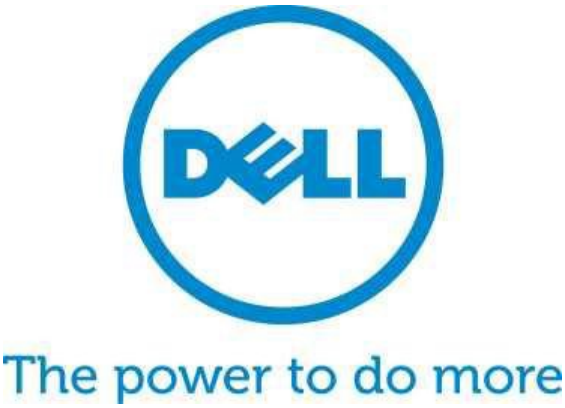
Dell Mobile Clinical Computing VMware® View Solution

Technisches White Paper von Dell



November 2012

Inhalt

Zielgruppe

Dieses White Paper ist für Testingenieure, Architekten und IT-Administratoren konzipiert, die am Entscheidungsfindungsprozess für die Planung, die Konfiguration und den Betrieb einer Desktop-Virtualisierungslösung im Gesundheitswesen beteiligt sind. Mit diesem Dokument sollen auch Lösungsarchitekten bei der Planung, dem Entwurf und der Bereitstellung der Dell Mobile Clinical Computing (MCC) Lösung unterstützt werden.

Einleitung

Das Gesundheitswesen ist heutzutage dynamisch und in hohem Maße auf die jeweils neueste Technologie angewiesen, um Diagnose und Behandlung zu beschleunigen und zu optimieren. Medizinisches Fachpersonal muss eine breite Palette an Endgeräten verwenden, um auf medizinische Anwendungen zuzugreifen, die lokal oder auf Servern in einem zentralisierten Rechenzentrum gehostet werden. Der Einsatz von Endgeräten war schon immer eine Herausforderung, weil häufig nicht alle benötigten Anwendungen auf jedem Gerät installiert sind. Deshalb muss das medizinische Fachpersonal unter Umständen warten, bis ein bestimmtes Endgerät verfügbar ist, wodurch die Patientenversorgung sich verzögern kann. Auch Sicherheits- und Compliance-Anforderungen bedeuten einen enormen Zeitaufwand. Sie erfordern oft, dass Benutzer ihre Anmeldeinformationen separat für jede Anwendung eingeben und sich auch für jede Anwendung separat wieder abmelden – und das bei jedem Raumwechsel. Im Laufe eines typischen Arbeitstags nimmt das sehr viel Zeit in Anspruch und ist schlicht unpraktisch – in vielen Kliniken verzichtet das Personal daher oft ganz auf eine ordnungsgemäße Abmeldung. Mit der **Dell Mobile Clinical Computing (MCC)** Lösung gehen Sie all diese Probleme effektiv an.

- Schnellere Verfügbarkeit von Endgeräten für das Klinik- und Pflegepersonal sowie schnellerer Zugriff und Neuzugriff
- Bereitstellung einer Instanz für einmaliges Anmelden (Single Sign-On, SSO), mit der das Klinik- und Pflegepersonal eine nahtlose Authentifizierung an Endgeräten und in mehreren Anwendungen durchführen kann
- Schneller und sicherer Zugriff auf Patienteninformationen nach Bedarf mithilfe von kontaktlosen und/oder biometrischen Authentifizierungsmethoden
- Weniger zeitaufwendige Clientverwaltung für IT-Mitarbeiter

Mit Dell MCC kann medizinisches Fachpersonal alle Vorteile der Desktop-Virtualisierung nutzen und gleichzeitig maximale Sicherheit gewährleisten, ohne den Klinik-Workflow zu beeinträchtigen. Die MCC Funktionen für Desktop-Virtualisierung sowie Identitäts- und Zugriffsverwaltung ermöglichen eine einmalige Anmeldung und eine sichere Authentifizierung. Wenn sich Pflegekräfte einem Terminal nähern oder sich an ihm anmelden, steht ihnen sofort der richtige Desktop zur Verfügung, mit allen benötigten Anwendungen und Patienteninformationen. Eine separate Authentifizierung für jede Anwendung oder gar jede Anwendungsebene ist nicht mehr notwendig. Pflegekräfte können sich nahtlos an jedem Endgerät in den Behandlungszimmern und in der Klinikumgebung anmelden und haben mehr Zeit für ihre Patienten. Sie können so mehr Patienten pro Woche (und pro Jahr) behandeln und ein höheres Serviceniveau bieten.

In einem weiteren White Paper haben wir im Rahmen europaweit durchgeführter Tests bereits nachgewiesen, dass unsere MCC Lösung auch im realen Klinikalltag hält, was sie verspricht*:

- Wöchentliche Produktivitätssteigerung von bis zu 215 Minuten und mehr pro Benutzer (Verbesserung um 9 %)
- Finanzieller Gewinn durch gesteigerte Produktivität von bis zu 11.500 € pro Jahr und Benutzer
- Angemessene Informationssicherheit ohne Beeinträchtigung der Benutzerfreundlichkeit
- Optimierung der Patientensicherheit, Versorgungsqualität und der Patientenzufriedenheit

Dell Mobile Clinical Computing (MCC)

Das Gesundheitswesen ist ein idealer Anwendungsfall für die Desktop-Virtualisierung, da dort verschiedenste Anforderungen und Probleme zusammentreffen: (1) Ein schneller Zugriff auf Anwendungen wie EMR wird benötigt, (2) Daten müssen geschützt werden, (3) Benutzersituationen und Anwendungen sind hoch spezifisch, (4) Geräte für Privatanwender, z. B. Tablet-PCs und Smartphones, bringen Sicherheitsrisiken mit sich und (5) IT-Abteilungen möchten Strukturen vereinfachen sowie anspruchsvolle (und sich möglicherweise widersprechende) Endbenutzeranforderungen erfüllen. Dell hat diese Herausforderung angenommen und eine flexible Lösung der Enterprise-Klasse speziell für das Gesundheitswesen entwickelt, die Kliniken innovative, praxisnahe Technologie, höchste Benutzerfreundlichkeit und perfekt auf die Klinikabläufe abgestimmte Funktionen an die Hand gibt.

Dell Mobile Clinical Computing (MCC) ist eine Lösung für Desktop-Virtualisierung sowie Identitäts- und Zugriffsverwaltung, die es medizinischem Fachpersonal ermöglicht, sicher, ortsunabhängig und von jedem Gerät aus auf Anwendungen und Daten zuzugreifen. Medizinische Einrichtungen müssen Pflegekräften eine hohe Produktivität ermöglichen und gleichzeitig strenge Datenverwaltungsauflagen einhalten, um Patientendaten bestmöglich zu schützen. Die Dell MCC Lösung bietet medizinischem Fachpersonal flexible, optimierte Datenverarbeitung – z. B. mit erhöhter Sicherheit, On-Demand-Zugriff auf Anwendungen und Daten, zuverlässiger Roaming-Konnektivität, Verfügbarkeit rund um die Uhr und verbesserter Rechenleistung. Gleichzeitig ermöglicht MCC der IT-Abteilung die zentrale Verwaltung aller Endbenutzerdaten und -Images, bei maximaler Endbenutzerflexibilität und -mobilität. Dank einer digitalen Identität und den zugehörigen virtualisierten Anwendungen, Desktops und Benutzerprofilen können Pflegekräfte von jedem beliebigen Gerät aus auf Anwendungen und Daten zugreifen und haben mehr Zeit, um die Patientenpflege weiter zu verbessern. MCC bietet Institutionen im Gesundheitswesen genau das, was sie brauchen:

- **Datensicherheit:** Daten werden im Rechenzentrum gespeichert, nicht auf dem Endgerät, wodurch das Risiko für Datendiebstahl oder -verlust effektiv erheblich reduziert wird. Multi-Faktor-Authentifizierung beugt nicht autorisiertem Zugriff vor.
- **Effizienter Klinikbetrieb:** Dank Lösungen für einmaliges Anmelden (Single Sign-On, SSO) können sich Benutzer schneller bei Anwendungen anmelden und haben so auch schneller Zugriff auf Patientenakten und andere wichtige Daten. Kontaktlose Chipkarten oder kontaktbasierte Smartcards ermöglichen dem Klinikpersonal eine einfache einmalige Anmeldung mit Authentifizierung. Zuverlässiges Sitzungs-Roaming ermöglicht den Zugriff auf virtuelle Desktops von jedem beliebigen Standort aus, über ein breites Portfolio an Endgeräten. Die völlige Unabhängigkeit von S und die Möglichkeit zum ortsunabhängigen Drucken sorgen für maximale Mobilität.
- **IT-Produktivität:** Die dynamische Bereitstellung von Benutzeranwendungen und -daten vereinfacht die Bereitstellung neuer virtueller Desktops. Dank zentralisierter Verwaltung aller virtuellen Images sind routinemäßige Wartung und Anwendungsaktualisierungen schnell und unkompliziert.

