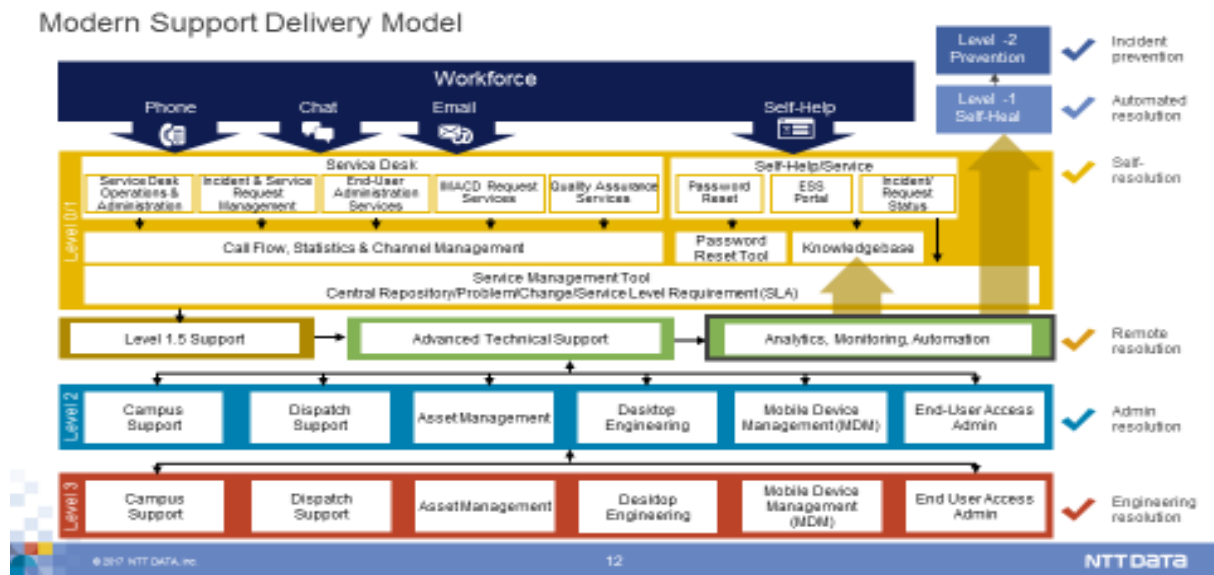


## Exhibit 1 (Catalogue of Services, Service Levels, Pricing)

### NTT DATA End-User Compute (EUC) Services



### EUC Services Catalog

**Table 1: NTT DATA's EUC Services Catalog Summary**

Services	Description
Service Desk	<ul style="list-style-type: none"> <li>Maintains best practice operating standards for delivery of NTT DATA-provided scope</li> <li>Industry standard ITIL service management techniques along with technologies such as ServiceNow (for ticket management) and Flexera (for managing software licenses).</li> <li>Processes include change management, incident management, problem management, request management, knowledge management, root cause analysis, and others</li> <li>NTT DATA will provide resolver group support for all in-scope services (Level 1, 2 and 3)</li> <li>NTT DATA will make every effort to identify, recommend, enable, and implement optimization including moving activities to Level 0 (automation and self-service)</li> </ul>
Asset and Configuration Management	<ul style="list-style-type: none"> <li>Provides process integration to support inventory and status tracking of hardware and software assets during their lifecycle</li> </ul>

Services	Description
	<ul style="list-style-type: none"> <li>• We leverage best practice IT Infrastructure Library (ITIL)-compliant processes in our asset and configuration solutions</li> </ul>
EUC Device Refresh	<ul style="list-style-type: none"> <li>• Supports the end-to-end asset lifecycle for the end-user hardware</li> <li>• Laptops, tablets, desktop PCs and printers are refreshed or removed from service in accordance with their established asset life cycles</li> <li>• Applies to leased and purchased EUC devices</li> <li>• Tools for automated and manual EUC device validation and scheduling</li> <li>• Integrated with Service Desk CMDB, Asset and Configuration Management Tools and Reports</li> </ul>
Field Tech Support Services	<ul style="list-style-type: none"> <li>• Resolves service requests, diagnostics, and incident remediation that require hands-on support</li> <li>• These resources are typically dispatched by Levels 1 or 2 resources when remote diagnostics and/or service expectations dictate (such as VIP or concierge support)</li> <li>• These resources provide Install, Move, Add, Change, and Delete (IMACD) of devices to and from the operating environment</li> <li>• Desktop refresh activities are also part of this service</li> </ul>
Service Center (Tech Bar)	<ul style="list-style-type: none"> <li>• Walk-up service based on first come/first serve or scheduled appointment</li> <li>• Drop off service</li> <li>• “Warm Swap” service (a temporary or permanent asset swap)</li> <li>• Remote replacement pre-build</li> <li>• Capability and new device testing</li> <li>• Device and peripheral vending</li> </ul>
Self-Healing and Automation	<ul style="list-style-type: none"> <li>• Toolset and processes to enable self-healing and configuration automation processes for all managed Windows PCs</li> </ul>
Installation Move Adds and Changes (IMAC)	<ul style="list-style-type: none"> <li>• Install, Move, Add, Change (IMAC) activities for client systems, including peripherals</li> </ul>
Patch Management	<ul style="list-style-type: none"> <li>• Patch management service delivery is focused on identifying applicable patches and distribute them through automated means to maintain Operating System (OS) compliance levels</li> <li>• NTT DATA provides for the preparation, testing, staging, deployment, auditing, and ongoing management of operating systems and functional software patches for applications on servers, desktops, and laptops across the enterprise network</li> </ul>
Software License	<ul style="list-style-type: none"> <li>• NTT DATA will use standard reports to monitor usage of systems and identify unused licenses that can be re-allocated to different</li> </ul>

