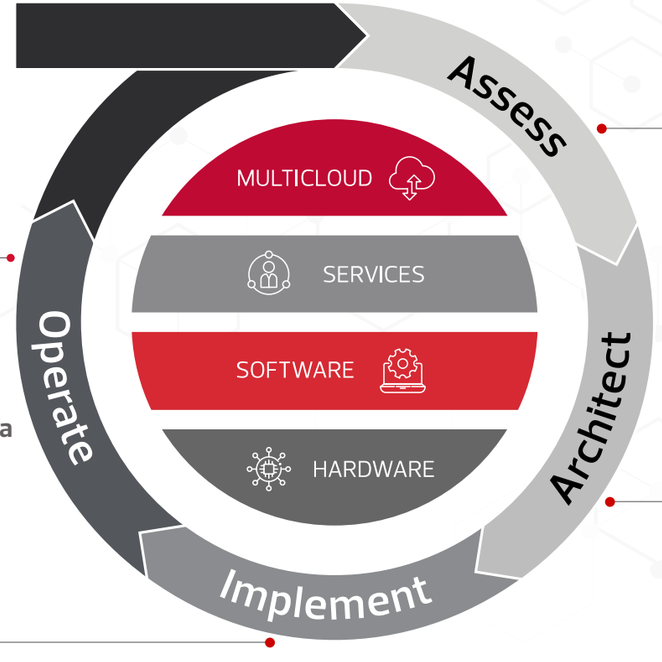
FULL STACK. FULL LIFECYCLE. FULL OUTCOMES.

Continuous Operations

- 24x7x365 Coverage

Proven Quality

- 3,000+ Certifications
- Nine locations across Canada
- International coverage



Trust at Scale

- 80+ Solution Architects
- 80+ Delivery consultants

Unmatched Expertise

- 20+ Years in the Canadian market
- 900+ Coworkers

Get More from Your Technology

We know IT. That's our business. When you partner with us, we take the extra load off your IT team. That way, they can focus on initiatives that turn IT into a competitive advantage while we help you maximize your IT investments and deliver real value for your customers. Our experts help you **assess, architect, implement and operate** your technology environment.

ASSESS

Our certified experts provide a suite of assessment services to help organizations understand their current level of maturity and plan steps to continue their journey towards an optimized hybrid cloud operating model. We focus on the following key areas of growth: portability, manageability, observability, resiliency and security.

ARCHITECT

We will help you build the plan to train your people, update your processes and implement technologies to accelerate your ability to handle the current and future technology needs. We take business goals and objectives and turn them into implementation plans and architectures that drive success for our customers.

IMPLEMENT

CDW Canada has a host of services to help customers train skills, change processes and implement technologies that deliver on business goals and objectives. From industry-leading professional services delivery consultants to staff augmentation services, CDW services provide what is needed to help customers be successful in their most complex projects.

OPERATE

Managed services are core to CDW Canada's ability to assist customers. More and more organizations are looking to consume "as a service" and our managed services SOC and NOC support customers with 24x7x365 coverage of their critical systems.

Infrastructure Services

CDW Canada's infrastructure services provide expertise, tools and resources to scale and future-proof your infrastructure. We help you upgrade your existing architecture and prepare for what's to come, whether you're on-premises, migrating to the cloud or already there.

PROFESSIONAL INFRASTRUCTURE SERVICES

As pressures mount for IT departments to deliver more services faster, infrastructures are being strained. Our experienced team of infrastructure professionals can help you discover hidden opportunities and navigate the solutions that best fit your environment.

[Explore Managed Infrastructure Services]

DATA CENTRE

- **Application Firewall**
  Deliver application firewall to allow only the authorized traffic. This is achieved via the advanced firewall manager (AFM) module.
  Supported Vendors: F5

- **Cloud Storage Deployment**
  Deploy and configure the services on the cloud as per the customer's requirement.
  Supported Vendors: AWS Data Sync, AWS FSx, Azure NetApp Files, Backup (DR), CVO, NetApp Cloud Sync and NetApp Cloud Manager

- **Cluster Switch Deployment/Upgrade**
  Upgrade the storage to switchless to the switched cluster with cluster interconnect switches. Upgrade the switch software and hardware.
  Supported Vendors: Broadcom

- **Data Centre Build and Migration**
  For large enterprises to migrate to future-proof data centre technologies such as ACI or NSX-T, we provide professional services to design/deploy and migrate seamlessly. For small-medium enterprises, we design and deploy a robust network with traditional equipment and technologies.
  Supported Vendors: Arista, Aruba, Cisco and VMware

- **DDOS Protection**
  Deliver Distributed Denial of Service (DDOS) Protection with the ASM module.
  Supported Vendors: F5

- **DNS Design and Implementation**
  BIG-IP DNS Design and implementation.
  Supported Vendors: F5

- **F5 as an Identity Provider (IdP)**
  Deliver the BIG-IP as an identity provider either for cloud or on-premise applications.
  Supported Vendors: F5

- **F5 as a Service Provider (SP)**
  Deliver the BIG-IP as service provider to get access to on-premise applications.
  Supported Vendors: F5

- **F5 QuickStart**
  BIG-IP cluster design and implementation (HA). Cloud-based or on-premise.
  Supported Vendors: F5

- **HCI Deployment**
  Multi-node cluster deployments, upgrades, virtual machine data migration and virtualization.
  Supported Vendors: Cisco UCS, FlexPod, NetApp and Nutanix

- **Kubernetes & Applications**
  Deploy and configure the Kubernetes cluster nodes and install the required application. Configure application data lifecycle management service for stateful applications using Astra.
  Supported Vendors: Astra, Google K8s and NetApp

- **LAN/WAN Network Refresh**
  Replacement of end-of-life devices with the latest devices. We have the expertise to work with any LAN/WAN vendor, and we are proficient in handling heterogeneous vendor environments.
  Supported Vendors: Aruba, Brocade, Cisco, Dell, Fortinet, HPe and Meraki

- **Load Balancer**
  Deliver virtual server to load balance and optimize user session over several backend servers.
  Supported Vendors: F5

- **Network Assessment**
  In-depth LAN/WAN network assessment with detailed report on pain-points, security concerns, configuration inconsistencies and recommendations.
  Supported Vendors: Arista, Aruba, Cisco, Dell, Fortinet, HPe and Meraki

- **Portal Deployment**
  Deliver a web portal where applications are available per active directory (AD) group membership.
  Supported Vendors: F5

- **SAN Switches Deployment**
  Fabric hardware and software deployments. SAN zoning and commissioning.
  Supported Vendors: Brocade and Cisco

- **SD-WAN Design and Deployment**
  Consulting, designing and deployment of SD-WAN solutions for small to large enterprises. This includes seamless integration with the existing network and migration to the new SD-WAN network with minimum downtime.
  Supported Vendors: Cisco, Fortinet, Meraki and Silver Peak

- **Secure Remote Desktop**
  Deliver secure remote desktop access via the application portfolio management (APM) portal.
  Supported Vendors: F5

- **Secure VDI Access**
  Deliver secure VDI access via the APM Portal.
  Supported Vendors: F5

- **Storage Assessments**
  Analyze storage capacity utilization, performance, quality of service (QoS), health and generate reports with recommendations.
  Supported Vendors: HPe, NetApp and Nutanix

- **Storage Automation (Ansible)**
  Automate the complex storage tasks using Ansible Automation.
  Supported Vendors: NetApp

- **Storage Data Migration**
  Data migration from various platforms to NetApp, Nutanix, HPE, Cisco UCS and cloud.
  Supported Vendors: AWS, Azure, HPe, NetApp and Nutanix

- **Storage Deployments**
  Storage hardware and software cluster deployments, upgrade/downgrade, decommissioning, data protection, consolidation and virtualization.
  Supported Vendors: HPE and NetApp

- **Storage Upgrade and Consolidation**
  Add nodes and disk shelves to the cluster and eject the end of life (EOL) hardware.
  Supported Vendors: HPE, NetApp and Nutanix

- **Virtual Desktop Solutions**
  New Horizon deployments, upgrades to existing deployments and health assessments.
  Supported Vendors: VMware Horizon/View

- **VMware Cloud on AWS**
  New deployments on AWS, VM migration to/from and VMC cloud optimization.
  Supported Vendors: AWS and VMware

- **VMware Network Virtualization**
  VMware NSX Data Centre is the network virtualization and security platform that enables the virtual cloud network, a software-defined approach to networking that extends across data centres, clouds, endpoints and more.
  Supported Vendors: VMware

- **vSphere Health Assessment**
  The health assessment covers the network, storage connectivity, ESXi servers and vCenter health.
  Supported Vendors: VMware

- **VxRail**
  Deploy new VxRail appliances, upgrade existing appliances, scale up or out of hardware.
  Supported Vendors: Dell and VMware

- **WAF Protection**
  Deliver WAF policy to protect applications against malicious requests.
  Supported Vendors: F5

- **Wireless LAN Deployment**
  Design and deployment of greenfield or brownfield Wireless LAN deployment for small to large enterprises.
  Supported Vendors: Aruba, Cisco and Meraki

- **Wireless Site Survey**
  Our wireless site surveys will provide critical data for successful Wi-Fi deployment planning and troubleshooting, allowing you to focus on business outcomes rather than infrastructure complexities.
  Supported Vendors: Aruba, Cisco and Wi-Fi 6

DATA PROTECTION

- **Backup Data Migration to Cloud**
  Moving backup data to the cloud has been the prime use case for utilizing cloud resources. More and more companies are replacing aging tape and disk storage for cloud storage. CDW can assess the customer's needs and implement a solution that best suits their requirements.
  Supported Vendors: Commvault, Dell and Veeam

- **Backup Environment Migration to Cloud**
  The reduction of on-premise resources is high on most customers' priority lists. Many customers are looking at migrating the backup environment to the cloud and keeping fewer resources on-premise. CDW can assess the environment and the customers' needs to architect a solution that will utilize cloud resources to protect backup data.
  Supported Vendors: Commvault, Dell and Veeam

- **Commvault Backup for AWS**
  CDW-certified consultants can implement protection for AWS workloads like EC2 and EKS, platfrom as a service (PaaS) databases like RDS and DocumentDB. Commvault's Live Sync can replicate from VMware and Hyper-V to AWS, from AWS to VMware and Hyper-V and Azure. CDW-certified consultants can architect and implement a solution to meet any and all needs of a customer.
  Supported Vendors: AWS and Commvault

- **Commvault Backup for Azure**
  CDW-certified consultants can implement protection for Azure workloads, PaaS databases, SAP Hana on Azure and SQL utilizing Commvault. Commvault's Live Sync can replicate from Vmware and Hyper-V to Azure, from Azure to VMware and Hyper-V and AWS. CDW-certified consultants can architect and implement a solution to meet any and all needs of a customer.
  Supported Vendors: Azure and Commvault

- **Commvault Backup Software Implementation**
  Enhanced implementation services of Commvault backup environments using Commvault's best practices and CDW's certified implementation consultants. During Implementation, CDW will assess the requirements, architect the environment and implement the solution to meet the service-level agreement's auditory requirements and reduce data loss.
  Supported Vendors: Commvault