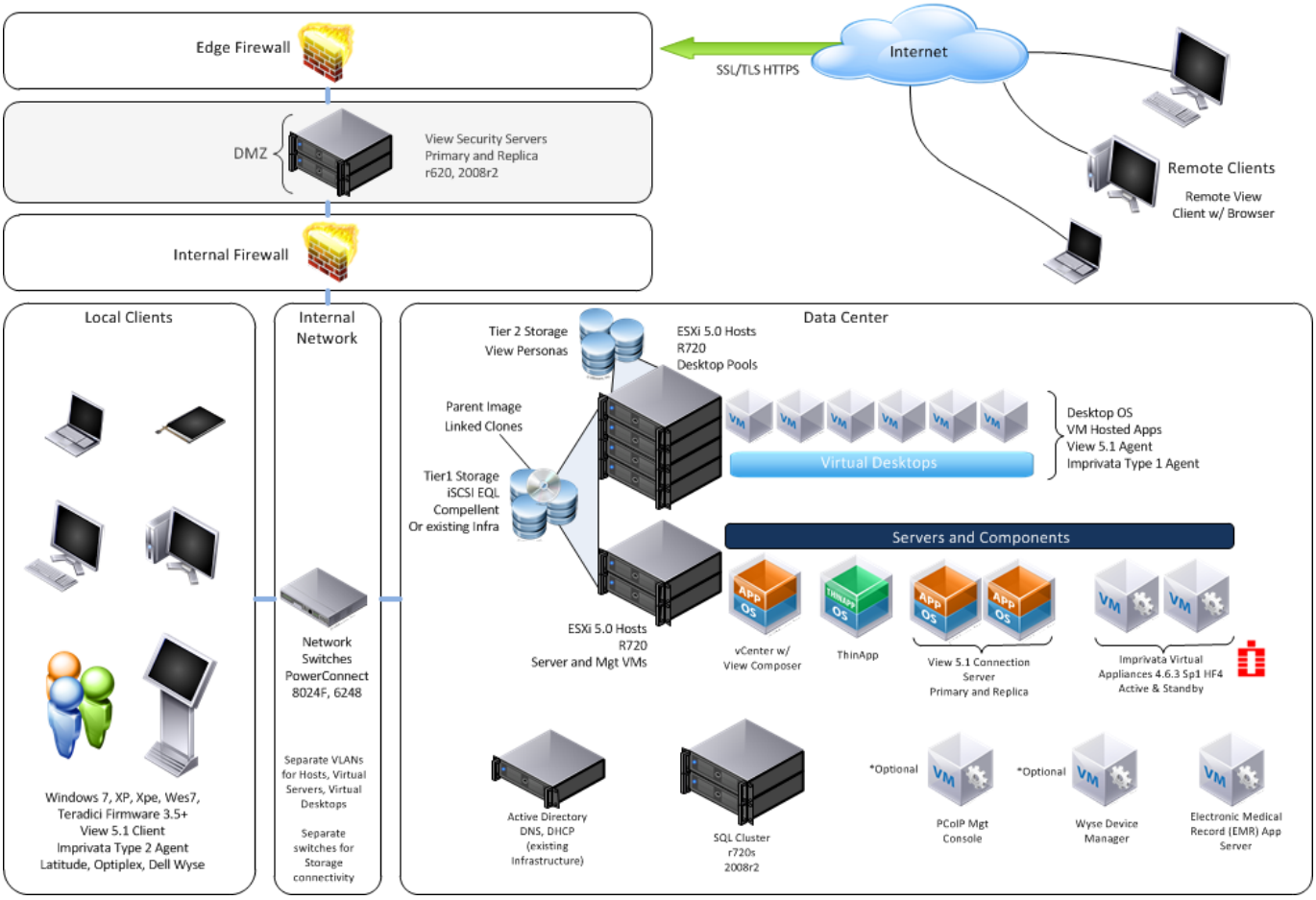
Die Dell MCC Lösung bietet Ihnen optimale Datensicherheit, einen effizienteren Klinikbetrieb und höhere IT-Produktivität. Ihre Schlüsselfunktionen:

- Schnelle, bedarfsgerechte Bereitstellung der richtigen Ressourcen, unabhängig von Standort oder Gerät
- Beschleunigter Benutzerzugriff über ID-Karten, biometrische Fingerabdrücke und Smartcards, wobei Anmeldedaten auf IT-Rollen basierenden Zugriffsdefinitionen unterliegen
- Nahtlose und zeitgebundene Übertragung von Sitzungsanmeldeinformationen und Benutzerdaten zwischen Workstation-Anmeldungsinstanzen, unterstützt durch Karten- oder Fingerabdruckanmeldung, sodass Benutzer den Sitzungsstatus geräteübergreifend beibehalten können
- Nahtlose Umleitung von Druckaufträgen an den Drucker, der dem jeweiligen Terminal am nächsten ist
- Automatisches Starten von Anwendungen, die im Benutzerprofil definiert sind
- Keine Notwendigkeit mehr für mehrere Kennwörter, dank Anwendungen mit einmaligem Anmelden
- Anpassung der Desktop-Umgebung entsprechend des Benutzerprofils
- Multi-Faktor-Authentifizierung über eine Kombination zweier beliebiger, von der MCC Lösung unterstützter Authentifizierungsmethoden, für zuverlässige Compliance mit Datenschutz- und Sicherheitsbestimmungen im Gesundheitswesen (z. B. HIPAA oder PCI)
- Benutzerfreundlichkeit

Referenzarchitektur

Dell MCC VMware View basiert auf der DVS Enterprise 6020 Lösung und wurde speziell für die neuen Dell Server der zwölften Generation optimiert. Die Referenzarchitektur umfasst Sitzungsmanagement, rollenbasierte Benutzer-arbeitsplätze sowie rollenbasierten Anwendungszugriff, einmaliges Anmelden, automatisierte Anwendungsstarts, Authentifizierung über kontaktlose Chipkarten oder kontaktbasierte Smartcards, Sitzungs-Roaming und schnelles Wechseln zwischen Benutzersitzungen auf Clientgeräten, die die definierten Kriterien erfüllen. Mit der Implementierung von Anwendungs- und Desktop-Virtualisierung wird die gesamte Desktop-Umgebung der Benutzer, einschließlich Betriebssystem, Anwendungen und Daten, von den Clientgeräten ins Rechenzentrum verlagert. So können Endbenutzerdaten, -anwendungen und -betriebssysteme zentral verwaltet werden, während gleichzeitig die Flexibilität auf Clientseite gesteigert wird und Endbenutzer sowohl lokal als auch remote auf benutzerspezifische Unternehmens-Desktops und Dell Clientsysteme zugreifen können.

Abbildung 1: Diagramm zur Referenzarchitektur der Dell MCC VMware View Lösung



Die Dell MCC VMware View Lösung ist in Rack- oder Blade-Server-Konfigurationen mit flexiblen Optionen für Tier 1- und Tier 2-Massenspeicher auf lokalen und/oder Dell EqualLogic™ oder Compellent Storage-Systemen verfügbar. Die Dell EqualLogic Storage-Plattform ermöglicht automatisierten Lastausgleich, Datenklassifizierung, Snapshots und Replikationen. In Tabelle 1 finden Sie nachfolgend eine Beispielkonfiguration für die Implementierung einer Kundenumgebung mit 500 gleichzeitigen Benutzern auf Dell Servern der zwölften Generation im Rack- oder Blade-Format sowie EqualLogic Storage-Lösungen.