Services	Description
Management & Optimization	users or over-usage that needs to be remedied with new or re-assigned licenses
Image Management	<ul style="list-style-type: none"> <li>Image management is designed to simplify the complexities of software image development, validation, deployment, and maintenance</li> <li>This service component helps our clients achieve platform stability and consistency while allowing them the flexibility to meet their specific business requirements</li> <li>The NTT DATA desktop engineering service team creates and manages new custom images supporting multiple desktop, notebook, and workstation platforms based on each clients' functional need, applications, operating systems, service packs, and system software and hardware drivers</li> </ul>
OS/App Software Distribution and Deployment	<ul style="list-style-type: none"> <li>Electronic software distribution and the infrastructure conduit to distribute timely packaged applications and patch updates</li> </ul>
Equipment Configurations - Hardware Asset Lifecycle	<ul style="list-style-type: none"> <li>Employ a process-centric approach to enable management and visibility of IT and business asset data elements from planning through asset retirement</li> <li>NTT DATA's asset management process ties together all aspects of the device/product lifecycle</li> </ul>
Software Lifecycle Management—Basic	<ul style="list-style-type: none"> <li>Track deployed software against license count</li> <li>Simple desktop licensing, for example, Microsoft and Adobe</li> <li>Upgrade and downgrade rights</li> <li>Support and main agreements</li> </ul>
Software Asset Management (SAM)	<ul style="list-style-type: none"> <li>Representing the business practice that manages and optimizes the purchase, deployment, maintenance, utilization, and disposal of software applications within an organization</li> </ul>
Software License Management (SLM)	<ul style="list-style-type: none"> <li>Representing the support for the processes and tools used by an organization to control and document where and how the company's software products are able to run in order to enforce and ensure compliance with software licenses</li> </ul>
Security Administration	<ul style="list-style-type: none"> <li>Maintains an appropriate security posture as defined by government agency policy</li> <li>This includes host intrusion and/or prevention measures (anti-virus, anti-malware) across device types, operating systems and form factors (Windows PC, MDM, and VDI)</li> </ul>
Disk Drive Encryption	<ul style="list-style-type: none"> <li>Full disk encryption</li> <li>Industry trends, particularly in regulated Environments, are moving in the direction of full disk encryption on the end points.</li> </ul>

Services	Description
EUC Device Depot	<ul style="list-style-type: none"> <li>• Secure Inventory Management</li> <li>• Scheduled Refresh of aged end-user devices</li> <li>• Warranty repair coordination</li> <li>• Disposition of aged end-user devices</li> </ul>
Endpoint Visibility and Control	<ul style="list-style-type: none"> <li>• See all devices, on and off your network, and collect hundreds of hardware, software, security, usage, and geolocation data points automatically, including historical logs.</li> <li>• Take remote action to remediate endpoint risks immediately, regardless of user or network status.</li> </ul>

## Service Desk

Designed to coordinate with your strategic initiatives and priorities, the Service Desk by NTT DATA is finely tuned to the specific needs of your business, whether those needs are planning, delivery operations or management of IT support. Our service next-generation workplace support technologies and capabilities, such as multichannel and social media, persona and use case profiling, self-help, self-service and self-healing — allowing you to benefit from a single point of contact for end-user service requests. Leverage and benefit from a standard delivery model that takes advantage of industry-best and global core competencies, tools and resources.