- **Commvault Hyperscale Appliance**
  Commvault Hyperscale is Commvault's approach to a scale-out solution for backup data storage. CDW can implement these backup devices into the production data centre or in remote locations as a single storage and compute solution for any environment to meet high resiliency and performance requirements.
  Supported Vendors: Commvault

- **Commvault VM Migration to Cloud**
  Customers need a safe method to migrate on-premise workloads to the cloud. CDW can utilize Commvault to first protect all the production workloads, then copy that data to the cloud and replicate the workloads into the Cloud platform workload. Commvault will replicate daily changes until ready for failover. When ready to cut over to the cloud, run the failover feature to shut down on-premise workloads and spin up the cloud workloads.
  Supported Vendors: Commvault

- **Data Domain Implementation**
  Dell Data Domain is a highly scalable data deduplication device for backup storage and can be scaled to cloud storage using a DDVE. CDW-certified consultants can architect and implement the storage device into any backup software to meet customer requirements.
  Supported Vendors: Dell

- **Data Protection Assessment**
  Provide a configuration and operational assessment of the customer's existing data protection environment. This assessment will be based on industry best practices with a configuration summary and remediation recommendations provided as the project deliverables.
  Supported Vendors: All vendors

- **Data Protection Platform Strategy Analysis**
  Inspect and assess the current data protection environment and IT roadmap plans to determine a strategy around which products and architectures would best align with their requirements.
  Supported Vendors: All vendors

- **Dell Backup for Azure**
  The Dell IDPA is a single management interface to backup all types of workloads, including on-premises, Azure and AWS workloads. CDW can introduce this cost-effective appliance into the environment seamlessly to manage all their needs in the cloud to backup PaaS and IaaS workloads. CDW's certified consultants can architect and implement the solution to protect these workloads.
  Supported Vendors: Dell

- **Dell Backup Software Implementation**
  Enhanced implementation services of Dell backup environments using Dell's best practices and CDW's certified implementation consultants. During Implementation, CDW will assess the requirements, architect the environment and implement the solution to meet the service-level agreement's auditory requirements and reduce data loss.
  Supported Vendors: Dell (IDPA, Avamar, Networker and PowerProtect)

- **DR Readiness Assessment**
  The DR Assessment is used to assess the customer's overall disaster recovery (DR) readiness and make recommendations for the improvement of their disaster recovery capabilities.
  Supported Vendors: All vendors

- **DR Replication**
  CDW's certified data protection consultants can implement a DR solution to meet customer needs to either a secondary location or to the cloud. Many customers have been replacing older physical DR sites with cloud DR sites to reduce costs.
  Supported Vendors: Commvault, Dell and Veeam

- **Environment Hardware Upgrades**
  Backup infrastructure hardware should be replaced when warranty terms expire to reduce maintenance costs and keep the hardware in good working condition. CDW data protection consultants can assist in decommissioning older hardware and replace with newer.
  Supported Vendors: Commvault, DELL and Veeam

- **Environment Software Upgrades**
  Backup environments should be upgraded on a regular basis with the latest security and operational enhancements. CDW's certified consultants can upgrade environments to meet customer requirements.
  Supported Vendors: Commvault, Dell and Veeam

- **ExaGrid Implementation**
  ExaGrid's tiered backup storage appliance is a highly scale-out alternative for backup storage that utilizes a landing zone for new backup data and an air-gapped long-term retention repository to protect data. ExaGrid can be used with any backup software and can be implemented by our trained CDW consultants.
  Supported Vendors: ExaGrid

- **IDPA Implementation**
  Dell IDPA is an all-in-one backup appliance delivering powerful, enterprise-grade data protection capabilities for any size environment. CDW's trained and certified consultants can implement these solutions into any environment to protect the required workloads.
  Supported Vendors: DELL

- **Office 365 Protection**
  With the Office 365 shared responsibility model, the customer is responsible for protecting their production data. CDW's certified consultants can architect and implement a solution to keep a secondary backup copy of the customer's SharePoint, Teams, OneDrive and O365 Mail data to meet the customer's auditory and retention requirements.
  Supported Vendors: Commvault, DELL, Metallic and Veeam

- **Remediation Efforts**
  In every environment, issues exist that might interfere with regular backup operations and can jeopardize important data protection service-level agreements and regulatory requirements. Our fully-certified consultants can assist in correcting issues within the environment.
  Supported Vendors: Commvault, Dell, IBM, Veeam and Veritas

- **Storage Level Integration (Snapshot)**
  Storage level snapshots can assist in reducing backup windows with the increasing sizes of backups. Backup software can manage snapshots, catalogue the backup data and copy backup data from the storage to secondary locations. CDW can implement snapshots for most of the storage vendors bringing backup times down to minutes from hours.
  Supported Vendors: Commvault, Dell and Veeam

- **Tape Library Implementation**
  Tape libraries are still being used in many customer environments and require replacement after warranty and maintenance periods end. CDW has vast experience using tape libraries and can implement new libraries and migrate data if required from older tape to a new tape. Our certified consultant can rack, install, upgrade and configure any backup software that the customer is utilizing today.
  Supported Vendors: Dell, HP, IBM and Quantum

- **Veeam Backup**
  CDW's certified consultants can implement Veeam Backup for AWS or Azure to protect workloads utilizing cloud storage. To do so, the consultant will gather information and requirements, implement the solution, test backups and restores and document the outcome of the project.
  Supported Vendors: AWS, Azure and Veeam

- **Veeam Backup Software Implementation**
  Enhanced implementation services of Veeam backup environments using Veeam's best practices and CDW's certified implementation consultants. During Implementation, CDW will assess the requirements, architect the environment and implement the solution to meet service-level agreements' auditory requirements and reduce data loss.
  Supported Vendors: Veeam

- **Veeam Hardened Repository – Immutability**
  Protecting backup storage is as important as protecting production data. A Veeam hardened repository protects Veeam backup data by creating that unchangeable and undeletable safe copy to eliminate the chances of ransomware encrypting the backup data. CDW can implement the Veeam hardened repository and add it to the backup infrastructure.
  Supported Vendors: Veeam

- **Veeam SOBR Implementation**
  A scale out backup repository (SOBR) consists of one or more backup repositories called a performance tier and capacity tier. CDW is seeing the uptick in implementation of Veeam SOBR to assist with growing backup data sizes and to start using object storage for longer-term data. CDW can architect and implement a SOBR to replace older configurations to meet capacity requirements on-premises and the cloud.
  Supported Vendors: Veeam

- **Veritas Backup Software Implementation**
  Enhanced implementation services of Veritas backup environments using Veritas's best practices and CDW's certified implementation consultants. During Implementation, CDW will assess the requirements, architect the environment and implement the solution to meet the service-level agreement's auditory requirements and reduce data loss.
  Supported Vendors: Veritas (NetBackup and Backup Exec)

- **VMWARE CLOUD (VMC) DEPLOYMENT**
  Installation and configuration of the following VMware applications: VMware Cloud and VMware HCX.
  Supported Vendors: AWS and VMware

- **VMWARE CLOUD (VMC) WITH VCDR DEPLOYMENT**
  Installation and configuration of VMware Cloud with VMware Cloud disaster recovery (VCDR) in the customer´s environment.
  Supported Vendors: AWS and VMware

MANAGED INFRASTRUCTURE SERVICES

Spend less time updating and maintaining systems and more time delivering business value. Get better performance and less downtime with CDW Canada's managed infrastructure services.

- **Cisco Meraki Managed Services**

  At CDW Canada, we get that networking across the hybrid cloud is critical for your business to operate effectively. With Cisco Meraki Managed Services by CDW, you can rely on best-in-class IT experts to monitor, manage and update your Cisco Meraki deployments: from wireless access points to MX security appliances.
  Supported Vendors: Cisco Meraki

- **Data Protection**

  A team of vendor-neutral solution architects at CDW Canada can assess your environment technically and position the best data protection solution that fits your business.
  Supported Vendors: Commvault, Veeam, VMWare and Zerto

  - **Backup as a Service (BaaS)**

    CDW's Backup as a Service (BaaS) allows your business to tap into resources and tooling that will help bring awareness and a sense of comfort to the company. Your IT teams can focus on providing value in other areas and feel confident that CDW is managing your backup environment.
    Supported Vendors: Commvault, Veeam, VMWare and Zerto

  - **Disaster Recovery as a Service (DRaaS)**
    CDW's Disaster Recover as a Service (DRaaS) allows your business to tap into resources and tooling that will help bring awareness and a sense of comfort to the company. Your IT teams can focus on providing value in other areas and feel confident that CDW is managing replication into your DR environment.
    Supported Vendors: Azure, Commvault and Zerto

- **Hosted Backup**
  For those organizations who currently utilize Commvault technology for their backups, CDW offers a hosted backup solution which provides a turn-key Commvault CommCell to either augment their current backup capacity or act as an offsite copy as an alternative to aging tape technology.
  Supported Vendors: Commvault

- **Managed Compute**
  CDW's Managed Compute: Hypervisor service allows your business to tap into resources and tooling that will help bring awareness and a sense of comfort to the company. Your IT teams can focus on providing value in other areas and feel confident that CDW is managing your hypervisor environment.
  Supported Vendors: Cisco, Dell, HPe, Hypervisor, Microsoft and RedHat

- **Managed Network Switching**

  Supported: Cisco, Meraki, F5
  The managed network service provides the day-to-day management of networking devices for customers. CDW provides the expertise and knowledge to provide monitoring/alerting, device administration and general capacity management for systems in scope.
  Supported Vendors: Aruba, Cisco, Fortinet, HPE and Meraki

  - **Managed F5**
    Managed F5 service allows your business to tap into resources and tooling that will help bring awareness and a sense of comfort to the business. Your IT teams can focus on providing value in other areas and feel confident that CDW is managing your F5 environment.
    Supported modules: base platform plus LTM, DNS (GTM), ASM and APM