Tabelle 1: Beispielkonfiguration für 500 gleichzeitige Benutzer

500 gleichzeitige Benutzer	Rack-Konfiguration	Blade-Konfiguration
Hoch verfügbare Infrastruktur	Sechs Clienthostserver: PowerEdge™ R720 Zwei Verwaltungsserver: PowerEdge R720 T1-Massenspeicher: Lokaler Massenspeicher Zwei ToR-Switches: PowerConnect™ 8024F	Ein Blade-Gehäuse Sechs Clienthostserver: PowerEdge M620 Zwei Verwaltungsserver: PowerEdge M620 T1-Massenspeicher: ein EqualLogic™ PS6110XS Blade-Switches: zwei PowerConnect M6348, zwei PowerConnect 8024-K Zwei ToR-Switches: PowerConnect 8024F
Virtualisierungssoftware	500 VMware View 5.1 Premier Dell Edition Lizenzen einschließlich View Persona Management AlwaysOn Desktop (optional für zusätzliche Notfall-Wiederherstellung und Hochverfügbarkeit)	
Software für die Identitäts- und Zugriffsverwaltung	Zwei Imprivata OneSign Appliances (optional physisch oder virtuell, virtuelle Konfiguration ist in Abbildung 1 dargestellt) 500 Lizenzen für Authentifizierungsverwaltung und einmaliges Anmelden Secure Walk-Away™ und OneSign Self-Service Password Management™ optional (siehe Seite 14)	
Multi-Faktor-Authentifizierung*	Kennwort, Pin, kontaktlose Chipkarten oder Smartcards*, biometrisch (* Beispiele für Smartcards siehe Anhang 1.0, Seite 24)	
Endgeräte	Dell Wyse Zero Clients (PCoIP oder RDP), Thin Clients (WES 7) Dell Latitude™ und OptiPlex™	
Verwaltungssoftware	Dell Wyse Device Manager (WDM)	

** Smartcard-Lesegeräte sind hardwareabhängig und nicht im Lieferumfang enthalten.*

Dell Desktop-Virtualisierungslösung (DVS) Enterprise

Die Dell MCC VMware View Lösung basiert auf der Dell DVS Enterprise Architektur. Diese wiederum baut auf den neuen PowerEdge™ Servern der zwölften Generation sowie VMware vSphere und View 5.1 auf.

Dell PowerEdge Server der zwölften Generation bieten höhere Arbeitsspeicherkapazität und mehr integrierte E/A-Vorgänge (Eingabe/Ausgabe) als die vorherige Generation. Dieses Plus an Kapazität ist ein entscheidender Parameter für Virtualisierungsleistung und Skalierbarkeit. Dank Intel® Xeon® Prozessoren mit mehreren Kernen, zusätzlichen DIMM-Steckplätzen, PCIe-Gen 3-Erweiterungssteckplätzen und der Möglichkeit, Hypervisoren per Secure Digital (SD)-Karte oder interner USB-Lösung zu integrieren, können Kliniken jetzt die Anzahl virtueller Maschinen pro Server ebenso maximieren wie die Verarbeitungsleistung ihrer virtuellen Umgebung. Werden PowerEdge Express Flash Solid-State-Festplatten direkt an CPU und Speicherbus angeschlossen, können Dell Server der zwölften Generation jetzt bis zu 18-mal mehr Microsoft® SQL Server® Transaktionen pro Sekunde durchführen.

Diese PCIe-SSD-Festplatten (PCI Express) sorgen für höhere Datenbank-, Anwendungs- und E/A-Leistung, sodass das Klinikpersonal Daten noch schneller optimal auswerten kann. Die Dell PowerEdge Server der nächsten Generation setzen in medizinischen Einrichtungen neue Maßstäbe in Sachen IT-Effizienz und ermöglichen Innovationen in der IT-Umgebung. Sie können nicht nur bis zu 50 % mehr virtuelle Maschinen ausführen als vorherige Generationen – dank Intel® Xeon® Prozessortechnologie können Server aus mehreren Generationen im selben virtualisierten Serverpool kombiniert werden. Failover, Lastausgleich und Notfall-Wiederherstellung werden so weiter optimiert.

Dell DVS Enterprise bietet unter anderem die folgenden zusätzlichen Vorteile:

- **Kosteneffizienz:** Kliniken können VDI-Pilotprojekte (50 bis 500 Arbeitsplätze) jetzt selbst starten, wahlweise auf Basis neuer oder vorhandener Dell Hardware oder auf Basis vorhandener Massenspeicher- und Netzwerkhardware anderer Anbieter. Die Blueprint- und die Hochverfügbarkeitsfunktion sind für weniger als 500 Arbeitsplätze jetzt optional, wodurch in der Testphase erhebliche Kosten eingespart werden können. Wenn der Pilotversuch positiv verläuft, können sie auf mehrere Tausend virtuelle Arbeitsplätze erweitert werden. Hierbei kann ein Großteil der in der ersten Investitionsphase erworbenen bzw. verwendeten Hardware weiter genutzt werden. Ein Komplettaustausch ist nicht notwendig.

- **Flexibilität:** DVS Enterprise ist jetzt für weitere Dell Hardware qualifiziert, einschließlich der neuesten Systeme (Dell Server der zwölften Generation sowie ausgewählte PowerConnect™ und Force10 Netzwerk-Switches). Das Lösungspaket funktioniert auch auf Massenspeicher- und Netzwerkeinheiten anderer Anbieter. So können Organisationen vorhandene, qualifizierte Hardware zur Implementierung einer zuverlässigen VDI-Lösung verwenden.

- **Skalierbarkeit:** Wenn ein Kunde die Anzahl virtueller Desktops erweitert, kann DVS Enterprise nahtlos mit neuer Hardware skaliert werden. Jegliche zuvor erworbene Hardware verbleibt weiter im Einsatz. So können Betriebskosten auch auf lange Sicht effektiv reduziert werden, gleich ob für Infrastrukturen mit 50 oder Tausenden von Benutzern. Des Weiteren ist das Dell Serviceportfolio modular aufgebaut und kann jederzeit an Ihre spezifischen Anforderungen angepasst werden. So findet jede Klinik die für Sie passende Lösung. Wir möchten ein zuverlässiger Partner für Einrichtungen im Gesundheitswesen sein und unseren Kunden maßgeschneiderte Unterstützung bieten, die ihre individuellen Bedürfnisse, Ressourcen und Spezialisierungen berücksichtigt.

- **Leistung:** Die Dell Lösung baut auf der neuesten Hardwaregeneration (Server, Massenspeicher, Netzwerke) auf. Sie haben Zugriff auf die schnellsten Prozessoren, die höchstmögliche Arbeitsspeicherkapazität, den derzeit niedrigsten Energieverbrauch sowie schnelle Netzwerktechnologie und können sich sicher sein, dass Ihre Investition sich langfristig auszahlt. Ergänzt wird die innovative Hardware durch Schlüsselsoftware aus unserer Kompatibilitätsliste (SCL), die von Dell getestet und empfohlen wurde, optimale Leistung garantiert und die Kosten pro virtuellem Desktop deutlich senkt. Die Integration der neuesten Versionen der VMware Virtualisierungssoftware stellt sicher, dass Benutzer stets Zugriff auf die aktuellste Technologie mit all ihren Vorteilen haben.

VMware View 5.1

- **VMware View** ist eine Lösung für die Desktop-Virtualisierung, mit der virtuelle Desktops, Anwendungen und Daten über das Rechenzentrum bereitgestellt werden können. VMware View gibt Ihnen eine umfassend skalierbare Schnittstelle für optimierte Verwaltung und schnellere Desktop-Bereitstellung an die Hand. Dank erweiterter rollenbasierter Verwaltung und zentralisierten Richtlinien für die Desktop-Sicherheit gewährleistet die Lösung umfassende Kontrolle über Ihre Desktop-Umgebung bei maximalem Schutz.

- **vCenter Server** bietet zentrale Verwaltungsfunktionen für über VMware vSphere virtualisierte Serverumgebungen. IT-Administratoren haben so deutlich umfassendere Kontrollmöglichkeiten als bei vergleichbaren Verwaltungsplattformen.

- **View Connection Server** ist eine Brokering-Lösung, die mit vCenter kommuniziert, um die Verwaltung virtueller Desktops zu ermöglichen. Sie umfasst die Erstellung virtueller Desktops, Funktionen für die Poolverwaltung sowie Steuermöglichkeiten für den Betriebszustand, beispielsweise das automatische Anhalten und Wiederaufnehmen. Für Redundanz kann Connection Server auch in einer Active/Passive-Konfiguration bereitgestellt werden.

- **View Composer** ist ein Softwareservice, der auf dem vCenter Server installiert ist. Über ihn Images verwaltet sowie mehrere, verlinkte Desktop-Klone von einem einzigen, zentralen Basis-Image aus erstellt werden. So ist es möglich, Benutzereinstellungen beizubehalten und gleichzeitig die Massenspeicheranforderungen zu senken.

- **VMware ThinApp** abstrahiert Anwendungen vom zugrunde liegenden Betriebssystem und sorgt so für effiziente Anwendungsvirtualisierung. Die Anwendungen werden in einzelne ausführbare Dateien gepackt, die sowohl voneinander als auch vom Betriebssystem isoliert sind und jederzeit konfliktfrei auf Endgeräten ausgeführt werden können. Die ThinApp Anwendungspakete können auf unterschiedlichen Windows Plattformen bereitgestellt werden.