Our experience, skillsets, processes and technologies provide you with:

- An enhanced user perception and end-user experience
- Transparency and cost reduction
- Metrics and proper process controls
- Service consistency across geographies
- The flexibility to respond to business change
- Visibility of high-priority, business-impacting incidents
- Timely data on service availability, quality, satisfaction and value

In providing IT Service Desk services, we will use industry standard ITIL service management techniques along with technologies such as ServiceNow (for ticket management) and Flexera (for managing software licenses). These processes and tools are integrated into a solution that we call Service Operations Manager, or SOM, which will enable a government agency to immediately benefit from our refined implementation of ServiceNow and best practices present in existing incident, problem management processes and mature asset management approach.

## Field Tech Support Services

Resolves service requests, diagnostics, and incident remediation that require hands-on support. These resources are typically dispatched by Levels 1 or 2 resources when remote diagnostics and/or service expectations dictate (such as VIP or concierge support). These resources provide Install, Move, Add, Change, and Delete (IMACD) of devices to and from the operating environment. Desktop refresh activities are also part of this service.

## Service Center (Tech Bar)

Our recommended service center approach attempts to satisfy all of these challenges by allowing users to determine how and when they want service. For environments typically considered “campus locations” service center resources provide:

- Walk-up service based on first come/first serve or scheduled appointment
- Drop off service
- “Warm Swap” service (a temporary or permanent asset swap)
- Remote replacement pre-build
- Advanced Technical Support (ATS), remote or in-person
- Capability and new device testing
- Device and peripheral vending

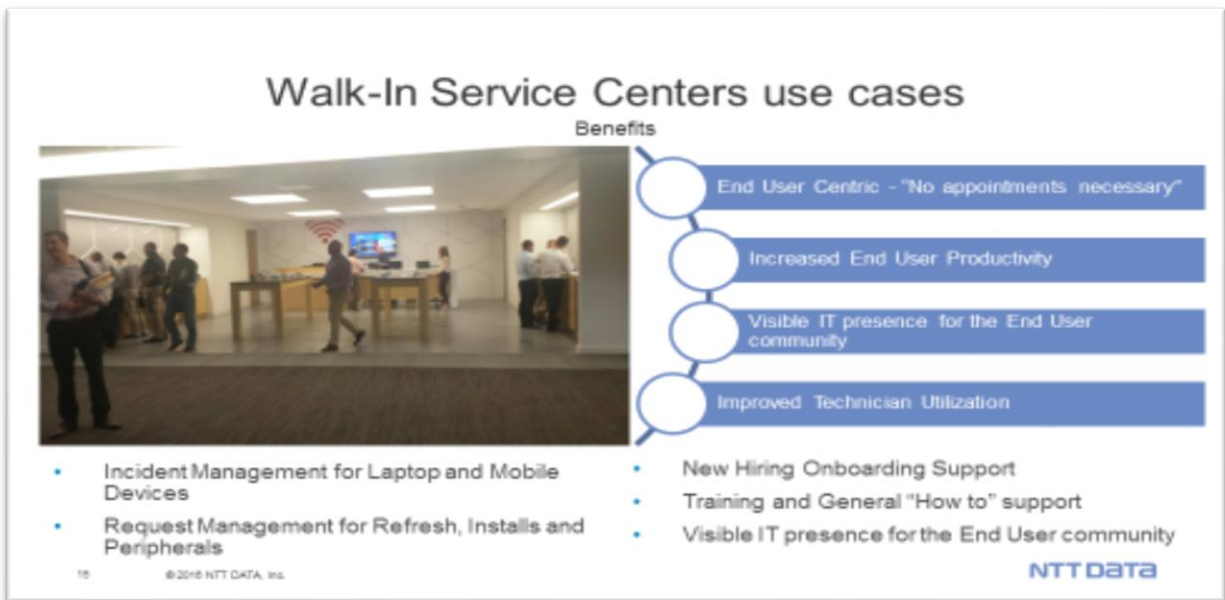


Figure 1: Tech Bar Illustration

Agents at the Service Center will have access to the ITSM tool and will be able to log tickets for users. During transition, a methodology can be devised to chargeback between the service desk and field services the amount of services provided by the Service Centers.

### Key Advantages of a Service Center

- Enhanced user experience
- Quick and effective issue resolution
- Improvement in support efficiency leading to cost savings

## Self-Healing and Automation

Significant portions of ticket volume and deskside support result from changes impacting the design intent of PC configuration. Many times these changes are unintended although on other occasions users with administrative rights intentionally reconfigure their device. Some of these changes may be a nuisance to the end user while others may be critical to security and operational standards.

NTT DATA recommends implementation of our standard toolset and processes to enable self-healing and configuration automation processes for all managed Windows PCs.

Each time an incident is resolved, our team will examine the process in an attempt to automate future repairs. For some problems, the tool can monitor system configuration watching for unintended change. Should a monitored change occur, the system can self-heal and report the change. In other cases where monitoring is not possible, the automation script can be placed in a self-service support library. These entries can be searched by users or referenced by support technicians.