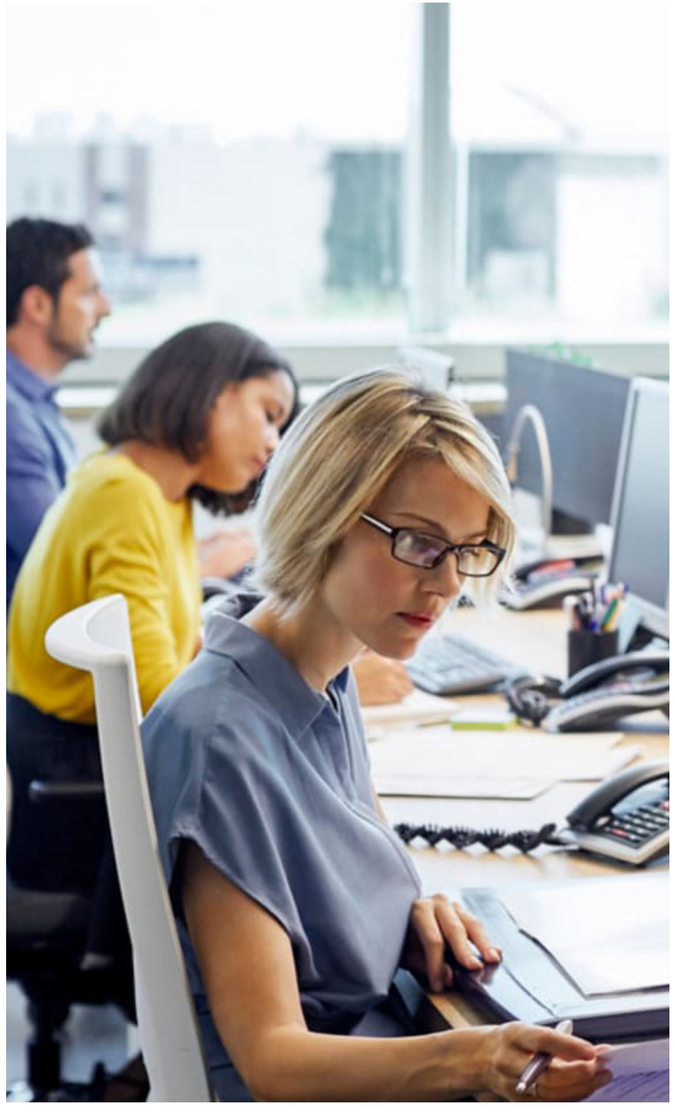
- **Managed SD-WAN**
  Let your internal IT teams focus on business performance while CDW's experts provide the day-to-day management of your SD-WAN devices.
  Supported Vendors: Cisco Meraki, Fortinet and Palo Alto

- **Managed Storage**
  The Managed Storage service provides the day-to-day management of storage devices for customers. CDW delivers the expertise and knowledge to provide monitoring/alerting, device administration and general capacity management for storage devices.
  Supported Vendors: Dell, EMC, HPE Nimble and NetApp

- **Monitoring as a Service**
  Monitoring as a Service is a base-level monitoring for a technology (networks, servers, virtual machines, extra) that provides customer notifications. CDW operates the monitoring system infrastructure on behalf of the customer but does not investigate the underlying cause of events or alarms. CDW delivers notifications to the customer for the customer's operations teams to handle.

- **Server Patch Management**
  In today's IT landscape, it's not unusual for system administrators to be under pressure to continuously deliver added value for the business. The reality is that systems may become vulnerable because of competing priorities. CDW can work with your administrators to provide a patching service to ensure your systems stay up to date and reduce the risk to your business.
  Supported Vendors: Microsoft, Red Hat Linux and CentOS

- **Site Recovery Manager**
  For VMware clients, CDW offers VMware Site Recovery Manager, which provides a fully integrated and automated offsite replication of the virtual infrastructure in the cloud.
  Supported Vendors: VMWare



Cloud Services

The added complexities of ever-evolving public and multi-cloud environments make careful planning and skilled management a must. CDW helps you design and augment your cloud capabilities, build your platform to your exact specifications and manage your cloud environment efficiently, securely and transparently.

PROFESSIONAL CLOUD SERVICES

CDW Canada partners with you on the journey by carefully considering your business objectives in light of proven cloud technologies that can deliver real business value. We can help you forge a clear path to upgrading, upskilling and filling skills gaps as you navigate the cloud journey. If you're already in the cloud, CDW Canada can help you develop a business-focused cloud strategy to help you get more value out of your cloud investment.
[Explore Managed Cloud Services]

AWS

- **Cloud Cost optimization**
  CDW's cloud experts help you optimize your cloud costs by evaluating your organization's cloud infrastructure, usage patterns and expenditure to identify cost-saving opportunities and provide actionable recommendations, best practices and strategies to reduce unnecessary spending and maximize cost efficiency.
  Supported Vendors: AWS

- **Cloud Penetration Testing**
  CDW's Cloud Penetration Testing Service is used to discover, identify and classify potential deficiencies and vulnerabilities in organizations' cloud environments; and help assess the related security posture. CDW's Cybersecurity consultants would attempt to identify and exploit vulnerabilities to simulate a malicious actor, and then provide recommendations to remediate issues.
  Supported Vendors: AWS

- **Licensing Evaluation and Discovery Service Assessment (LEADS)**
  CDW's Licensing Evaluation and Discovery Service (LEADS) enables businesses to assess and optimize current on-premises and cloud environments based on actual resources and utilization and third-party licensing. It has three key focus areas: identify legacy licensing savings, technical performance assessment and LEADS assessment results.
  Supported Vendors: AWS

MICROSOFT SERVICES

- **Architecture and Deployment Expertise With Azure Compute, Network, Load Balancers, Databases**
  Provide guidance for designing and building solutions on Azure using best practices and architecture. Design forward-thinking, flexible environments that allow businesses to move their workloads to the cloud and onboard the latest technologies and services to streamline availability and delivery.

- **Azure AD Identity Protection**
  Identity protection accomplishes automating the detection and remediation of identity-based risks, investigation of risks and exporting risk detection data to other tools.

- **Azure Firewall**
  Azure Firewall is a cloud-native and intelligent network firewall security service that provides threat protection for your cloud workloads running in Azure. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

- **Azure Security Assessment**
  Assess and ensure that Azure cloud security best practices are being met or exceeded. Review existing deployments and provide recommendations based on feedback from consultants experienced in the field.

- **Business Process Automation: Power Apps, Power Automate Flow and Azure Logic Apps**
  Assess your security and compliance posture within your Microsoft 365 environment to align with Microsoft's recommended best practices. We provide a report of the current state of your tenant with a prioritized list of actionable recommendations to help you identify and fix potential security issues in your environment.

- **File Services Migration**
  Migration from on-prem to SharePoint and/or OneDrive.

- **MCI Workshops**

  - **Azure Defender for Cloud (formerly "Security Centre")**
    Microsoft Defender for Cloud is a cloud security posture management (CSPM) and cloud workload protection platform (CWPP) for all of your Azure, on-premises and multi-cloud (Amazon AWS and Google GCP) resources. Defender for cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises: continually assess, secure and defend.

  - **Azure Security and Governance Workshops**
    Help customers learn how to maximize the value of Teams by integrating apps and workflows tailored to their business needs. Customers receive a report with actionable recommendations to drive deployment and next steps.

  - **Collaborative Apps (formerly Teams Apps & Solutions)**
    Work through various frontline worker challenges and pain points to identify top prioritized scenarios for customers' frontline workforce. Customers receive a report with actionable recommendations to drive deployment and next steps.

  - **Defend Against Threats with SIEM Plus XDR (formerly Threat Protection)**
    Understanding customers' security goals and objectives, then identifying real security threats across email, identity and data within their production environment to showcase the Microsoft Sentinel and Microsoft 365 Defender experience. Customers receive a report with actionable recommendations to drive deployment and next steps.

  - **Enable Frontline**
    Showcase the value of Microsoft Endpoint Manager to show customers how to manage users' devices, apps and identities from anywhere. Customers receive a report with actionable recommendations to drive deployment and next steps.

  - **Endpoint Management**
    Showcase the art of the possible for Microsoft Teams hybrid meeting and meeting room experiences that empower people to work from anywhere, at any time. Customers receive a report with actionable recommendations to drive deployment and next steps.

  - **Hybrid Meetings and Rooms (Formerly Hybrid Meetings)**
    Help customers at the early stage of their cloud transformations envision agile work scenarios and how to enable their employees to be productive and secure with Microsoft 365. Customers receive a report with actionable recommendations to drive deployment and next steps.

  - **Microsoft 365 Digital Workforce (Formerly Transition to Cloud)**
    Discover customers' unique business scenarios, showcase employee experience transformationn and demonstrate the "Art of the Possible" across the Viva suite with Topics, Connections or Learning. Customers receive a report with actionable recommendations to drive deployment and next steps.

  - **Microsoft Sentinel**
    Demonstrate how Microsoft Sentinel helps organizations use intelligent security analytics and threat intelligence to detect and quickly stop active threats.

  - **Microsoft Viva**
    Help customers discover how Microsoft Viva Insights helps individuals, managers and leaders gain personalized insights and actionable recommendations that help everyone in an organization thrive. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **MCI Workshops**
  - **Microsoft Viva Insights**
    Help customers evaluate their current telephony and PBX needs, then demonstrate the end-to-end Microsoft Teams calling experience to showcase Microsoft Teams Phone as a telephony solution. Customers receive a report with actionable recommendations to drive deployment and next steps.
  - **Mitigate Compliance and Privacy Risks (Formerly Manage and Investigate Risk)**
    Demonstrate how Microsoft Purview helps customers detect, investigate and take action to mitigate risk and ensure compliance in their modern workplace. Customers receive a report with actionable recommendations to drive deployment and next steps.
  - **Modernize Communications**
    Gain visibility into the customers' hybrid work end-user computing goals, and demonstrate Windows 11, Windows 365 and Azure Virtual Desktop solutions that provide a secure desktop experience from virtually anywhere.
  - **Next-Gen Windows (Formerly Next-Gen Endpoints)**
    Customers receive a report with actionable recommendations to drive deployment and next steps.
  - **Protect and Govern Sensitive Data (Formerly Discover Sensitive Data)**
    Help customers understand, manage and mitigate hidden privacy and regulatory risks within their own environment with Microsoft Purview. Customers receive a report with actionable recommendations to drive deployment and next steps.
  - **Secure Identities and Access (Formerly Securing Identities)**
    Help customers find and mitigate identity risks and safeguard their organization with a seamless identity solution. Customers receive a report with actionable recommendations to drive deployment and next steps.
  - **Secure Multi-Cloud Environments (Formerly Hybrid Cloud Security)**
    Help customers identify current, ongoing risks to their cloud environment using Microsoft Defender for Cloud and Azure Network Security to define the next steps to accelerate their security journey. Customers receive a report with actionable recommendations to drive deployment and next steps.
  - **Microsoft Defender for Endpoint, Office 365 and Identity Protection**
    Help customers manage their on-prem devices. Operating system (OS) and application deployment, updates, patching, policy layering and enforcement, remediation and reporting. Co-management with Intune and 365 Endpoint Manager are also available.
  - **Microsoft Intune/Mobile Device Management**
    This platform helps customers manage, analyze, automate and understand their data and utilize it in a way to accelerate their business goals.
  - **Microsoft Teams Deployment**
    Migrate files off your network file server into SharePoint Online and OneDrive for Business inside secure cloud storage hosted by Microsoft to gain access to your files from any device with an internet connection inside and outside your corporate network without needing a VPN.
  - **Microsoft Teams Voice – Cloud VoIP**
    Deploy Microsoft Teams to work with teammates via secure workspace chat, videoconferencing meetings, document collaboration, built-in cloud storage and application integration.

- **Microsoft Viva: Viva Topics, Viva Insights, Viva Connections and Viva Learning**
  Bring your phone system to the cloud with Teams Voice, adding phone system calling capabilities to modern collaboration software, allowing organizations to have auto attendants, call queues and conference numbers.

- **Microsoft/Office 365 Best Practice Assessments**
  Have a CDW delivery engineer consultant assess your Microsoft 365 environment to ensure your Teams, SharePoint, OneDrive and basic Microsoft 365 Admin Centre controls, policies and settings are configured to align with Microsoft's recommended best practices. We provide a report of the current state of your tenant with a prioritized list of actionable recommendations to help you identify and fix potential issues in your environment.