- **VMware Security Server** bietet einen sicheren Zugriff auf den View Connection Server und ermöglicht es Benutzern, über das Internet auf den virtualisierten Desktop-Pool zuzugreifen.

- **View Persona Management** (nur View Premier Edition) weist zustandslosen Floating-Desktops dynamisch Benutzerprofile zu. Damit können IT-Administratoren die Migration von physischen zu zustandslosen virtuellen Desktops optimieren und alle Benutzereinstellungen beibehalten.

- **View Storage Accelerator** sorgt dafür, dass beim Lesen virtueller Desktop-Images gemeinsam genutzte Image-Blöcke zwischengespeichert werden. Das reduziert die Massenspeicherlast während so genannter Boot-Storms, d. h., wenn viele Systeme gleichzeitig hochgefahren werden.

- **View Enhanced USB** macht die Installation eines Gerätetreibers auf Clientseite überflüssig. Ein generischer USB-Arbitrator wird auf Clientseite implementiert, ein Standard-USB-Hub im Agenten. So kann VMware View eine breitere Palette an USB-Geräten unterstützen und sogar auf Multifunkions-USB-Geräten hoch detaillierte Remote-Geräte-Richtlinien durchsetzen (z. B. Aktivieren/Deaktivieren von Massenspeicher-Dateikopien).

Client- und Endgeräte

Endgeräte, die im Gesundheitswesen eingesetzt werden, müssen jederzeit zuverlässig arbeiten. Dell Wyse Thin Clients haben keine beweglichen Teile, wie Festplattenlaufwerke, die ausfallen könnten. Ihre Laufzeit ist in der Regel doppelt so lang wie die herkömmlicher Desktop PCs, was nicht nur für geringere Anschaffungskosten sorgt, sondern auch Aktualisierungszyklen überflüssig macht. Außerdem stellt die zentralisierte Verwaltung optimale Systemleistung sicher, da Updates und Patches remote in wenigen Minuten durchgeführt werden können und hierzu weniger IT-Mitarbeiter notwendig sind als für die Wartung von Legacy-Endgeräten.

Hier einige Beispiele für Zugriffsszenarien mit Dell Wyse Thin und Zero Clients:

- In der Notaufnahme zeigt ein Patient eine atypische Reaktion auf die Anästhesie. Der Chirurg ruft die Patientenakte in Sekunden auf, um Angaben zu Allergien nachzulesen und alternative Behandlungsmöglichkeiten zu finden.
- Das Klinikpersonal überprüft selbst die Rezeptbestellung, bevor ein Medikament ausgegeben wird, und muss sich nicht mehr beim zuständigen Arzt rückversichern.
- Im Krankenzimmer überprüft eine Pflegekraft die geplante Schmerzmedikation und kann dem Patienten mitteilen, wann die nächste Dosis verabreicht wird, ohne erst im Schwesternzimmer nachsehen zu müssen.
- Ein Arzt meldet sich am Dell Wyse Cloud Client über die PocketCloud Remote Desktop Software an, um eine Patientenakte zu lesen und eine Frage außerhalb der Sprechstunde zu beantworten.

Mit Dell Wyse Thin und Zero Clients stehen Pflegekräften schon Sekunden nach der Anmeldung Ihre persönlichen Desktop-Daten und -Anwendungen zur Verfügung. Auf einem Endgerät können so mehrere separate, absolut sichere Sitzungen direkt nacheinander ausgeführt werden, ohne Risiko, dass Daten unbefugt eingesehen werden können. Dank der Unterstützung für eine sichere integrierte Authentifizierung per einmaligem Anmelden können Benutzer sich über ein kontaktloses Chipkarten-Lesegerät in Sekunden an einer sicheren, personalisierten Desktop-Umgebung anmelden. Mobile Clinical Computing (MCC) Endgeräte müssen einen lokalen Agenten innerhalb des Gerätebetriebssystem ausführen. Zu den unterstützten Betriebssystemen zählen die 32- und 64-Bit-Versionen von Windows® 7 auf Dell Latitude™ Notebooks und Dell OptiPlex™ Desktop-PCs sowie integriertes WES7 (Windows® 7) auf Dell Wyse Thin und Zero Clients mit Teradici Firmware Version 3.5 oder höher. Endgeräte können so konfiguriert werden, dass Benutzer sich lokal an einem Gerät anmelden. Für den OneSign Agenten müssen jedoch noch immer alle konfigurierten Authentifizierungsrichtlinien erfüllt werden. Der Clientagent wird auch auf den übergeordneten Images der virtuellen Maschinen installiert.

In der nachstehenden Tabelle sehen Sie welche Funktionen in einer MCC Umgebung auf welchen Dell Clientprodukten zur Verfügung stehen.

Tabelle 2: MCC Funktionen von Client-/Endgeräten

Gerätefamilie	Typ	Betriebssystem	SSO	Karte	SWA*	Fingerabdruck-Lesegerät	Multi-Faktor-Authentifizierung
Dell OptiPlex™	Desktop-PC	Windows® 7	✓	✓	✓	✓	✓
Dell Latitude™	Notebook	Windows® 7	✓	✓	✓	✓	✓
Dell Wyse P20/P25	Zero Client	–	✓	✓			✓
Dell Wyse Z90x	Thin Client	WES7 oder WES 2009	✓	✓	✓	✓	✓
Dell Wyse C90x	Thin Client	WES7 oder WES 2009	✓	✓	✓	✓	✓
Dell Wyse R90x	Thin Client	WES7 oder WES 2009	✓	✓	✓	✓	✓
Dell Wyse X90x	Thin Notebook	WES7	✓	✓	✓	✓	✓
Dell FX100	Zero Client	–	✓	✓			✓

* Secure Walk-Away

Dell Wyse Zero Client Geräte

Dell Wyse P20 (und bald auch P25) Zero Clients können als kontaktlose Chipkarten-Endgeräte in MCC View/OneSign Implementierungen verwendet werden. Authentifizierung über kontaktlose Chipkarten wurde zuerst im Dezember 2011 in der Teradici Firmware Version 3.5 eingeführt. Aktuell ist im Lieferumfang des Dell Wyse P20 die Firmware Version 4.0 enthalten. Sie wird in View/OneSign Umgebungen vollständig unterstützt. Diese Version der Firmware ermöglicht P20 eine Kommunikation mit der OneSign Appliance und schützt das Gerät, indem der OneSign Login-Dialog eingeblendet wird, noch bevor die sonstigen Anmeldeaufforderungen für die Domäne oder das Gerät angezeigt werden. Die zulässigen Authentifizierungsmöglichkeiten sind Benutzername/Kennwort, kontaktlose Chipkarten und/oder PIN. Sie können beliebig kombiniert werden, um eine Multi-Faktor-Authentifizierung in der Umgebung und in den Anwendungen umzusetzen.

Obwohl alle Dell Clientgeräte mit Unterstützung für MCC vielseitige Benutzerfunktionen bieten, ist die Leistung von Dell Wyse P20 Zero Clients in der MCC View/OneSign Konfiguration einzigartig. Die Dauer für die erste Anmeldung und für den Sitzungstransfer beträgt in VMware View Desktop-Gruppen, die über RDP- oder PCoIP-Protokolle verbunden sind, durchschnittlich fünf Sekunden. Dell Wyse P20 reduziert die Dauer und die Kosten für die Sicherung und Wartung herkömmlicher Desktop-PCs durch zentralisierte Bereitstellungen, Updates, Patches und Verwaltung erheblich. Mit dem Dell Wyse P20 ist ein zeit- und standortunabhängiger Zugriff auf personalisierte Desktops über kompakte Endgeräte möglich, die einfach hinter Bildschirmen, in Krankenzimmern oder in der Notaufnahme eingerichtet werden können. Wireless-Modelle sind außerdem perfekt für Roaming-EMR und Workstation-Zugriff geeignet. Darüber hinaus benötigen P20 Zero Clients sehr wenig Strom – etwa 90 % weniger als herkömmliche PCs. So können medizinische Einrichtungen Tausende Euro pro Jahr bei den Kosten für Heizung, Belüftung und Klimatisierung sparen. Dank des niedrigen Energieverbrauchs, des geringen Platzbedarfs, der minimalen

Angriffsfläche, der überzeugenden Leistungsmerkmale und der umfassenden zentralisierten Verwaltung mithilfe von Wyse Device Manager ist Dell Wyse P20 die ideale Wahl für jede medizinische Einrichtung.

Der Dell Wyse P20 Zero Client ist die marktführende Desktop-Virtualisierungsplattform für VMware View 5, die Imprivata OneSign Virtual Desktop Access™ und Teradici PCoIP Firmware Version 3.5 integriert und so die Benutzererfahrung eines PCs mit sicherer Authentifizierung kombiniert.