These processes reduce or eliminate repair duplication, eliminating tickets and associated support labor. Most importantly user disruption is also minimized or eliminated entirely.

## **Installations, Moves, Adds, and Changes (IMACs)**

NTT DATA performs Install, Move, Add, Change (IMAC) activities for client systems, including peripherals.

We will perform IMAC activities for supported hardware including peripherals, and supported software, at designated end-user locations and update the system of record asset management and service request management systems accordingly. Disposal-related tasks are incorporated into the related IMAC service description.

At the completion of each service request, NTT DATA personnel will orient the authorized user about the new or modified supported hardware and supported software to ease the transition from the old configuration to the new.

Service requests will be opened for only one supported asset, that is, one service request will not involve multiple supported assets.

## **Patch Management and Support Methodology**

Patch management service delivery is focused on identifying applicable patches and distribute them through automated means to maintain Operating System (OS) compliance levels across government agencies. NTT DATA provides for the preparation, testing, staging, deployment, auditing, and ongoing management of operating systems and functional software patches for applications on servers, desktops, and laptops across the enterprise network.

Patch management is a key component in maintaining an updated and secure computing network. Proper patch management results in reduced incidents, improved application performance and uptime, and reduced security risk. This can help to significantly reduce the effort of distributing patches to government agencies laptops/PCs, enabling remote PCs to automatically receive patches anytime and anywhere they connect to the internet. The application allows administrators to efficiently monitor patch status and securely distribute patches from Microsoft and other leading vendors.

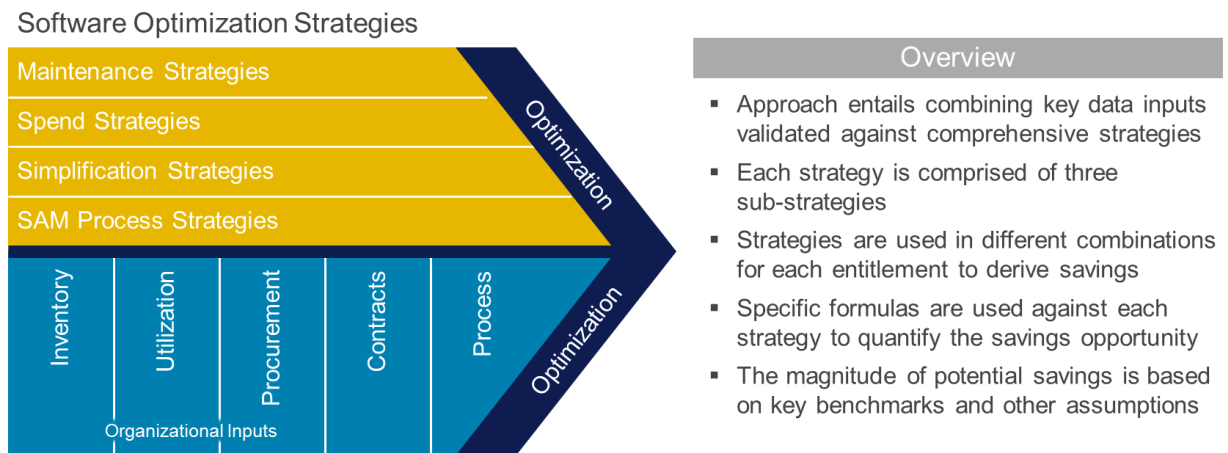
## **Software License Management & Optimization tool Reporting Capabilities**

NTT DATA will use standard reports to monitor usage of systems and identify unused licenses that can be re-allocated to different users or over-usage that needs to be remedied with new or re-assigned licenses.

### **Software License Optimization**

NTT DATA's Software Asset Management (SAM) solution team creates self-funding mechanisms by assessing our client's existing software portfolio. The alignment of the approved software catalog to the client's software portfolio enables the most effective and efficient utilization of resources going forward. Prioritizing the publishers contained in the corporate portfolio by total spend and agreement anniversary dates provides an evolutionary approach to software savings over time.

The integration of an automated software requisition process assures compliance and optimization of all software investments. This approach, depicted in the following graphic, renders Effective Licensing Position (ELP) statements for all publishers in the Definitive Software Library (DSL), which, in this case, will be the recommended Software License Management and Optimization tool:



*Figure 2: Software Optimization Strategies: Inventory, usage, procurement and contractual data is used to build Effective License Positions (ELPs). Key processes that affect optimization are reviewed on an ongoing basis.*

## OS/App Software Distribution and Deployment

NTT DATA provides electronic software distribution and the infrastructure conduit to distribute timely packaged applications and patch updates. This service component allows for software to be prioritized and scheduled for distribution to the desktop. This helps promote the optimal operation of the end-user computing environment.