- **Microsoft/Office 365 Migration: Exchange, SharePoint, OneDrive, Lync/SFB to Teams**
  Migrate your on-premises mail, files and instant message chats into Microsoft 365 to unlock the power of cloud-based applications and services with anywhere, any device access.

- **Multi-Factor Authentication (MFA)/Conditional Access**
  Tighten your security to protect your organization's assets by implementing multi-factor authentication to require people to verify their identity using more than a password before accessing your environment. Use conditional access policies to apply the right access controls when needed to keep your organization secure.

- **SCCM/Microsoft Endpoint Manager**
  The Microsoft Power Platform is a powerful set of applications that allow a customer to automate processes, build solutions, analyze data and create virtual agents.

- **SharePoint/OneDrive Implementation**
  Deploy the Microsoft Viva suite modules within Microsoft Teams to improve employee wellbeing with Viva Insights, engage and inform employees with personalized content in Viva Connections, create a knowledge management system that connects, manages and protects knowledge and expertise with Viva Topics, and create a centre for learning where employees can discover, share, recommend and learn with Viva Learning.

- **Solution Assessment – Cloud Security Assessment**
  Assess your security posture within your cloud environment to align with a prioritized list of actionable recommendations to help you identify and resolve potential security risks.

- **Windows Hello for Business**
  Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

MULTICLOUD SERVICES

- **Automation QuickStart**
  A simplified approach to automating a workload. Designed to focus on a pre-determined workload and leverage modern automation principles to quickly and easily set up a fully automated solution in the cloud.
  Supported Vendors: Azure

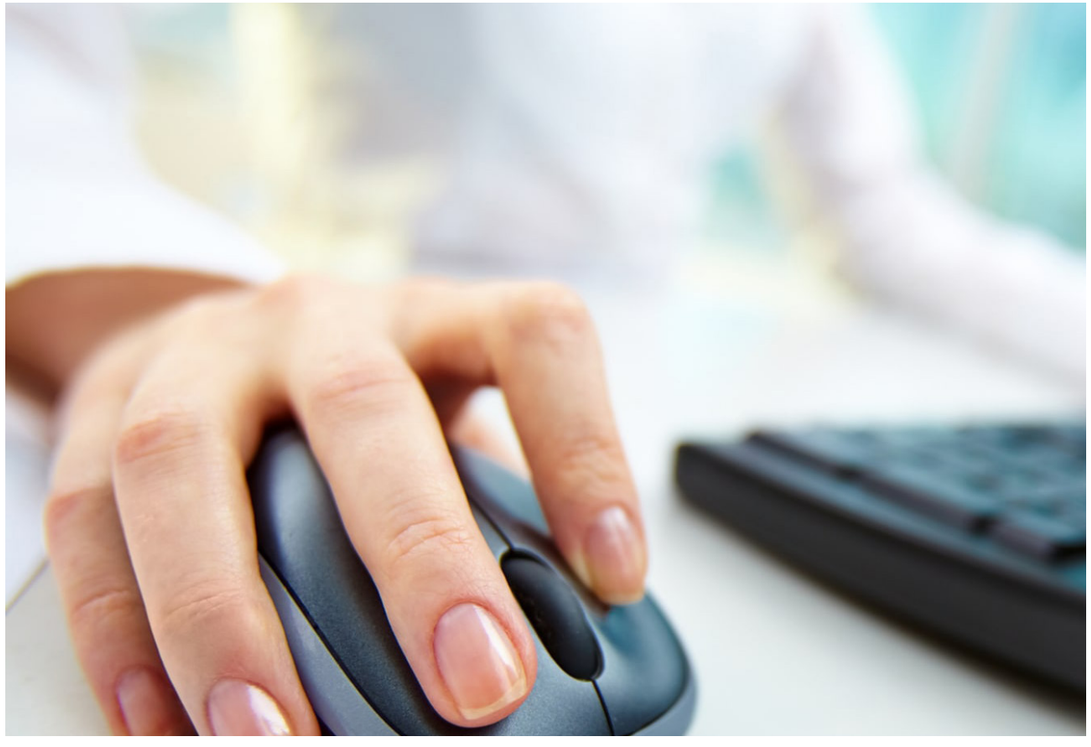
- **CIS – Best Practice Assessment**
  In-depth review of the customer's current cloud environment to ensure it meets well-architected framework requirements. Recommendations are provided for remediation.
  Supported Vendors: AWS and Azure

- **Cloud Community**
  Leverage CDW's international business while keeping your network and data here in Canada, with services such as unified communications as a service (UCaaS), backup as a service (BUaaS), disaster recovery as a service (DRaaS) and connectivity.
  Supported Vendors: 8x8, Convergia and RingCentral

- **Cloud Disaster Recovery (DRaaS)**
  Deploy, adopt and integrate data protection in the public cloud securely. Scale where needed, as well as keep you informed of any changes and help you maximize the ROI on your cloud investments and achieve your business outcomes faster.
  Supported Vendors: AWS, Azure and Commvault

- **Cloud Landing Zone**
  Professional services engagement to build out the foundational requirements and services of a cloud environment. These foundational services ensure the customer is set up for success in future growth and operations of the cloud.
  Supported Vendors: AWS and Azure

- **Cloud Migration QuickStart**
  A programmatic engagement designed to quickly and easily assist customers with their cloud migration.
  Supported Vendors: AWS and Azure



- **Cloud Readiness Assessment**
  In-depth review of the technical and business factors that will impact a workload's readiness for public cloud. Provides customers with the financial and technical analysis of each workload and the recommended future state that will meet the customer's requirements.
  Supported Vendors: AWS and Microsoft

- **Database Migration Assessment**
  Assessment of the existing data on-premise to migrate into the cloud (examples of data types will be SQL, MySQL).
  Supported Vendors: AWS and Azure

- **Email Migration Microsoft Office 365**
  Assessment and implementation on-premise Google to O365.
  Supported Vendors: Microsoft

- **Microsoft 365 Business Voice Remote Jumpstart**
  Basic deployment of Business Voice using Microsoft Teams.
  Supported Vendors: Microsoft

- **Microsoft 365 Security Workshop**
  Enablement workshop to make sure the client is choosing the correct products to implement into O365 (e.g., Microsoft defender for O365).
  Supported Vendors: Microsoft

- **Microsoft Azure + Veeam (Solutions for the Always-on Enterprise)**
  Design and deployment of a solution focused on assisting customers in effectively operating a multi-cloud environment. This engagement will allow customers to automate service deployment, leverage cost management tool and govern security/compliance from a centralized group.
  Supported Vendors: Azure and Veeam

- **Microsoft Azure Jumpstart**
  Create are basic landing zone for both AWS and Azure.
  Supported Vendors: AWS and Azure

- **Microsoft Teams Meetings Readiness**
  Assessment of the client's environment to define if Microsoft Teams can be adopted.
  Supported Vendors: Microsoft

- **Veeam QuickStart**
  An assessment of the customer's current environment, architect, install and configure components of the Veeam Availability Suite, including Veeam backup and recovery and Veeam One Server.
  Supported Vendors: Veeam

- **Virtual Desktop Pilot**
  Pilot and Enterprise Production deployment of Azure Virtual Desktop (AVD). .
  Supported Vendors: Microsoft

- **Well-Architected Framework**
  The well-architected review is a systematic approach to evaluating cloud architectures and can help you identify and fix potential issues with your environment.
  Supported Vendors: AWS and Amazon

- **Voice and Meeting With Adoption**
  Assess existing environment to move to Microsoft Teams adoption.
  Supported Vendors: Microsoft

- **Windows Autopilot Assessment (Intune)**
  Provides the ability to automate the onboarding and customization of a device that is shipped directly to the end user.
  Supported Vendors: Microsoft

- **Windows Autopilot Assessment and Pre-provisioning with Intune**
  Intune assessment to make sure clients are ready for white-glove services.
  Supported Vendors: Microsoft

MANAGED CLOUD SERVICES

As cloud environments become more complex, you need the right service provider with the skills and experience to take your cloud-based applications and services to the next level. CDW has years of experience managing cloud platforms and providing our customers with the insight, support and cloud know-how you need to keep ahead of the market. Reach your account team to discuss how CDW can help you achieve your business goals in the cloud.

- **Managed AWS**
  Growth in cloud-based services and infrastructure means organizations are finding it harder to manage technology complexity. CDW will help you adopt and integrate AWS securely, provide ongoing support, or we can manage the environment for you. CDW can help you scale where needed, as well as keep you informed of any changes and help you maximize the ROI on your AWS investments and achieve your business outcomes faster.

- **Managed Azure**
  Managing an ever-evolving cloud environment requires specialized skills — especially when production or business-critical systems must remain online without disruption. Our comprehensive next-generation managed services for Azure is backed by more than 20 years of managed services support experience. Enlisting CDW, a proven and trusted partner, can make keeping your organization operating optimally more accessible.

Digital Workspace Services

At CDW, we can help you leverage technology to empower your employees, serve your customers and create exceptional experiences. Explore our digital workspace solutions that go from endpoint to workspace to productivity and collaboration.

- **Business Process Automation: Power Apps, Power Automate Flow and Azure Logics Apps**
  Assess your security and compliance posture within your Microsoft 365 environment to align with Microsoft's recommended best practices. We provide a report of the current state of your tenant with a prioritized list of actionable recommendations to help you identify and fix potential security issues in your environment.

- **Email Migration Microsoft Office 365**
  Assessment and implementation on-premise Google to O365.

MCI WORKSHOPS

- **Azure Defender for Cloud (formerly "Security Centre")**
  Microsoft Defender for Cloud is a cloud security posture management (CSPM) and cloud workload protection platform (CWPP) for all of your Azure, on-premises and multi-cloud (Amazon AWS and Google GCP) resources. Defender for cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises: continually assess, secure and defend.

- **Azure Security and Governance Workshops**
  Help customers learn how to maximize the value of Teams by integrating apps and workflows tailored to their business needs. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Collaborative Apps (formerly Teams Apps & Solutions)**
  Work through various frontline worker challenges and pain points to identify top prioritized scenarios for customers' frontline workforce. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Defend Against Threats with SIEM Plus XDR (formerly Threat Protection)**
  Understanding customers' security goals and objectives, then identifying real security threats across email, identity and data within their production environment to showcase the Microsoft Sentinel and Microsoft 365 Defender experience. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Enable Frontline**
  Showcase the value of Microsoft Endpoint Manager to show customers how to manage users' devices, apps and identities from anywhere. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Endpoint Management**
  Showcase the art of the possible for Microsoft Teams hybrid meeting and meeting room experiences that empower people to work from anywhere, at any time. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Hybrid Meetings and Rooms (Formerly Hybrid Meetings)**
  Help customers at the early stage of their cloud transformations envision agile work scenarios and how to enable their employees to be productive and secure with Microsoft 365. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Microsoft 365 Digital Workforce (Formerly Transition to Cloud)**
  Discover customers' unique business scenarios, showcase employee experience transformation and demonstrate the "Art of the Possible" across the Viva suite with Topics, Connections, or Learning. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Microsoft Viva**
  Help customers discover how Microsoft Viva Insights helps individuals, managers and leaders gain personalized insights and actionable recommendations that help everyone in an organization thrive. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Microsoft Viva Insights**
  Help customers evaluate their current telephony and PBX needs, then demonstrate the end-to-end Microsoft Teams calling experience to showcase Microsoft Teams Phone as a telephony solution. Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Modernize Communications**
  Gain visibility into the customers' hybrid work end-user computing goals, and demonstrate Windows 11, Windows 365 and Azure Virtual Desktop solutions that provide a secure desktop experience from virtually anywhere.