Dell Wyse P20 Zero Client

Dell Wyse Zero Clients erleichtern die elektronische Dokumentation von Patientenakten, um eine strenge Einhaltung von Compliance-Anforderungen und schnelleren, zuverlässigeren Zugriff auf kritische Daten und lebenswichtige Anwendungen sicherzustellen. Mit Imprivata OneSign Virtual Desktop Access müssen Pflegekräfte eine kontaktlose Chipkarte nur an ein Authentifizierungs-Lesegerät halten, das mit dem Dell Wyse P20 verbunden ist. Innerhalb von Sekunden wird die Sitzung auf einem personalisierten Desktop fortgeführt, ohne dass eine Anmeldung notwendig ist.

Zu den weiteren Vorteilen von Dell Wyse P20 zählen:

Einfach: Die sichere Anmeldung dauert nur sechs Sekunden mit einer kontaktlosen Chipkarte.

Äußerst schnell: Schnelle Bereitstellung vielfältiger Roaming-Desktops mit allen Benutzerdaten und Anwendungen

Sehr sicher: Kein Risiko für Diebstahl, Manipulationen oder Verlust. Durch die zentralisierte Verwaltung aller Anwendungen und Daten werden Betriebs- und Wartungskosten reduziert und es wird eine richtlinienbasierte Zugriffssteuerung ermöglicht.

Kostengünstig: Die skalierbare Bereitstellung senkt die Investitionsausgaben für wachsende Organisationen. Der niedrige Stromverbrauch – bis zu 90 % geringer als bei Desktop PCs – reduziert Kosten für Strom und Kühlung.

Leistungsstark: Höchste Leistung und brillante Grafikverarbeitung

Gute Konnektivität: Einfache Konnektivität mittels Ethernet über LAN oder WAN mit vier USB-Ports, um eine Vielzahl an Peripheriegeräten, einschließlich Lesegeräten für kontaktlose Chipkarten, anzuschließen

Einfach zu verwalten: Mit der zentralen Verwaltung können die Sicherheit erhöht und die Bereitstellung, Wartung und Aktualisierung vereinfacht werden.

Umweltfreundlich: Benötigt weniger als 15,5 Watt bei Vollbetrieb

Vielseitige Benutzerfunktionen: Unterstützung mehrerer Bildschirme dank Multimedia-Wiedergabe und HD-Audio

Dell Wyse P25 Zero Client

Der Dell Wyse P25 Zero Client der nächsten Generation kann auch als Endgerät für kontaktlose Chipkarten in MCC View/OneSign Implementierungen verwendet werden. Der Zero Client verwendet die aktuellen Tera 2 PCoIP-Prozessoren von Teradici in Verbindung mit einer Zwischenspeicherung auf Clientseite, um die verfügbare Netzwerkbandbreite zu optimieren. Bei Bedarf können zwei HD-Bildschirme unterstützt werden und es wird mit nur 8 Watt erheblich weniger Energie als beim P20 verbraucht, wenn der P25 an eine Tastatur, eine Maus oder einen Bildschirm angeschlossen ist. Dank seines wesentlich kleineren Formfaktors kann er noch einfacher an der Rückseite eines Monitors angebracht werden.

Bei der Verwendung des P25 in einer MCC View/OneSign Umgebung ist es wichtig, die Bildschirmauflösung von Monitor und virtueller Maschine aufeinander abzustimmen. (Wenn die Werte nicht übereinstimmen, wird die virtuelle Maschine nicht angezeigt.)

Imprivata OneSign 4.6

Imprivata OneSign ermöglicht eine sichere Authentifizierung und einmalige Anmeldung an Anwendungen, sodass Ärzte und Pflegekräfte nicht mehrere unterschiedliche Kennwörter kennen und eingeben müssen. Außerdem gelingt die Anmeldung schneller. Kliniken können so ihre Compliance-Anforderungen leichter einhalten. Mit OneSign werden auch die identitätsorientierte Authentifizierung und Zugriffsdienste über System- und zeitliche Grenzen hinweg durch vollständig verteilte Verwaltung, delegierte Administration und unterbrechungsfreien Betrieb erweitert. Die integrierte Authentifizierungsverwaltung, die einmalige Anmeldung, der Remote-Zugriff und die Funktionen von OneSign ermöglichen es medizinischen Einrichtungen, eine einzige zentralisierte IT-Zugriffsrichtlinie für Mitarbeiter erfolgreich zu etablieren, die sämtliche Zugriffsaspekte für alle Benutzer, Berechtigungen, Standorte und Bedingungen regelt.

- **Die OneSign Server Appliance** ist eine maßgeschneiderte physische oder virtuelle Appliance, die äußerst sicher ist und keine Änderungen an der vorhandenen IT-Infrastruktur der Organisation, einschließlich des AD-Schemas, erfordert. Die physische Appliance umfasst 1 HE. Die Bereitstellung zweier Appliances sorgt für integrierte Redundanz und, falls notwendig, für automatischen Failover bei laufendem Betrieb. Mit der Appliance werden Benutzerkennwörter, Benutzerprofile, Anwendungsprofile und Authentifizierungsmethoden verwaltet. In Kundenumgebungen, in denen kontaktlose Chipkarten bereits für den Zugang zu Gebäuden verwendet werden, können vorhandene Chipkarten in manchen Fällen auch für die MCC Authentifizierung genutzt werden.

- **OneSign Agent** befindet sich auf den Workstations und auf virtuellen Desktops auf der Clientseite und dient der Verwaltung von Benutzerzugriff und dem Upload der Benutzeraktivitätsdaten in die OneSign Appliance. In einer Zero Client Umgebung ist der OneSign Agent in die Geräte-Firmware integriert. Der Agent verarbeitet die Authentifizierung der Benutzer lokal über ID-Karten, biometrische Fingerabdrücke oder einmalige Tokens und Kennwörter. Sobald ein Benutzer auf dem OneSign System authentifiziert wird, kann der Benutzer automatisch an bereitgestellten Anwendungen angemeldet werden, wenn diese gestartet werden. Der OneSign Agent ist für die lokale Weiterleitung der Benutzeranmeldedaten an Anwendungen und Domänen zuständig. Er lädt Anmeldedaten und Anwendungsinformationen bei der Anmeldung von der OneSign Appliance herunter und fragt in vom OneSign Administrator festgelegten Abständen Änderungen ab. Der Agent versetzt die Appliance bei Bedarf in den Standy-Modus und wechselt automatisch zur Hot-Standby-Appliance, wenn die Verbindung zur primären Appliance unterbrochen wird.

- **OneSign Administrator UI** ist eine webbasierte Schnittstelle zur Verwaltung aller Aspekte der OneSign Konfiguration, einschließlich der Benutzer, Anwendungen, Agent-Einstellungen, Kennwortautomatisierung und Überwachungsberichte.

- **Einmaliges Anmelden (Single Sign-On, SSO)**: ermöglicht höhere Sicherheit durch das einmalige Senden von Anmeldedaten zur Authentifizierung. Die einmalige Anmeldung erhöht die Sicherheit für Benutzer, die Zugriff auf vertrauliche Daten haben. Anwendungen, für die für einen Zugriff Anmeldedaten erforderlich sind, verfügen über ein Profil in der SSO-Lösung. Sobald das Anwendungsprofil erzeugt wurde, werden Benutzer einmal aufgefordert, die Anmeldedaten für diese Anwendung einzugeben. Beim erstmaligen Einloggen zu Beginn der Schicht werden die Anmeldedaten jedes Mitarbeiters für dessen Benutzerprofil gespeichert. Bei darauf folgenden Login-Versuchen werden die Anmeldedaten der Benutzer nicht wieder abgefragt, sondern automatisch eingefügt. Der Authentifizierungsprozess wird somit maßgeblich vereinfacht. Die Richtlinien können so festgelegt werden, dass Benutzer ihre eigenen Kennwörter verwalten können. Durch die Benutzerfreundlichkeit und zusätzliche Sicherheit der erweiterten Authentifizierung mit einmaligem Anmelden (Single Sign-On, SSO) über Ausweise, Karten und/oder biometrische Authentifizierung tritt diese Option jedoch in den Hintergrund.