## Image Management

NTT DATA's engineering team support Windows images (build/re-builds) in accordance with a government agency's requirements and prescribed standards. Image management is designed to simplify the complexities of software image development, validation, deployment, and maintenance. This service component helps our clients achieve platform stability and consistency while allowing them the flexibility to meet their specific business requirements.

The NTT DATA desktop engineering service team creates and manages new custom images supporting multiple desktop, notebook, and workstation platforms based on each clients' functional need, applications, operating systems, service packs, and system software and hardware drivers.

By producing a base image that is completely agnostic and can be applied universally we minimize image lifecycle management overhead while creating a standardized baseline for all devices. The build components allow for unique per-agency, per-person customization that provide the needed flexibility in a dynamic enterprise environment.

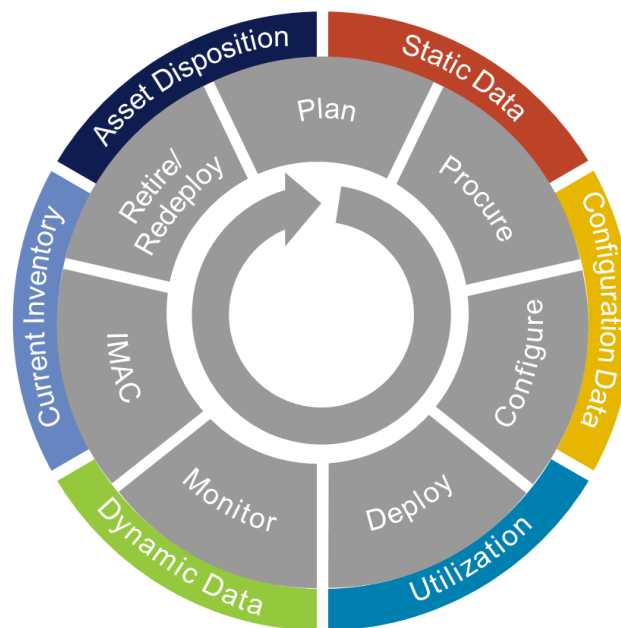
The introduction of new hardware and software standards into the production environment requires careful testing and acceptance. This ensures that the build environment meets the needs of GETs agencies and assists in the management of the customer's user expectations.

## Equipment Configurations - Hardware Asset Lifecycle

Our ITIL-aligned asset management team delivers an industry best practices approach to the management of each asset's lifecycle. This process leads to greater cost management, improved compliance, and mitigation of risks. We employ a process-centric approach to enable management and visibility of IT and business asset data elements from planning through asset retirement.

NTT DATA's asset management process ties together all aspects of the device/product lifecycle. Our asset management process consists of the following activities or processes:

- Initial entry and updates, through several methods:
  - Procurement/purchasing process
  - Automated discovery via current toolset
  - Change/request management processes
- Changes and validation
- Updates to the CMDB
- MONTHLY reconciliation process



*Figure 3: Hardware Asset Management Workflow*

## Software Configurations - Software License Management and Compliance

The software configurations typically focuses on end user software with the features below:

- Software Asset Management (SAM) representing the business practice that involves managing and optimizing the purchase, deployment, maintenance, utilization, and disposal of software applications within an organization
- Software License Management (SLM) representing the support for the processes and tools used by an organization to control and document where and how the company's software products are able to run in order to enforce and meet compliance with software licenses



# Virtualized Desktop Infrastructure Services

## Best practices for virtualized delivery

NTT DATA developed a comprehensive service portfolio and developed our own set of best practices over the course of many years of providing virtualization services to customers. We understand that every customer's needs and requirements are different, so we adopted a platform agnostic approach to virtualization. We first analyze the business requirements and project drivers and then recommend the right solution to meet the need.

Additionally we feel that the following best practices are key for successful virtualized deployments:

**Make decisions based on fact** – using analytics to drive desktop and application virtualization increases user adoption and user satisfaction

**Don't build an infrastructure that is not modular and cannot scale with your needs**

**Provide a blend of technologies and profiles to right-size delivery:**

- Offer persistent and non-persistent desktops
- Provide private resource and shared-session computing
- Incorporate access to virtual desktops and virtualized applications