- **Next-Gen Windows (Formerly Next-Gen Endpoints)**
  Customers receive a report with actionable recommendations to drive deployment and next steps.

- **Microsoft 365 Business Voice Remote Jumpstart**
  Basic deployment of Business Voice using Microsoft Teams.

- **Microsoft Intune/Mobile Device Management**
  This platform helps customers manage, analyze, automate and understand their data and utilize it in a way to accelerate their business goals.

- **Microsoft Teams Meetings Readiness**
  Assessment of the client's environment to define if Microsoft Teams can be adopted.

- **Microsoft Teams Deployment**
  Migrate files off your network file server into SharePoint Online and OneDrive for Business inside secure cloud storage hosted by Microsoft to gain access to your files from any device with an internet connection inside and outside your corporate network without needing a VPN.

- **Microsoft Teams Voice – Cloud VoIP**
  Deploy Microsoft Teams to work with teammates via secure workspace chat, videoconferencing meetings, document collaboration, built-in cloud storage and application integration.

- **Microsoft Viva: Viva Topics, Viva Insights, Viva Connections and Viva Learning**
  Bring your phone system to the cloud with Teams Voice, adding phone system calling capabilities to modern collaboration software, allowing organizations to have auto attendants, call queues and conference numbers.

- **Microsoft/Office 365 Best Practice Assessments**
  Have a CDW delivery engineer consultant assess your Microsoft 365 environment to ensure your Teams, SharePoint, OneDrive and basic Microsoft 365 Admin Centre controls, policies and settings are configured to align with Microsoft's recommended best practices. We provide a report of the current state of your tenant with a prioritized list of actionable recommendations to help you identify and fix potential issues in your environment.

- **SCCM/Microsoft Endpoint Manager**
  The Microsoft Power Platform is a powerful set of applications that allow a customer to automate processes, build solutions, analyze data and create virtual agents.

- **Virtual Desktop Pilot**
  Pilot and Enterprise Production deployment of Azure Virtual Desktop (AVD).

- **Virtual Desktop Solutions**
  New Horizon deployments, upgrades to existing deployments and health assessments.

- **Voice and Meetings With Adoption**
  Assess existing environment to move to Microsoft Teams adoption.

- **Windows Autopilot Assessment (Intune)**
  Provides the ability to automate the onboarding and customization of a device that is shipped directly to the end user.

- **Windows Autopilot Assessment and Pre-provisioning with Intune**
  Intune assessment to make sure clients are ready for white-glove services.

- **Windows Hello for Business**
  Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

ENDPOINT (AV, EDR, XDR)

- **Endpoint Health Check**
  Review current endpoint technology design and implementation and provide guidance on improvements that can be made.

- **Endpoint Migration/Implementation**
  New deployment: deployment is from the ground up, no existing endpoint technology is being used. Migration: customer has deemed endpoint technology ineffective or costly to maintain effectively, CDW to remove and install better- suited technology for the customer.

Security Services

CDW Canada's Security Services provide independent evaluations of your security posture and help you fortify your weaknesses. Our certified experts design comprehensive strategies and solutions for protection and response.

PROFESSIONAL SECURITY SERVICES

You can rely on our team of experts to implement and review your professional security services. We also have authorized training centres to help your internal team make the most of your security technologies.
[Explore Managed Security Services]

- **Authorized Training Centre**
  CDW is the only authorized training centre for F5 and Palo Alto Networks. Several courses and dates are available and can be booked accordingly on the CDW ATC portal.
  Supported Vendors: F5 and Palo Alto

- **Cloud Security Posture Assessment (CSPA)**
  Help customers gain visibility of potential misconfiguration in public cloud IaaS or PaaS in AWS, Azure, or GCP. This service will leverage a cloud security posture management (CSPM) tool to query the targeted public cloud and provide findings and recommendations for any gaps/risks identified. The goal is to drive CSPM sales and potential cloud remediation work.
  Supported Vendors: AWS, Azure and GCP

ENDPOINT (AV, EDR, XDR)

- **Endpoint Health Check**
  Review current endpoint technology design and implementation and provide guidance on improvements that can be made.
  Supported Vendors: CrowdStrike, Cylance, Microsoft and Palo Alto

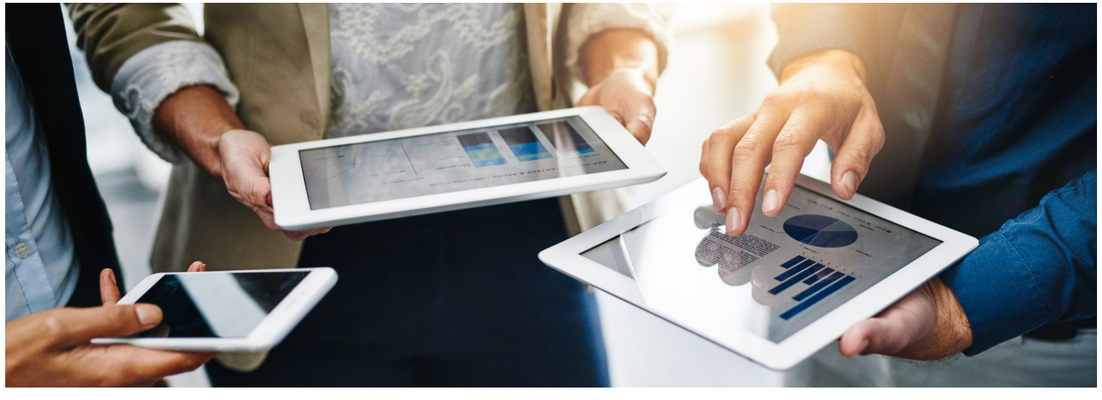
- **Endpoint Migration/Implementation**
  New deployment: deployment is from the ground up, no existing endpoint technology is being used. Migration: customer has deemed endpoint technology ineffective or costly to maintain effectively, CDW to remove and install better-suited technology for the customer.
  Supported Vendors: CrowdStrike, Cylance, Microsoft and Palo Alto

IDENTITY AND ACCESS MANAGEMENT

- **IAM/SSO/Migration/Implementation**
  Customers looking to implement identity management with no current solution in place. Integrating lightweight directory access protocol (LDAP)/active directory (AD) and integrating single sign-on (SSO) into corporate applications.

  Customers looking to replace their identity management with an IAM solution currently in place. Porting an already existing LDAP/AD and SSO configuration to better technology and improving the architecture.
  Supported Vendors: Centrify, Microsoft and Okta

- **IAM/SSO Health Check**
  Review current SSO/IAM implementation and provide a report to show possible areas of improvement.
  Supported Vendors: Centrify, Microsoft and Okta



NETWORK SECURITY

- **FortiGate Rapid Deployment Services**
  Rapid Deployment for implementing a greenfield NGFW firewall solution or rapid deployment for like-for-like migration between vendor firewall platforms.
  Supported Vendors: Fortinet

- **Next-Generation Firewall (NGFW) Health Check**
  In-depth review of NGFW firewall throughput, architecture, design and availability to ensure stable operation.
  Supported Vendors: Cisco, Fortinet, Palo Alto Networks and SonicWall (partner supported)

- **Next-Generation Firewall (NGFW) Implementation Services**
  Design and implementation of a greenfield NGFW firewall solution or a like-for-like migration between vendor firewall platforms.
  Supported Vendors: Cisco, Fortinet and Palo Alto Networks

- **SD-WAN Implementation**
  Discovery, design and implementation of a software-defined area network (SD-WAN) solution, starting by gathering customer requirements, identifying current infrastructure and building out an SD-WAN solution. Followed by a staged migration of production services.
  Supported Vendors: Cisco, Fortinet and Palo Alto Networks

- **SASE Rapid Deployment Service**
  Rapid deployment for implementation of a greenfield SASE solution.
  Supported Vendors: Cisco, Fortinet and Palo Alto Networks

- **FortiGate Rapid Deployment Services**
  Rapid deployment for implementing a greenfield NGFW firewall solution or rapid deployment for like-for-like migration between vendor firewall platforms.
  Supported Vendors: Fortinet

- **NGFW (Next-Generation Firewall) Rapid Deployment Service (PA-220, PA-400, PA-1400, and PA-3200/3400 Series)**
  Rapid deployment for implementing a greenfield NGFW firewall solution or rapid deployment for like-for-like migration between vendor firewall platforms. This service is a value-focused alternative to vendor-provided quickstart services.
  Supported Vendors: Palo Alto Networks

- **PAN-OS Upgrade Service**
  Downtime caused by upgrades is costly to your business. Our team has the expertise and experience to assist you in planning and patching your critical Palo Alto Networks infrastructure to avoid downtime and confirm your upgrades take place as seamlessly as possible.
  Supported Vendors: Palo Alto Networks