- **Sitzungs-Roaming**: Durch Session Roaming kann das Risiko der ungewollten Kennwortfreigabe oder der gemeinsamen Nutzung von Benutzerkonten minimiert werden, das beim Anwendungszugriff durch Benutzer, die sich an mehreren Computern anmelden, entsteht. Über mehrere gemeinsam genutzte MCC Clients wird ein unternehmensweiter benutzerspezifischer Arbeitsplatz bereitgestellt. So wird das Risiko der Kennwortfreigabe maßgeblich reduziert und Benutzer haben die Möglichkeit, bei jeder Sitzung und an jedem System in individualisierten Betriebssystemumgebungen mit angepassten Anwendungen zu arbeiten. Um die Geschwindigkeit des Sitzungs-Roamings zu beschleunigen, bleibt die Sitzung solange in einem statischen Zustand aktiv, bis sich der Benutzer endgültig abmeldet. In diesem statischen Zustand kann die Sitzung von jedem beliebigen Endgerät im Unternehmen aus fortgeführt werden.

- **Rollenbasierter Zugriff**: Benutzer können ausschließlich die Anwendungen nutzen, für die sie aufgrund ihrer Rolle eine Berechtigung besitzen. Dadurch wird garantiert, dass der Anwendungszugriff nur berechtigten Benutzern möglich ist. IT-Administratoren können mithilfe von Richtlinien festlegen, ob der Zugriff auf Grundlage des Status, der Rolle, der Ausweis-ID und/oder des physischen Standorts des Mitarbeiters gewährt oder abgelehnt wird. Benutzerprofile werden innerhalb der SSO-Lösung erstellt und mit den Anmeldedaten des Benutzers gekoppelt. Mithilfe von Profilen kann auch bestimmt werden, mit welchem Image der virtuelle Desktop des Benutzers erstellt wird. Krankenschwestern kann so beispielsweise ein Windows 7-basierter Desktop zugewiesen werden, während Techniker einen Windows XP-basierten Desktop erhalten.

- **Sicherheitsserver/Gateway**: für Remote-Benutzer; verschlüsselte Zugriffspunkte vom Internet bis zu den Rechenzentrumsservern mittels SSL (HTTPS)

    1. Transparente Verschlüsselung und Authentifizierung aller Verbindungen zum Schutz vor potenziellen Bedrohungen
    2. Verweigerung des direkten Zugriffs auf interne Unternehmensressourcen über das Internet
    3. Mögliche Nutzung von zweistufiger Authentifizierung ohne Konfiguration der Serverinfrastruktur
    4. Bereitstellung einer vereinfachten Client-Firewall

- **Sicherer Zugriff auf Endgeräte:** Endbenutzergeräte werden mit Sicherheitssoftware für die einmalige Anmeldung (SSO) und starke Authentifizierung ausgestattet, die zentral im Rechenzentrum verwaltet wird. In einem vom Systemadministrator festgelegten Intervall ermitteln die auf den Endgeräten installierten Agenten über die SSO-Lösung, ob Updates zur Verfügung stehen oder Sicherheitsrichtlinien verändert wurden. Dieses Intervall kann je nach Bedarf festgelegt werden. Es können mehrere Sicherheitsprofile festgelegt werden, die verschiedene Authentifizierungsschritte erfordern. Für eine mehrstufige Authentifizierung in Bereichen, in denen höhere Sicherheitsanforderungen herrschen, kann so beispielsweise die Überprüfung des biometrischen Fingerabdrucks mit einer Smartcard oder einer PIN-Nummer kombiniert werden.

- **Authentifizierung:** Authentifizierungsoptionen werden über die OneSign Verwaltungskonsole des Administrators festgelegt und einzelnen oder allen Benutzern basierend auf bestehenden Mitgliedschaften in Active Directory Gruppen zugewiesen. Wenn neue Authentifizierungsrichtlinien eingeführt werden, können Benutzer ihre Karten oder Fingerabdrücke selbständig registrieren, wodurch der Einführungsprozess und der Verwaltungsaufwand maßgeblich vereinfacht werden. Mit OneSign kann ebenfalls eine kontrollierte und verwaltete Registrierung durchgeführt werden. Nur wenn die Authentifizierungsrichtlinien mindestens eine Authentifizierungsmethode aus mindestens zwei verschiedenen Kategorien für die Authentifizierung vorschreiben, kann von mehrstufiger

Authentifizierung gesprochen werden. Übliche Kombinationen für die mehrstufige Authentifizierung sind vor allem kontaktlose Chipkarten und PIN-Nummer oder Fingerabdruck und PIN-Nummer. Um sowohl die Compliance- als auch die Sicherheitsanforderungen einer Klinik zu erfüllen, ermöglicht die Dell MCC Lösung die Kombination mehrerer Authentifizierungsmöglichkeiten:

1. Verschlüsselte Kennwörter wie PIN-Nummern
2. Physische Token wie Karten, Ausweise, Token oder spezielle Geräte
3. Physische biometrische Authentifizierung über den Fingerabdruck

- **Secure Walk-Away**™: Schutz für Desktop-PCs vor unberechtigtem Zugriff auf vertrauliche Informationen durch die automatische Sperrung des PCs, wenn der Benutzer seinen Arbeitsplatz verlässt. Die Sperrung einer Sitzung wird bei Secure Walk-Away (SWA) mithilfe von Gesichts- und Bewegungserkennung erreicht. Die Gesichtserkennung wird über die Webcam von Endgeräten ermöglicht, die automatisch Daten zu den Gesichtszügen des Benutzers speichert, die dann zur Authentifizierung dienen. Wenn der Benutzer seinen Arbeitsplatz verlässt, wird der Desktop automatisch gesperrt. Kehrt der Benutzer wieder zurück, wird er durch die Gesichtserkennungstechnologie erkannt und der Desktop wird automatisch entsperrt. Bei dieser Methode werden keine Bilder der Benutzer aufgenommen, gespeichert oder an die OneSign Appliance weitergeleitet. SWA kann je nach Kundenanforderungen individuell konfiguriert werden. So kann die Dauer, nach der der Desktop abgedunkelt oder gesperrt wird oder nach der eine erneute Anmeldung über die Gesichtserkennung noch möglich ist, ja nach Bedarf des Kunden angepasst werden. Für die Gesichtserkennung erfordert SWA eine integrierte oder über USB angeschlossene Webcam. Die Richtlinien können außerdem so festgelegt werden, dass die Sitzung eines Endgerätes automatisch gesperrt wird, wenn die externe Webcam vom System getrennt wird. Dies sorgt für zusätzliche Sicherheit.

- **OneSign Self-Service Password Management:** Benutzer können ihr primäres Domänenkennwort über ein Portal selbständig zurücksetzenund sind so nicht mehr auf den Helpdesk angewiesen. Auch Benutzer außerhalb des Netzwerks, wie Vertragspartner, können auf das Portal zugreifen, um beispielsweise ein OneSign Verzeichniskonto anzufordern oder OneSign Physical/Logical zu nutzen. Dieses lässt sich in führende Gebäudezugangssysteme, beispielsweise von AMAG, Honeywell, Lenel, S2 und Tyco, integrieren und sorgt so für zusätzliche Kontrolle über den Authentifizierungsprozess. Als Teil des Authentifizierungsprozesses kann OneSign Physical/Logical beispielsweise bestätigen, dass ein zugangsberechtigter Benutzer das Gebäude betreten hat, da seine Smartcard an einem Türsensor des Zutrittsystems registriert wurde. Erst dann kann sich der Benutzer für die Verwendung seines Computers authentifizieren. Auf diese Weise kann sichergestellt werden, dass nicht befugten Personen der Zugang verweigert wird und nur berechtigte Personen Zugriff auf Unternehmenssysteme erhalten. OneSign Physical/Logical bietet somit eine umfassende standortbezogene Lösung für den Zutritt und die Authentifizierung.

- **Zentrale Sicherheitsrichtlinien für Benutzer und Gruppen:** Über zentrale Sicherheitsrichtlinien für Benutzer und Gruppen werden Methoden für die Benutzerauthentifizierung, Regeln für die Sperrung bei Authentifizierungsverstößen, Benutzerprobleme, gleichzeitige Benutzersitzungen und die Sperrung der Zugriffstasten für gemeinsam genutzte Workstations geregelt. Außerdem sind darin Regeln für die eigenständige Verwaltung von Kennwörtern festgelegt. Verstößt ein Benutzer während des Zugriffs auf sein Konto gegen die in den Sicherheitsrichtlinien festgelegten Regeln, kann dieser Benutzer gesperrt werden.

- **Sichere Kommunikation:** Jegliche Kommunikation zwischen dem Agenten und der Appliance findet über sichere HTTP(S)- und SSL-Protokolle auf den Ports 443 oder 81 sowie über 128-Bit-AES-Verschlüsselung statt. Die Kommunikation zwischen Appliances und die Datenbankreplikation werden über verschlüsselte Tunnel auf den Ports 22 und 1521 mittels proprietärem Imprivata Secure Exchange (ISX) Protokoll gesendet.