## NTT DATA Virtual Workspace Services

A service practice built from years of real world experience		
DELIVERY TYPES	DELIVERY MODELS	DELIVERY PLATFORMS
Agile infrastructure <ul style="list-style-type: none"><li>• On-premise</li><li>• Private Hosted</li><li>• Public</li></ul>	Match user needs to delivery <ul style="list-style-type: none"><li>• Application only</li><li>• Virtual desktops</li><li>• Shared-session desktops</li></ul>	Deep expertise across platforms <ul style="list-style-type: none"><li>• Citrix XenApp / XenDesktop</li><li>• VMWare Horizon</li><li>• Microsoft, Nutanix, others</li></ul>
Industry leading practice professionals & technologies		
DELIVERY BEST PRACTICES		
Application Delivery	Published and streamed applications, application layering	
Image and persona management	User focused design matching users to efficient images/personas	
Infrastructure	Flexibility with business needs driving infrastructure decisions	
There is more to it than just "VDI"		
© 2017 NTT DATA, Inc.		
14		
NTT DATA		

Figure 4: NTT DATA Virtual Workspace Services

## Defining the Intent of VDI

Virtual Desktop Infrastructure is a term the industry uses to describe a very specific technology. For example VMware Horizon View and Citrix XenDesktop are the industry-leading solutions in providing full desktop features accurately labeled VDI. Various other technologies provide either desktop or virtualized application capabilities.

VDI technologies started up almost as long ago as Windows. Originally we used VDI to virtualize applications over Wide Area Networks (WANs) when client server applications required Local Area Network (LAN) capable speeds. This allowed remote resources to efficiently leverage applications that otherwise could not be used.

The core operating principal of VDI versus Mobile Device Management (MDM) or traditional managed PC is not well understood, leading to confusion as to why one implementation is better than another. Fundamentally VDI moves all processing away from the end point to the hosting location. The hosting location is most often the same data center that services core application and collaboration solutions. Increasingly; however, as application and collaboration resources move to the cloud, the hosting location becomes less important.

As an example, one of our clients is in the media and entertainment industry. Their core business is to design, simulate, and construct complex graphical content from several continents. As the entertainment business goes through its own digital revolution, Intellectual Property (IP) protection and ability to scale are the overriding concerns of their business. Without the ability to leverage cloud solutions and burst capacity, critical business operations may slow down causing the loss of business and/or production delay penalties.

Because VDI shifts all processing away from the end point it avoids all risks associated with local processing. For example:

- **Crashes:** Ultimately devices crash and tend to do so at the most inopportune time.
- **Lost data:** Even without security and IP risks, the potential for lost data, time and productivity resulting from an event cannot be avoided with local processing.
- **Lost productivity:** Recovery time to receive a new device and restart or reset lost work cannot be recovered.
- **Inconvenience:** Local processing devices only enable portability by moving the device. In contrast VDI sessions are portable regardless of device portability.

VDI is typically appropriate when one, or more, of these conditions exist:

- Connectivity to centralized applications and data
- LAN based, fixed location devices
- Remote connection capabilities degrade performance of applications that perform local processing
- Temporary access to remote resources
- High security requirements for environments containing Personal Health Information (PHI) and Personal Credit Information (PCI)
- Session stability in mission critical use cases
- Jurisdictional IP protection
- Geographic, weather, infrastructure, social, and other environmental instability situations

## VDI Services Catalog

**Table 2: NTT DATA's VDI Services Catalog Summary**

Services	Description
Turnkey Workspace-as-a-Service	<ul style="list-style-type: none"><li>• Hosted virtual desktops and applications delivered from NTT DATA's global data centers</li><li>• Infrastructure Estimation</li></ul>
Virtual Workspace Services	<ul style="list-style-type: none"><li>• NTT DATA will remotely manage and maintain an on-premise desktop and application virtualization solution, whether that resides</li></ul>

Services	Description
(VWS) Managed Services	<p>in your data center, a third-party data center, or even in a public cloud hosted solution.</p> <ul style="list-style-type: none"> <li>• Infrastructure Estimation</li> <li>• NTT DATA will deploy agents in your environments to capture metrics to help you understand how your users are currently consuming applications and resources and how their environments are currently performing.</li> <li>• Custom Design</li> </ul>
Service Desk	<ul style="list-style-type: none"> <li>• Maintains best practice operating standards for delivery of NTT DATA-provided scope</li> <li>• Industry standard ITIL service management techniques along with technologies such as ServiceNow (for ticket management) and Flexera (for managing software licenses).</li> <li>• Processes include change management, incident management, problem management, request management, knowledge management, root cause analysis, and others</li> <li>• NTT DATA will provide resolver group support for all in-scope services (Level 1, 2 and 3)</li> <li>• NTT DATA will make every effort to identify, recommend, enable, and implement optimization including moving activities to Level 0 (automation and self-service)</li> </ul>
Patch Management	<ul style="list-style-type: none"> <li>• Patch management service delivery is focused on identifying applicable patches and distribute them through automated means to maintain Operating System (OS) compliance levels</li> <li>• NTT DATA provides for the preparation, testing, staging, deployment, auditing, and ongoing management of operating systems and functional software patches for applications on servers, desktops, and laptops across the enterprise network</li> </ul>
Image Management	<ul style="list-style-type: none"> <li>• Image management is designed to simplify the complexities of software image development, validation, deployment, and maintenance</li> <li>• This service component helps our clients achieve platform stability and consistency while allowing them the flexibility to meet their specific business requirements</li> <li>• The NTT DATA desktop engineering service team creates and manages new custom images supporting multiple desktop, notebook, and workstation platforms based on each clients' functional need, applications, operating systems, service packs, and system software and hardware drivers</li> </ul>
Security Administration	<ul style="list-style-type: none"> <li>• Maintains an appropriate security posture as defined by government agency policy</li> <li>• This includes host intrusion and/or prevention measures (anti-virus, anti-malware) across device types, operating systems and form factors (Windows PC, MDM, and VDI)</li> </ul>