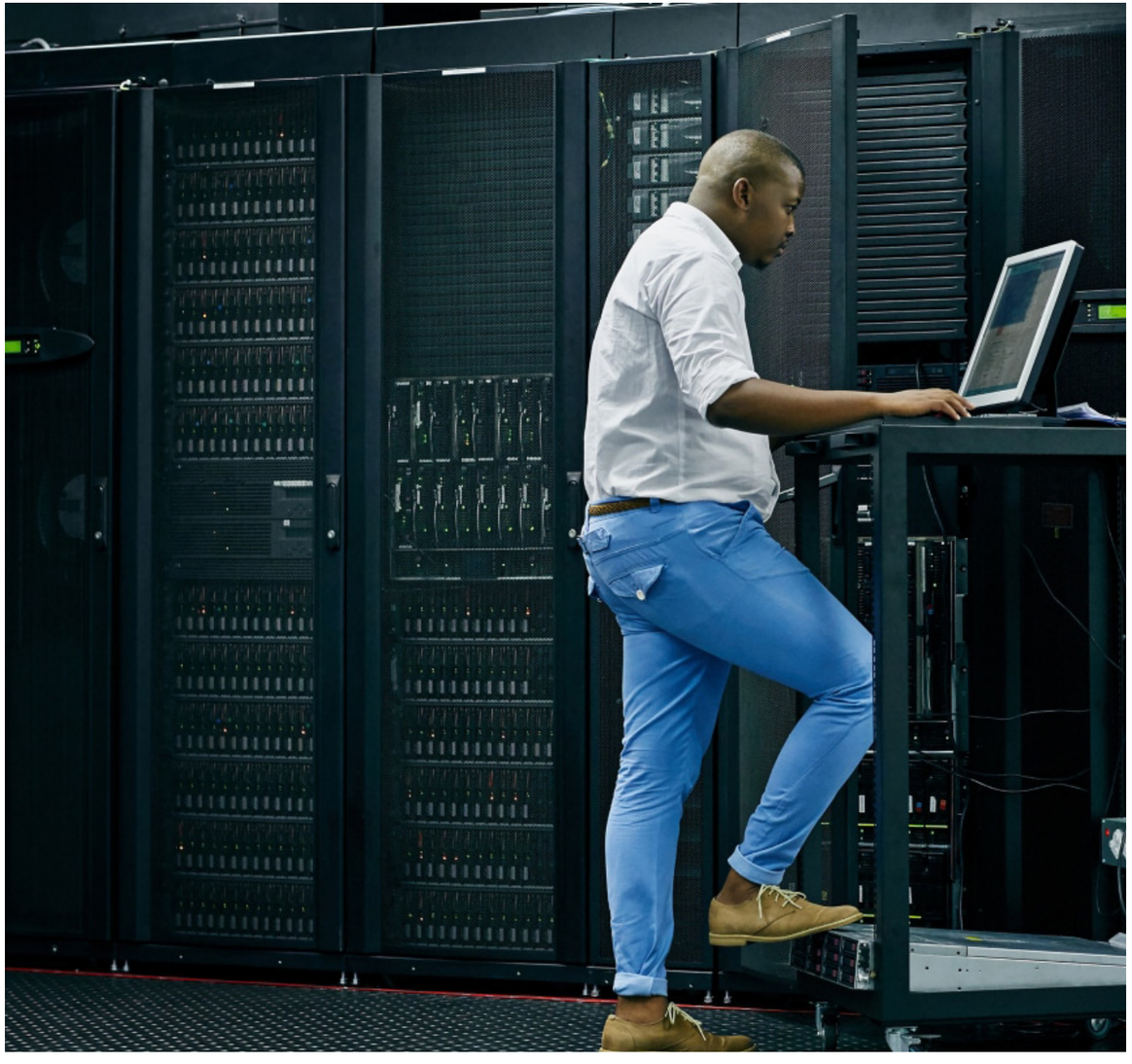
- **SASE Implementation**
  Discovery, design and implementation of a secure access services edge (SASE) solution, starting by gathering customer requirements, identifying current infrastructure and building out a SASE framework. Followed by a staged migration of production services.
  Supported Vendors: Palo Alto Networks

SIEM & ANALYTICS

- **SIEM Health Check**
  Review of an existing platform to ensure that it is configured for optimal performance and contains the right log sources and content to support appropriate security monitoring.
  Supported Vendors: LogRhythm and Splunk

- **SIEM Migration/Implementation**
  The design and implementation of a SIEM solution from the ground up, including software installation and configuration, log source integration, as well as the implementation of alerts/use cases, reports and dashboards, based on the customer's requirements.
  In the case of migrations, we work closely with the customer to understand what needs to be moved over from the existing solution and what can be deprecated.
  Supported Vendors: LogRhythm and Splunk

- **SIEM Upgrade**
  System review and operational health check of an existing platform, followed by planning and executing a platform upgrade.
  Depending on how dated the platform is, multiple upgrades may be required, as well as a review of the memory/compute/storage requirements for the latest software versions.
  Supported Vendors: LogRhythm and Splunk



MICROSOFT SECURITY

- **Azure Active Directory IAM Rapid Deployment**
  Microsoft Entra is a suite of cloud-based identity solutions that provide a host of identity and access management capabilities. Azure AD, a core Microsoft Entra solution and provides identity as a service features and capabilities, including cloud unified identity management, single sign-on, conditional access, identity protection and identity lifecycle management. This rapid deployment, optimized for small to medium-sized businesses, enables customers to quickly realize value from their investment in Azure AD.

- **M365 Defender Rapid Deployment**
  Microsoft 365 Defender is an XDR solution that natively coordinates detection, prevention, investigation and response across endpoints, identities, emails and applications. This rapid deployment, optimized for small to medium-sized businesses, enables customers to realize value from their investment in Microsoft 365 security.

- **Microsoft Purview Data Loss Rapid Deployment**
  Microsoft Purview is an advanced data governance, risk and compliance platform that allows organizations to govern, protect and manage their data. With Microsoft Purview's data loss prevention capabilities, organizations can define sensitive information patterns and detect those patterns within information assed protect against unintentional or accidental sharing of sensitive information. This rapid deployment, optimized for small to medium-sized businesses, enables customers to quickly realize value from their investment in Microsoft Purview Data Loss Prevention.

- **Sentinel Deployment Rapid Deployment**
  Microsoft Sentinel is an advanced security analytics, threat intelligence, threat hunting and automation platform that allows organizations to correlate threat signals from multiple sources to increase attack detection, increase threat visibility, accelerate incident response. This rapid deployment, optimized for small to medium-sized businesses, enables customers to quickly realize value from their investment in Microsoft Sentinel.

MANAGED SECURITY SERVICES

Many Canadian organizations are not confident in their ability to detect and respond to a cybersecurity breach. A lack of in-house expertise and an insufficient number of skilled personnel are two of the top reasons respondents cited as to why organizations cannot effectively manage their security posture. CDW's managed security services allow you to leverage our highly specialized skills, technology and expertise, directly matched to your business need, all for a predictable monthly cost.

- **Managed Defender**
  The CDW Managed Detection & Response with Defender for Endpoint service enables advanced threat detection through automated correlation of events, resulting in faster incident qualification, response and containment of threats.
  We couple Defender for Endpoint's detection, prevention, investigation and response capabilities with 24x7 analyst lead monitoring, analysis and remediation.
  Supported Vendors: Microsoft

- **Managed NGFW (Next-Generation Firewall)**
  Growth in cloud-based services and infrastructure means organizations are finding it harder to manage technology complexity. CDW will help you adopt and integrate NGFW securely, provide ongoing support, or we can manage the environment for you. CDW can help you scale where needed, as well as keep you informed of any changes and help you maximize the ROI on your NGFW investments and achieve your business outcomes faster.
  Supported Vendors: Cisco, Fortinet and Palo Alto

- **Managed Palo Alto Network Services**
  Having Palo Alto Network solutions continuously monitored for service availability and performance is easier with CDW's managed services. Our services are managed by certified experts to deliver in-depth analysis and response.
  Supported Vendors: Palo Alto

  - **Managed Cortex XDR**
    Enables advanced threat detection through automated correlation of events across network, cloud and endpoint solutions, delivering faster qualification, response and containment of threats. Provides 24/7/365 threat monitoring and management, change and configuration management and monthly service reporting. Simplifying threat detection, correlation and response into one complete solution.
    Supported Vendors: Palo Alto

- **Managed SASE (Prisma Access)**
  CDW's Managed SASE (Prisma Access) consolidates all the networking and security capabilities organizations need into one single cloud-delivered platform, providing security to any user and to all applications from anywhere. This solution consists of two layers: security as a service (SaaS) and network as a service (NaaS).
  Supported Vendors: Palo Alto

- **Managed SD-WAN (Prisma SD-WAN)**
  The Prisma SD-WAN solution is a cloud-first solution that eliminates the costs of expensive multiprotocol label switching (MPLS) network solutions, improves end-user experience and provides scalability to modernize network performance and security.
  Supported Vendors: Palo Alto

- **Managed SIEM**
  Managed Cloud SIEM provides our Customers with a central event repository, where data for all security events across an organization are stored, analyzed and acted on. This high-touch, intelligence-driven service is backed by our team of threat analysts who provide extensive security analysis and threat detection.
  Supported Vendors: Log Rhythm and Splunk

- **Managed SIEM as a Service**
  Improve overall security posture by quickly identifying cyber threats across the network and cloud environments, providing customers with the correct response strategy to defend against these threats. SIEM as a service provides customers with an enterprise-wide view of security across their environment by leveraging industry-leading tools. Security threats correlated into a single pane of glass view into the security ecosystem.
  Supported Vendors: Log Rhythm

Risk Advisory Services

CDW's senior consultants can help you detect your organization's vulnerabilities, create a plan to minimize cyber risk and guide your company on how to comply with government privacy legislation.

GOVERNANCE RISK AND COMPLIANCE

- **Third-party Certification Readiness**
  It provides guidance on the adoption of the ISO framework, identifies gaps in coverage, determines compliance and implements missing controls. This can be a helpful first step towards adoption and eventually ISO 27001 certification.
  Security Frameworks: CIS Controls, ISO 27001, ISO 27017, ISO 27018 and NIST CSF

- **Business Impact Assessment**
  A business impact assessment (BIA) is intended to analyze the impact on the business if key processes and functions are disrupted. The assessment will focus on identifying critical processes within each line of business, assessing the impact of disruption to those processes and identifying resource requirements for each line of business.
  The purpose of this engagement is to assist the customer organization in prioritizing the recovery of business services by establishing recovery objectives for each line of business and its associated processes.

- **Gap Assessment**
  Gap assessments provide clients with a comparison and analysis of the technical, physical and administrative controls that make up their security or privacy program against a specific industry standard. Cyber Risk is capable of performing gap assessments against a variety of industry security and privacy standards. Below are some examples of the most common standards used to perform gap assessments.
  Security Frameworks: CIS Top 20 (Formerly SANS TOP 20), ISO 27001, ISO 27017, ISO 27018 and NIST CSF

- **Holistic Security Assessment**
  A holistic security assessment combines a threat risk assessment with penetration testing to provide a holistic understanding of an organization's security posture. Unlike these standalone services, the holistic security assessment includes an integrated report, leveraging the insights from both assessments to provide additional context.

- **Incident Response Plan Development, Runbook Development and Tabletop Exercise**
  Incident response plan (IRP) development and tabletop exercises are designed to help assess an organization's existing IRP or build a new one. The development of this plan includes both the organizational requirements to manage the incident response program, such as defining roles and responsibilities, establishing authorization and incident declaration processes, as well as technical runbooks that outline the organization's approved response plans for specific threat scenarios (e.g. ransomware infection, business email compromise). Following the establishment of the IRP and associated technical runbooks, CDW cyber risk consultants will facilitate a tabletop with customer stakeholders to walk through an incident scenario and simulate the response to a relevant threat scenario.