Notfall-Wiederherstellung/-Kontrolle und Hochverfügbarkeit

Die Digitalisierung von Patientenakten kann Behandlungsfehlern vorbeugen, die Patientensicherheit erhöhen und für bessere klinische Ergebnisse sorgen. Wenn Pflegekräfte aber nicht auf wichtige Anwendungen wie EMR zugreifen können, weil das Rechenzentrum ausgefallen ist, kann das schlimme Folgen haben. In dem Moment, in dem elektronische Geräte Akten und Rezeptblöcke ersetzen, muss die Zuverlässigkeit, Verfügbarkeit und Sicherheit des zugrunde liegenden Systems zu jedem Zeitpunkt garantiert sein. Aus diesem Grund hat die Modernisierung von Desktops für den direkten Datenzugriff am Behandlungsort einen hohen Stellenwert für IT-Angestellte und Klinikmitarbeiter gleichermaßen. Auch bei einem Ausfall oder einer Störung muss sich das Klinikpersonal jederzeit auf die Verfügbarkeit der Desktops und Anwendungen für die Patientenpflege verlassen können. Dank der Dell MCC VMware View Lösung verfügen medizinische Einrichtungen jetzt über nie da gewesene Desktop- und Anwendungszuverlässigkeit und -verfügbarkeit.

Die Dell MCC VMware View Lösung sorgt dafür, dass die Anwendungen und der Desktop jedes Benutzers im Rechenzentrum zentralisiert werden. Die Bereitstellung des unternehmensweiten Clientsystems erfolgt entweder mit einer gewissen Anzahl von lokal installierten Anwendungen oder mit Anwendungen, die über das Rechenzentrum zur Verfügung gestellt werden. Bei einem Notfall ermöglicht dies die erneute Bereitstellung der Clientsysteme über allgemeine Images, sodass die benötigte Zeit für die Wiederherstellung in einen vollständig betriebsfähigen Zustand maßgeblich verringert wird.

Die Dell MCC VMware View Lösung kann außerdem auch in einer hoch verfügbaren skalierbaren Server-Cluster-Umgebung eingerichtet werden. Hier beugt sie gezielt kritischen Schwachstellen (Single Points of Failure) vor und fängt geplante und ungeplante Ausfallzeiten im Klinikalltag auf. Hochverfügbarkeit wird durch die Einrichtung der Server in einem Hochverfügbarkeits-Cluster gewährleistet, der für Netzwerk-Lastausgleich konfiguriert ist. Der SQL Datenbankserver ist in einem Active/Passive-Modus konfiguriert. Das heißt, dass nur einer der Knoten aktiv ist, während der andere eine passive Instanz der Datenbank vorhält. So können ein unterbrechungsfreier Betrieb und minimale Ausfallzeiten ermöglicht werden. Bei der Bereitstellung im Cluster werden der native DRS, HA und vMotion aktiviert, um die Redundanz zu erhöhen und die Fehlertoleranz und Verfügbarkeit zu steigern. Die View Connection Server Rolle kann auch für mehrere Knoten bereitgestellt werden. Der Back-End-Massenspeicher für alle Serverkomponenten wird je nach Kundenanforderungen in einer RAID 5-, RAID 6- oder RAID 10-Konfiguration und mit mehreren Pfaden und Schnittstellen für absolute Netzwerkredundanz bereitgestellt.

Für Umgebungen, die im Hinblick auf virtuelle Desktops ein hohes Maß an Redundanz und Fehlertoleranz erfordern, bietet Dell die **VMware AlwaysOn Desktop** Referenzarchitektur. Mit dieser können die Verfügbarkeitsanforderungen des Klinikpersonals jederzeit und problemlos erfüllt werden. Abgesehen von der Redundanz der Back-End-Server und -Infrastruktur ermöglicht diese Konfiguration die Replikation an mehreren Standorten und von mehreren Instanzen in der gesamten VDI-Umgebung. Dadurch wird bei Standortausfällen eine automatische Verlagerung auf Standby-Standorte und -Infrastrukturen ermöglicht. Bei einer Active/Active-Desktop-Umgebung werden zwei identische Desktop-Images ausgeführt, sodass Benutzer auch bei einem Ausfall des primären Standorts schnell auf ihre Anwendungen und Desktops zugreifen können. Wenn die Infrastruktur eines Gesundheitsdienstleisters durch eine Naturkatastrophe oder eine andere schwere Störung ausfällt, kann sich das Klinikpersonal, das zumeist auch unter den Ersthelfern vertreten ist, immer und überall auf problemlosen Zugriff auf klinische Desktops und wichtige Anwendungen verlassen.

Diese neue Architektur bietet kontinuierliche Überwachungsfunktionen und Lastausgleich mit konstanter Datenreplikation an verschiedenen Standorten. So haben Benutzer die Gewissheit, dass die VMware AlwaysOn Lösung für Datenzugriff direkt am Behandlungsort den Endbenutzer bei einem Ausfall des primären Standorts nahtlos an den sekundären Standort weiterleitet. Das Klinikpersonal wird in seiner Arbeit kaum beeinträchtigt. Mit dieser Lösung kann die IT nun Desktops bereitstellen, die jederzeit verfügbar sind, sodass das Klinikpersonal problemlos und von jedem beliebigen Standort aus auf Anwendungen und Daten zugreifen kann, wenn diese am dringendsten benötigt werden.

Sicherheit

In IT-Umgebungen des Gesundheitswesens ist schneller Zugriff auf klinische Anwendungen und Daten von höchster Bedeutung – Zeit ist ein entscheidender Faktor. Aus diesem Grund spielt Datensicherheit bei einem Großteil des Klinikpersonals eine untergeordnete Rolle: Viele nutzen unsichere oder sogar gemeinsame Kennwörter, wodurch das Risiko für unbefugte Datenzugriffe stark ansteigt. Um Zeit zu sparen und ihre Arbeitsabläufe zu optimieren, nutzen Pflegekräfte heutzutage zudem häufig modernste Tablet-PCs und Smartphones an ihrem Arbeitsplatz.

Dies stellt eine zusätzliche Gefährdung für die Desktop-Infrastruktur dar. Durch menschliche Fehler, E-Mail-Angriffe, Netzwerkviren sowie infizierte Websites und Downloads ist die Datensicherheit täglich in Gefahr – und das auf praktisch jedem traditionellen Desktop-PC. Mit der anhaltenden IT-Consumerization wird es auch für medizinische Einrichtungen immer schwieriger, wichtige Daten und Ressourcen optimal zu schützen und gleichzeitig eine ausreichende Netzwerkleistung zu garantieren. Sicherheitsverletzungen können für Gesundheitsdienstleister schwere Folgen und Auswirkungen haben: hohe Geldbußen aufgrund von Daten, die an einen falschen Drucker gesendet wurden, unbefugte Datenzugriffe oder verlorene mobile Geräte, wie Smartphones oder Tablet-PCs, auf denen, entgegen der Sicherheitsrichtlinien, Patientendaten gespeichert sind.

Häufige Sicherheitsprobleme in Umgebungen im Gesundheitswesen:

- Gefährdung von Endgeräten durch Malware, Viren, Diebstahl, Verlust und Hardwareausfall
- Datenrisiken durch unberechtigten Zugriff und Datendiebstahl über Wechselmedien wie USB
- Schwierigkeiten bei der Sicherung Hunderter oder Tausender PCs mit den aktuellsten Patches oder Updates zur stetigen Einhaltung von Compliance-Anforderungen
- Zahlreiche neue Tablet-PCs, Smartphones und Notebooks, die durch neue Trends in der Arbeitswelt, wie Consumerization, in das Netzwerk eingebunden werden müssen
- Zeit- und Arbeitsaufwand für die Implementierung von Authentifizierungsmethoden wie SSO oder Zwei-Faktor-Authentifizierung auf einzelnen PCs in hoch sicheren Umgebungen

Viele Organisationen erwägen Virtualisierung als eine effektive Lösung. Eine virtuelle Desktop-Infrastruktur (VDI, Virtual Desktop Infrastructure) ist sicherer, da Daten in einem sicheren Rechenzentrum und nicht auf unsicheren Endgeräten gespeichert werden. Zusätzlich können strenge Sicherheits- und Zugangsrichtlinien von einem zentralen Standort aus deutlich einfacher umgesetzt werden. Da die IT jederzeit volle Übersicht und Kontrolle über den Netzwerk- und Dateizugriff sowie über die Systemwartung hat, ist auch die Compliance mit rechtlichen oder branchenspezifischen Bestimmungen mit der VDI-Architektur viel unkomplizierter.