## Flexible Delivery Options

NTT DATA has three primary offerings for our customers interested in desktop and application virtualization solutions:

- Turnkey Workspace-as-a-Service
  - Hosted virtual desktops and applications delivered from NTT DATA's global data centers. NTT DATA provides both the virtual infrastructure and managed services to host customer's images and applications, which provide an easy interface for users to access your business applications anywhere, anytime, from any device.
- Virtual Workspace Services (VWS) Managed Services
  - NTT DATA will remotely manage and maintain an on-premise desktop and application virtualization solution, whether that resides in your data center, a third-party data center, or even in a public cloud hosted solution. Our virtualization experts will manage the infrastructure and platform end-to-end and free up your resources to focus on business initiatives.
  - NTT DATA will deploy agents in your environments to capture metrics to help you understand how your users are currently consuming applications and resources and how their environments are currently performing. The data returned from these agents will provide deeper insights into the overall end-user experience and helps ensure right-sized resource delivery.

For the Workspace-as-a-Service and Managed Services offerings, we support solutions based on VMware and/or Citrix, Microsoft, and other virtualization architectures. NTT DATA believes that there is no one virtualization solution that can meet every customer's requirements, so we have adopted a platform-independent virtualization practice, rather than focus on one product or technology.

This approach allows us to maintain the flexibility needed to deploy virtualized desktops and applications to users in the way that makes the most sense on a case-by-case basis. In every engagement we routinely see a mix of needing to provide some virtual desktops and some virtual applications but rarely is it entirely one or the other. Our end-user analytics platform will help make sense of how users are consuming resources today so we can design a solution to meet their needs.

# MDM Services Catalog

Smartphones and tablets are transforming the way we do business, allowing users to be more productive and responsive to business demands. In addition to corporate-liable devices, companies are opening access to employee-owned devices for email and enterprise access. And this expansion of mobility devices and services can place a strain on your IT staff with challenges such as tighter security requirements, new mobile applications and high expectations from end users. Mobile Device Management Services by NTT DATA offer you the tools and expertise to reduce costs via our proven solutions.

**Table 3: NTT DATA's MDM Services Catalog Summary**

Services	Description
Mobile Device Management (MDM), Bring Your Own Device (BYOD), and Choose Your Own Device (CYOD)	<ul style="list-style-type: none"><li>• By leveraging the our Enterprise Mobility Management (EMM) solution and integrating industry-leading technologies from partners such as VMWare Workspace One, our Mobile Device Management (MDM) technology provides the full end-to-end and seamless handhelds</li></ul>
Mobile Email Management	<ul style="list-style-type: none"><li>• Utilizing a fully integrated technology stack from vendors, such as Microsoft ActiveSync and VMware Workspace One, the mobile email management function enables secure business productivity and email application management for the government agency users</li><li>• Configuring and maintaining a secure access and data sharing to and of government agency resources using secure browsing, secure file access, and instant messaging capabilities</li></ul>
Mobility Infrastructure Support	<ul style="list-style-type: none"><li>• NTT DATA provides the management and monitoring of the mobility infrastructure and its integration points into the messaging, information security, networking, and content sharing environments, enabling an “as a service” model for your enterprise.</li></ul>
Service Desk	<ul style="list-style-type: none"><li>• Maintains best practice operating standards for delivery of NTT DATA-provided scope</li><li>• Industry standard ITIL service management techniques along with technologies such as ServiceNow (for ticket management) and Flexera (for managing software licenses)</li><li>• Processes include change management, incident management, problem management, request management, knowledge management, root cause analysis, and others</li><li>• NTT DATA will provide resolver group support for all in-scope services (Level 1, 2 and 3)</li></ul>