- **Internal Audit**
  Internal audits are conducted to prepare clients for external certification audits. Internal audits facilitate the maintenance of certifications against standards such as ISO 27001, ISO 27017, ISO 27018 and NIST CSF. The intent of the engagement is to perform a third-party internal audit of the client's security program to identify any non-conformance against the standard and provide recommendations for remediation.
  Security Frameworks: CIS Controls, ISO 27001, ISO 27017, ISO 27018 and NIST CSF

- **PCI DSS Initial Assessment**
  An initial PCI compliance assessment is intended to help organizations understand their PCI DSS-related compliance requirements and establish a remediation roadmap for compliance.
  Security Frameworks: PCI DSS

- **Privacy Impact Assessment**
  Privacy impact assessments (PIA) are performed to ensure privacy risks are addressed in a client's information handling practices. The objective of this assessment is to identify, assess and prioritize deficiencies in current privacy practices against the client's privacy obligations to determine compliance with required and addressable regulatory requirements and associated risks with gaps in compliance.
  Security Frameworks: PIPEDA, HIPAA and GDPR

- **Risk Assessment**
  Risk assessments are performed to assist clients in understanding security threats, vulnerabilities and associated risks that may affect confidentiality, integrity, and availability of client data, supporting infrastructure/systems and critical applications. Risk assessments include a gap assessment against industry security standards to identify vulnerabilities in the client's environment. The risk assessment focuses on people, processes and technologies that interact with the client's sensitive information.
  Security Frameworks: CIS Controls, ISO 27001, ISO 27017, ISO 27018 and NIST CSF

- **Threat Risk Assessment**
  Threat risk assessments (TRA) are performed to provide additional threat analysis context that a standard-based risk assessment does not. In addition to what is covered in a risk assessment, a TRA will also provide additional context related to various threat vectors that might affect the target organization.
  Security Frameworks: CIS Controls, ISO 27001, ISO 27017, ISO 27018 and NIST CSF

- **Security/Privacy Program Certification Preparation**
  Security/Privacy Program Certification Preparation aids clients in certifying their program against an industry standard. Certification preparation includes a gap and risk assessment to determine additional controls that need to be implemented and identify risks to the organization; program implementation; an internal audit to ensure controls are aligned with the standard; and external audit management and support. Below are some examples of the most common standards used
  Security Frameworks: CIS Controls, ISO 27001, ISO 27017, ISO 27018 and NIST CSF

- **Security/Privacy Program Implementation**
  Security/Privacy program implementation includes the customization of technical, administrative and physical controls to protect a client's sensitive information and privacy. The services include implementation of policies, procedures, and forms; establishment of a governance committee; information security awareness training; risk management and program metrics. Program implementation often uses an industry security standard as a baseline for implementation; below are some examples of the most common standards used.
  Security Frameworks: CIS Controls, ISO 27001, ISO 27017, ISO 27018 and NIST CSF

- **Security/Privacy Program Maintenance Retainer**
  The Security/Privacy Program Maintenance Retainer service is geared toward clients that have achieved certification against an industry standard and require ongoing support for the maintenance of certification. Activities included in the program maintenance retainer include, but are not limited to: annual risk assessment, annual internal audit, external audit management, governance committee meetings and ad hoc security/privacy consultation.

- **Security Health Check**
  CDW's security health check will assess your organization's security program to assist you in understanding your security posture and identify where any major vulnerabilities exist in your environment that malicious actors could exploit. This cost-effective solution will help you establish a plan to address the five most critical risks to your environment, providing tailored recommendations that are relevant to your business and preparing you for a path of continuous security maturity development while you grow your business.

- **Virtual CISO**
  The virtual chief information security officer (vCISO) service is an on-demand program that meets the unique needs of a client to support their security governance, risk and compliance functions. This program facilitates sharing the knowledge and experience of outsourced corporate security, compliance and internal audit department, while not incurring the full financial burden. The CDW Cyber Risk group acts as a trusted advisor to build and maintain the client's information security and risk posture.

PENETRATION TESTING

- **Penetration Testing and Adversarial Simulation**
  It helps the customer understand their risk of exposure more clearly, so they are better equipped to make informed business decisions. We uncover security vulnerabilities in their environment, understand the company's security posture and test its readiness to withstand and respond to a real-world cyberattack.

  - **API Penetration Testing**
    A penetration test focused on identifying vulnerabilities in API endpoints and protocols that could be exploited to negatively impact the confidentiality, integrity and availability of associated data.

  - **Cloud Penetration Testing**
    CDW's Cloud Penetration Testing Service is used to discover, identify and classify potential deficiencies and vulnerabilities in organizations' cloud environments; and help assess the related security posture. CDW's Cybersecurity consultants would attempt to identify and exploit vulnerabilities to simulate a malicious actor, and then provide recommendations to remediate issues.

  - **Email Social Engineering**
    Email phishing, a type of social engineering, is a common tactic utilized by threat actors when targeting an organization to gain sensitive information or network access. Email social engineering campaigns assess an organization's employee security awareness of these types of attacks by measuring link click rate, malicious attachment execution or the submission of user credentials on a compromised login portal.

  - **Mobile Application Penetration Testing**
    A penetration test that simulates an attack against a mobile application to identify client-side vulnerabilities including, but not limited to, insecure data storage, build misconfigurations and insufficient reverse engineering security controls.

  - **Network Penetration Test (Internal or External)**
    An external penetration test encompasses a scan of an organization's external-facing infrastructure to identify vulnerabilities, manually verify issues and exploit them to demonstrate what could be accomplished by a threat actor.

    An internal penetration test demonstrates what an external attacker could accomplish after they have breached an organization's perimeter. Internal network penetration testing includes scanning, validation and exploitation of discovered vulnerabilities, as well as manually probing the network for additional attack vectors not typically identified with automated scanners.

  - **Network Vulnerability Assessment (Internal or External)**
    A vulnerability assessment utilizes automated tools and manual techniques to identify and validate vulnerabilities within internal or external network infrastructure.

  - **OSINT Assessment**
    Open-source intelligence (OSINT) is a form of intelligence collection that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. Intelligence gathering is performed to determine entry points into an organization, be it physical or electronic, in order to highlight what information the organization makes public and how it can be used by a determined attacker.

  - **Phone Social Engineering**
    Phone-based social engineering, or vishing, is a tactic used by threat actors to attempt to gain sensitive information or persuade a user to perform an action that could lead to a security breach via text messaging or phone calls. Phone social engineering engagements assess employee security awareness against voice or text-based attacks which could put the organization at risk.

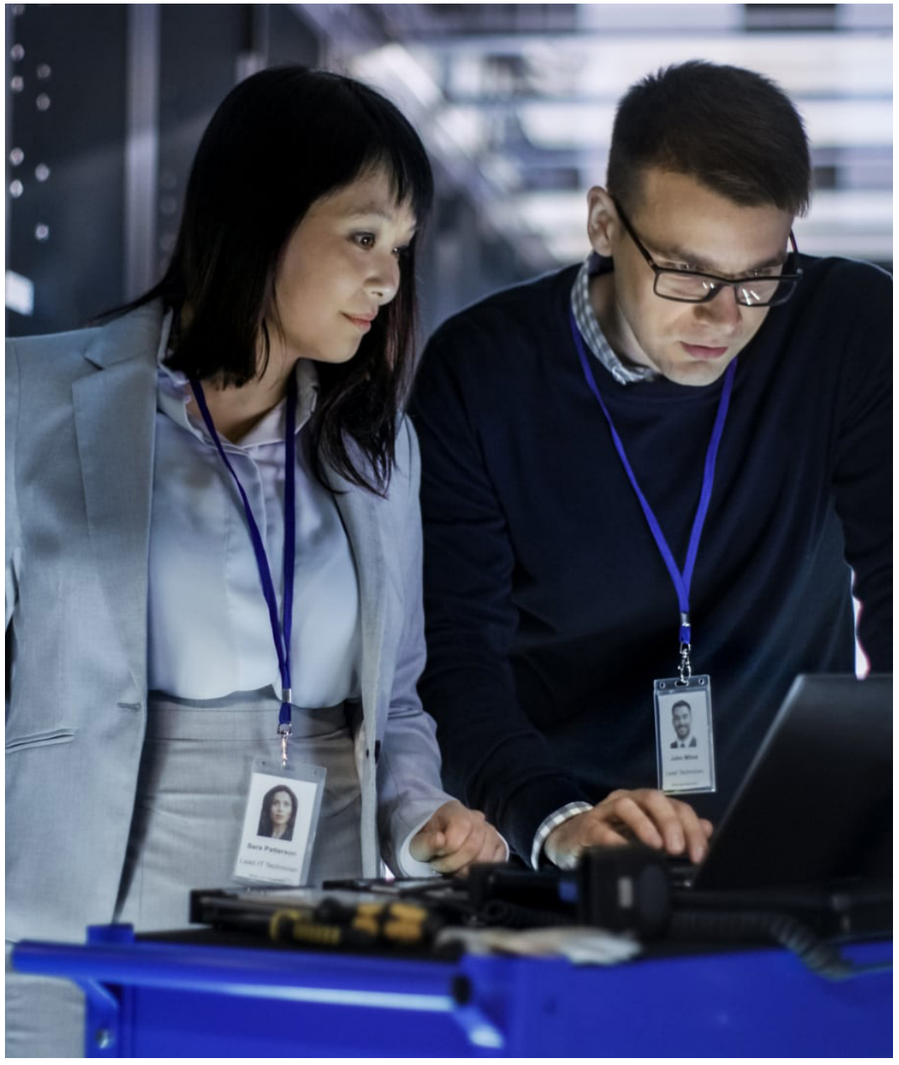
  - **Physical Social Engineering**
    On-site social engineering is used to assess the physical and environmental security controls of a site as well as security protocols, such as confirming the identities of staff and visitors, preventing unauthorized access, etc. Sometimes, physical social engineering is also paired with penetration testing services such as dropping malicious USB keys and attacking targets if they are plugged into a device on the target network.

  - **Red Team Assessment**
    An assessment recommended for organizations with a mature security practice; red team engagements focus on testing an organization's detection and response capabilities to real-world attack scenarios. These longer-running assessments emulate a dedicated threat actor attempting to gain a foothold within an organization by means of exploiting technical vulnerabilities or using various types of social engineering in order to achieve a pre-determined goal while remaining undetected on the network.

- **Scenario-Based Penetration Testing**
  A penetration test focused on a specific scenario and objective (i.e., emulating a threat actor that has compromised an internal workstation). Typically time-based, this penetration test aims to identify vulnerabilities and deficiencies that would be exploited by real-world threat actors in a given scenario and is not meant to be a comprehensive assessment of the entire network infrastructure.

- **Targeted Attack Penetration Testing**
  A limited penetration test focused on typical attack pathways abused by threat actors from an external network perspective. Includes a one-time social engineering engagement from pre-templated scenarios to measure click-rate, credential capturing or malicious payload execution.

- **Web Application Penetration Testing**
  Web application penetration testing is performed to identify and exploit vulnerabilities in the web application and its components using manual and automated techniques.



VULNERABILITY MANAGEMENT

- The CDW Vulnerability Management Service provides regular network-level and application security vulnerability scanning of your environment for systems that may be misconfigured or vulnerable to exploitation. Typically, a local scanning agent will be placed in the customer's network to allow scanning of internal hosts that are not accessible from the internet.

  CDW's scan uses a series of discovery processes to identify all active systems and services. Each identified service is then scanned for vulnerabilities, based on a current and comprehensive list of vulnerabilities, exploits and state criteria. Results are compiled into a report and delivered to the customer. The report will highlight the vulnerabilities discovered, according to severity and risk and list recommended remediation steps.

ServiceNow

IT service management and digital workflow platforms are rapidly becoming a cornerstone of IT. As a ServiceNow® Partner, CDW helps you optimize the value of your ServiceNow® investment and streamline IT operations across your organization.