Services	Description
	<ul style="list-style-type: none"> <li>• NTT DATA will make every effort to identify, recommend, enable, and implement optimization including moving activities to Level 0 (automation and self-service)</li> </ul>
Asset and Configuration Management	<ul style="list-style-type: none"> <li>• Provides process integration to support inventory and status tracking of hardware and software assets during their lifecycle</li> <li>• We leverage best practice IT Infrastructure Library (ITIL)-compliant processes in our asset and configuration solutions</li> </ul>
Application Distribution	<ul style="list-style-type: none"> <li>• Support MDM (Workspace One) the conduit and primary mechanism to distribute mobile applications for supported mobile devices running iOS or Android.</li> <li>• Publish packaged internal mobile applications to the application catalog for self-service.</li> <li>• Publish applications that are publicly available from the Apple App Store or Google Play Store to the government agency MDM application catalog for self-service</li> <li>• Create and manage application assignment groups within MDM</li> <li>• Provide MDM reports on the mobile application delivery status</li> </ul>
Field Tech Support Services	<ul style="list-style-type: none"> <li>• Resolves service requests, diagnostics, and incident remediation that require hands-on support</li> <li>• These resources are typically dispatched by Levels 1 or 2 resources when remote diagnostics and/or service expectations dictate (such as VIP or concierge support)</li> <li>• These resources provide Install, Move, Add, Change, and Delete (IMACD) of devices to and from the operating environment</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Maintains an appropriate security posture as defined by government agency policy</li> <li>• Digital Certificates</li> </ul>

## How we deliver mobile device management

Our services combine industry-leading technology and expertise to automate and streamline the process of deploying and managing mobile devices and middleware infrastructure. We provide flexible delivery options for mobile device management (MDM), tailored to the supported environment and your unique specifications. For managed service configurations, we remotely support mobile infrastructure components and their integration points into the messaging, security and data sharing environment — enabling a seamless as-a-service delivery model for the managed mobility function. To support end users, our service provides Level 1 service desk support, focused on remediating end-user device access and usage issues. We answer common mobile device utilization questions and support provisioning and configuration enablement requests.

## Keep your mobile environment secure

Our services provide you with the tools to implement security policies and compliance strategies. You can configure and customize user roles to meet specific business requirements — assigning each user and administrator the permissions they need to execute their job responsibilities.

## Enable your applications

Our MDM application management module provides automatic deployment and control of applications on mobile devices. Based on customized criteria, it gives you the ability to automatically deploy business-critical mobility applications to users. Existing applications deemed unnecessary, can be removed, and users can be prevented from installing or reinstalling unapproved applications.

## Reduce IT support and labor costs

Our robust MDM feature set reduces IT support and labor costs for mobile devices. Our self-service portal lets employees provision and support their mobile devices without help desk intervention and streamlines your organization's provisioning and support process. Additionally, our real-time cost management feature helps you control costs associated with usage thresholds.

## Security

In the mobile landscape, digital certificates do more than act as a security gate for internal content. These certificates allow complete confidence in virtual interaction and discretion by providing:

- **Cross-platform Scalability:** Digital certificates can be leveraged to protect data across many different mobile platforms. Digital certificates can be used to securely transfer the same message via either email or instant messaging. The extensibility of certificate security allows organizations to avoid implementing multiple inferior single point security solutions that ultimately leave data vulnerable as it moves from point to point.
- **Multi-functionality:** Once a user or device receives a certificate, it can be utilized across many different platforms for a variety of purposes.
  - **Encryption:** Certificates can be used to encrypt digital information regardless of the platform. For example, the S/MIME standard leverages certificates for email encryption, while the HTTPS protocol utilizes SSL to provide web page encryption.
  - **Message Signing:** Enterprises in need of digital message signatures can leverage certificates in order to prove message integrity and show that the message originates from an authenticated sender and was not altered by any malicious third party. S/MIME can also provide email message signing to reassure the recipients that the sender is exactly who they say they are.
  - **Authentication:** Lastly, because digital certificates contain identifying information about both the user and the device that has been certified by a trusted source, certificates provide secure authentication into a number of systems such as email, Wi-Fi, and VPNs.
- **High Security:** Digital certificates are much more secure than traditional passwords because they are not susceptible to common password cracking methods such as brute force or dictionary attacks.

## Technical Integration

Integration points that may be of particular interest to a government agency may include: Microsoft (MS) Active Directory, Office365, OneDrive for Government, SharePoint, Certificates, Files Systems, and WebApps.

Each represent a move toward a more mobile, flexible workforce that allows for secure transmission of data as well as secure mechanisms for managing content types on devices whether corporate owned or BYOD.

An agency identity management application and MDM must be integrated into a common enterprise environment. At the basic level, this involves sharing the same directory structure. A common directory simplifies the operational aspects of the overall system, but also allows a consistent policy structure around AD group membership.