E-GOVERNANCE RISK AND COMPLIANCE (EGRC)

- Achieving regulatory compliance involves a significant investment of time, effort and money toward creating and adopting a well-planned framework. Maintaining that framework has proven to be highly challenging. The CDW eGRC service is powered by ServiceNow and addresses this issue by ensuring ongoing controls are always top of mind, actionable and most importantly, easy to report.

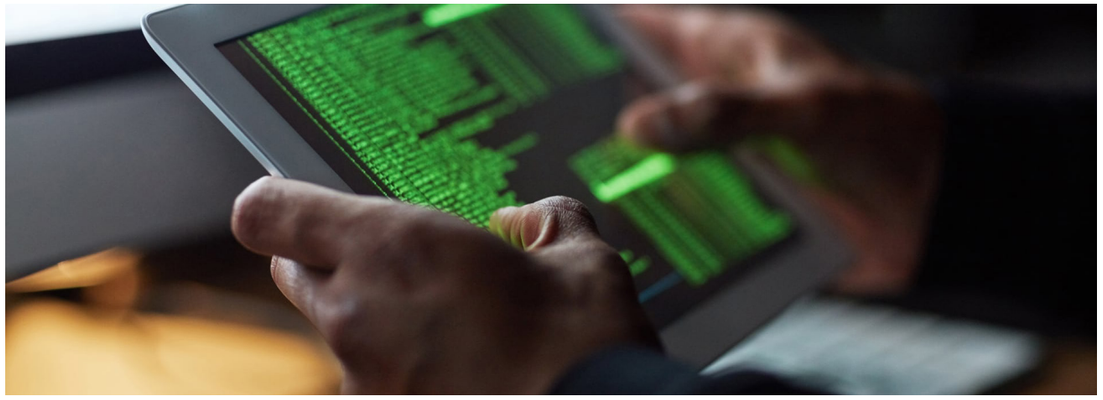
- **Implementation Services**

  - **Customer Service Management (CSM)**
    ServiceNow Customer Service Management (CSM) makes it possible to fix and prevent issues permanently by connecting customer service to other departments and automating processes across teams for faster resolution. With CSM, you can solve customer problems by bringing front, middle and back offices together, proactively addressing customer issues and instantly handling common customer requests.

  - **IT Operations Management (ITOM)**
    Organizations are adopting a hybrid or cloud-first strategy as they pursue digital transformation. This allows unprecedented agility but also creates new challenges for IT. ServiceNow ITOM will enable you to overcome them. ITOM Visibility creates an accurate, current record of your entire environment and the services flowing across it. ITOM Health cuts through event noise, using the power of AIOps and automation to help you quickly detect, diagnose and remediate service issues. ITOM Optimization helps reduce cloud spending by identifying and operationalizing cost optimizations and by creating a standard operating model across multiple clouds—delivering effective adaptive governance.

  - **IT Service Management (ITSM)**
    Our ServiceNow ITSM solution provides scalable workflows to manage and deliver IT services to your users through a single cloud-based platform called NOW. The ITSM solution can help increase your agents' productivity, resolve issues quickly and improve user satisfaction. Powered by platform native AI, you can promptly accelerate technology changes, view recommended actions for incoming tickets or requests, and drive self-service and automation through enterprise chatbot technology.

  - **Security Operations (SecOps)**
    ServiceNow Security Operations (SecOps) brings incident data from your security tools into a structured response engine that uses intelligent workflows, automation and a deep connection with IT to prioritize and resolve threats based on their impact on your organization.



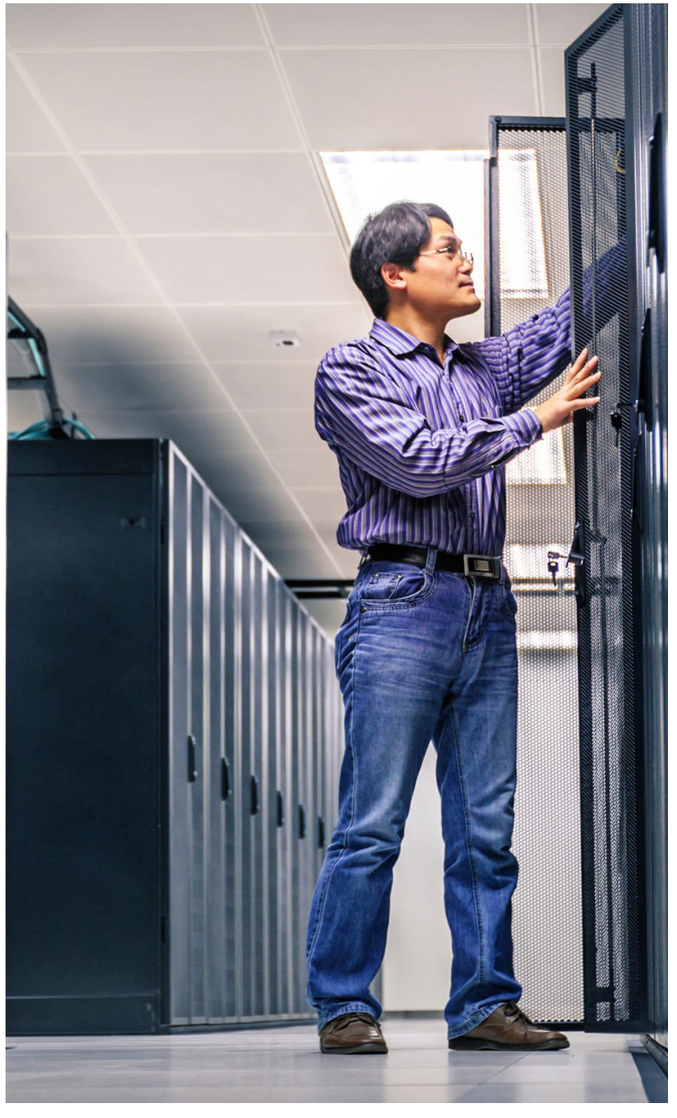
- **Maturity Assessment and Roadmap**
  Ensure your ServiceNow instance's ongoing maturity and adoption with our specialized maturity assessment. This assessment builds a just-in-time path, from the current state to a recommended future state, outlining your best-fit journey. This is an advisory services-led engagement that infuses a best-practice view of the future, incorporates a business-led approach and then designs a custom plan for ongoing ITSM and toolset maturity.

- **Smart CIP**
  Using continuous service improvement (CSI) principles, SmartCIP focuses on improving service management in your organization. Our support services consultants meet with you to provide the resources, impetus and accountability necessary to keep improvement initiatives from being lost in the clutter of the many demands on your time.

- **ServiceNow Add-ons: SmartScan**
  As more applications are implemented within your ServiceNow platform, the instance must continue to be optimized for growth and scale without degrading performance. SmartScan is a thorough evaluation of your ServiceNow platform to ensure best practices are in place to give you the greatest return on investment.

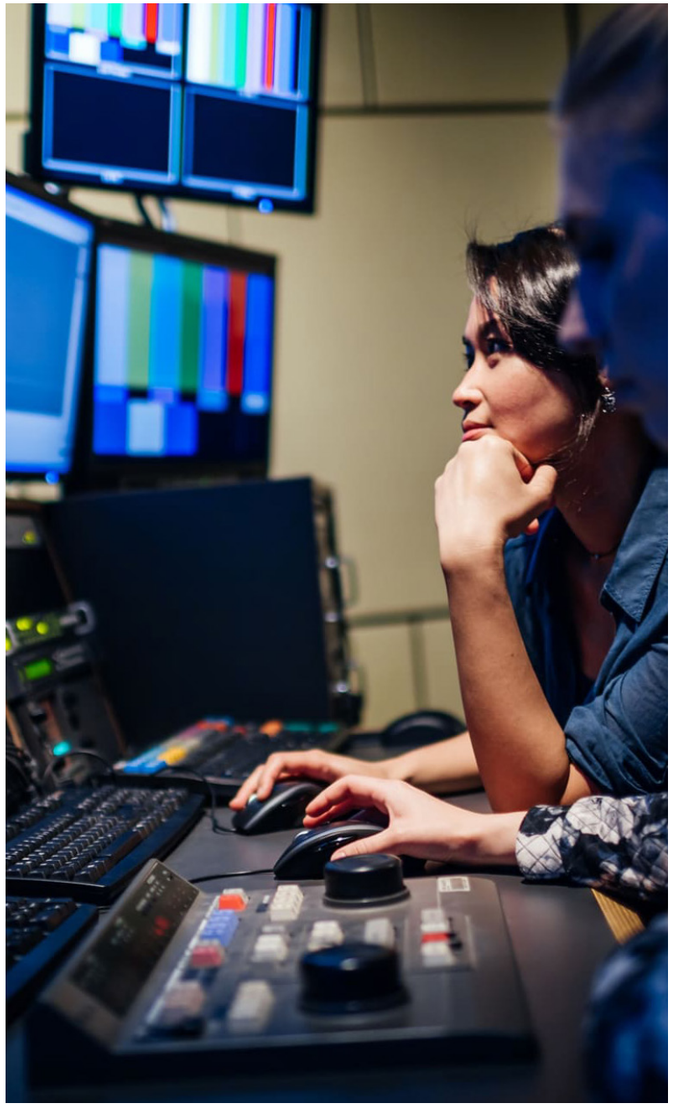
- **ServiceNow Add-ons: Upgrade Assistance**
  We use ServiceNow's proven six-phase approach to upgrade your instance of ServiceNow to the next sequential release. We'll help you plan, prepare and migrate successfully to a newer release of ServiceNow, verifying custom applications along the way or implementing new ones if necessary.

- **ServiceNow Roadmap Calibration**
  As your use of the ServiceNow platform adapts and grows, it's essential to look at your current roadmap to decide if it's still an actionable plan that can keep growing with you. Roadmap calibration is an engagement during which CDW's advisory consultants will conduct a review that focuses on updating your initial maturity assessment to deliver a multi-year, multi-phase view in identifying opportunities, benefits and investment levels and subsequently design a recommended approach for the ongoing maturity and adoption of your ServiceNow platform.



Media & Entertainment

CDW is the leading Canadian software solution provider for the media and entertainment (M&E) industry. We serve thousands of clients, ranging from freelancers and start-ups to some of the largest studios in the industry.
Our M&E experts work hand in hand with our infrastructure, cloud and security teams to provide you with the best-in-class offerings that will keep your projects on time, secure and on budget.



- **Media and Entertainment IT Solutions**
  These services include StudioCloud, a community cloud for the digital media industry, offering on-demand computing to studios. The predictable, per-use cost model of StudioCloud allows studios to save money, time and assets by matching the availability of IT resources with the project demands and timetables.
  Supported Vendors: Autodesk, Dell, EMC and Intel

- **StudioCloud**
  We've levelled the playing field and created StudioCloud Powered by Intel, a completely secure, fully-managed, infinitely scalable solution customized to you. Select the number of nodes and the term length you need based on the project at hand. Best of all, we offer an MPAA-audited environment for studios of any size. Plus, our facilities offer a fully-managed service with 24/7/365 monitoring and support from StudioCloud engineers backed by our own network and security operations centre.
  Supported Vendors: Autodesk and Intel