Für die Bereitstellung der Betriebssysteme, Anwendungen und Daten der Benutzer nutzt die Dell MCC VMware View Lösung Anwendungs- und Desktop-Virtualisierungstechnologie und kann so viele der häufigen Schwierigkeiten lösen. Mit der Zentralisierung von Ressourcen kann zudem das Datenrisiko auf Endgeräten durch Diebstahl oder Verwaltungsfehler reduziert und ein unterbrechungsfreier Betrieb dank höherer Konsistenz für verteilte Daten und Anwendungen garantiert werden. Darüber hinaus kann Endbenutzern auch Zugriff über rollenbasierte Profile ermöglicht werden und zentrale Änderungen können an den Benutzer statt an das Clientendgerät weitergegeben werden.

Die Lösung ermöglicht es Administratoren, Richtlinien festzulegen, mit denen der Zugriff auf bestimmte Standorte, Netzwerke und Benutzertypen beschränkt wird, sodass die Risiken für Datenverlust verringert und bessere Verwaltbarkeit und Notfall-Wiederherstellung auf Organisationssebene gesichert werden können. Dies ist möglich, da Daten nicht auf dem lokalen Client gespeichert werden und nur verschlüsselte Bildschirmdaten auf dem Endgerät ankommen. Statt separat auf jedem einzelnen Endgerät, können Administratoren Sicherheitsrisiken nun außerdem proaktiv und zentral in einem Rechenzentrum verwalten. Dadurch können Kosten gespart und höhere Verfügbarkeit für Endbenutzer sichergestellt werden.

In Verbindung mit Imprivata OneSign bietet die Dell MCC VMware View Lösung ein deutlich höheres Maß an Sicherheit in medizinischen Einrichtungen. Diese Sicherheit ist mithilfe von Funktionen für sicheren Zugriff auf Endgeräte, Sicherheitsserver/Sicherheits-Gateways und sichere Kommunikation fest in die Architektur von OneSign

integriert. Vom Standpunkt des Endbenutzers aus bietet OneSign Funktionen wie mehrstufige Authentifizierung, Secure Walk-Away, zentrale Benutzer und Gruppenrichtlinien sowie rollenbasierten Zugriff. Dank dieser Funktionen müssen sich Benutzer nicht mehr verschiedene Kennwörter merken, während Krankenhäuser gleichzeitig Compliance-Vorschriften einhalten, verwalten und optimieren können. Mit Imprivata OneSign können Organisationen im Gesundheitswesen erfolgreich eine einzige, zentrale IT-Zugriffsrichtlinie für Mitarbeiter festlegen, für alle Zugriffsaspekte, von Benutzern über Berechtigungen bis hin zu Standorten und Bedingungen.

Im Hinblick auf Clientgeräte bieten die Dell Wyse Thin Clients einen zusätzlichen Sicherheitsfaktor, da sämtliche Daten auf Servern im Rechenzentrum gespeichert werden und die Einhaltung von Compliance-Vorschriften und die Notfall-Wiederherstellung so vereinfacht werden. Mithilfe von Authentifizierungslösungen und der zentralisierten Verwaltung können Endgeräte ohne Umstände gesperrt werden. Die integrierten Authentifizierungslösungen für eine einmalige Anmeldung ermöglichen extrem sicheren mobilen Zugriff auf wichtige Patientendaten in nur wenigen Sekunden. Auf den spezifisch für VMware Umgebungen konzipierten Dell Wyse Zero Clients werden darüber hinaus keine Daten bzw. Betriebssysteme lokal ausgeführt. Sie verfügen daher über keine angreifbare Oberfläche und das Risiko einer Beeinträchtigung durch Viren, Malware, Diebstahl oder Datenverlust wird reduziert.

Die Dell Wyse Thin und Zero Clients eignen sich für Umgebungen, in denen hohe Sicherheit und Zuverlässigkeit gefragt sind. Mithilfe der Dell Wyse Clients können IT-Mitarbeiter Richtlinien anpassen, um das Leistungs-, Sicherheits- und Funktionsprofil von virtuellen Desktops für beliebige Benutzer – von mobilen Mitarbeitern und anspruchsvollen Benutzern bis hin zu Support-Mitarbeitern – zu definieren und auf verschiedene Geschäftsinitiativen, wie Offshoring, Fusionen und Übernahmen und Erweiterung von Zweigstellen, abzustimmen. Dank der offenen, skalierbaren und bewährten Architektur können mithilfe von Dell Wyse Verwaltung, Support und Integration vereinfacht und gleichzeitig eine sichere, zuverlässige Plattform für die Datenverarbeitung geschaffen werden, die sogar die strengsten Sicherheits- und Compliance-Anforderungen erfüllt. Zu den Vorteilen für IT-Abteilungen im Gesundheitswesen zählen:

- Zentralisierte Netzwerkverwaltung für umfassende Transparenz und Kontrolle über den Zugriff auf und die Verwendung von Endbenutzergeräten, unabhängig vom Zugriffsgerät oder vom Standort
- Schnelle, kosteneffiziente und konsistente Aktualisierungen und Patches für Gerätesicherheit und Konsistenz bei Software-Images und Anwendungen
- Vereinfachte Richtlinienverwaltung für konsistente Einhaltung von behördlichen und branchenweit geltenden Compliance-Bestimmungen
- Bei Bedarf einfache und zeitnahe Integration mit einer Reihe von Geräten mit Funktionen für die einmalige Anmeldung sowie mit sicherer Authentifizierung für erhöhte Sicherheit
- Beträchtliche Reduzierung des Risikos von Datenverlust durch Malware, Viren, Diebstahl oder den Ausfall von Hardware, da sämtliche Daten und Anwendungen im gesicherten Rechenzentrum aufbewahrt werden

Systemverwaltung

Systemverwaltungsfunktionen werden über vCenter, View Manager, die Administratoroberfläche von OneSign SSO, Wyse Device Manager und die Teradici PCoIP-Verwaltungskonsole geboten. Lösungen für Systemverwaltungsansprüchen, die über die von vSphere, View und SSO-Anbieter hinausgehen, finden Sie unter dem nachstehend angegebenen Link zu den Dell Standard- und Enterprise Lösungen für Systemverwaltung.

Mit DVS Enterprise können Betriebssystemmigrationen, Anwendungsaktualisierungen und Sicherheits-Patches optimiert werden, indem das Betriebssystem, die Anwendungen und die Benutzereinstellungen vom Clientsystem in das Rechenzentrum übertragen werden. Die Desktop-Verwaltung wird somit zentralisiert. Administratoren bleiben zeitaufwendige Vor-Ort-Besuche zur Unterstützung bei softwarebezogenen Problemen erspart. Gesperrte Master-Images ermöglichen beispielsweise eine "Selbstreparatur" – beim Auftreten von Systemproblemen kann die IT-Abteilung ganz einfach das betroffene System erneut hochfahren und ein unbeeinträchtigtes Image wiederherstellen. Dell DVS Enterprise bietet einen einfachen, zuverlässigen und umfassenden Ansatz für die zentralisierte Desktop-Verwaltung, mit dem Benutzer sicheren Zugriff auf Daten und Anwendungen erhalten. Dadurch werden die Flexibilität

erhöht, Trends wie IT-Consumerization und BYOD (Bring Your Own Device) optimal in die Infrastruktur eingebunden und die Produktivität schlussendlich erhöht.

Mit der Dell MCC Lösung können IT-Abteilungen im Gesundheitswesen Thin und Zero Clients im gesamten Unternehmen, unabhängig vom Standort, einfach verwalten. Die Dell Wyse Device Manager (WDM) Software ermöglicht eine standortunabhängige vereinfachte Konfiguration und Verwaltung sowie den Einblick in mehrere Tausend Dell Wyse Endgeräte. Dell WDM ermöglicht sichere Kommunikation auf HTTPS-Basis und eine umfassende Geräterichtlinie für die Konfigurationsverwaltung. Die Lösung bietet eine Bestandsverwaltung und Statusüberwachung in Echtzeit, die auf einer standardmäßigen SQL Datenbank aufbaut und Remote-Repositorys für Software optimiert.

Die Funktionen von Dell Wyse Device Manager (WDM) umfassen u. a.:

- Sichere HTTPS-basierte Kommunikation
- Umfassende Geräterichtlinie und Konfigurationsverwaltung
- Bestandsverwaltung und Statusüberwachung in Echtzeit, die auf einer standardmäßigen SQL Datenbank aufbaut
- Remote-Imaging
- Optimierung von Remote-Software-Repositorys
- Administrationsdelegation für Support-Mitarbeiter von Drittanbietern
- Common Criteria Certification

Dell MCC Beratungs- und Implementierungsservices

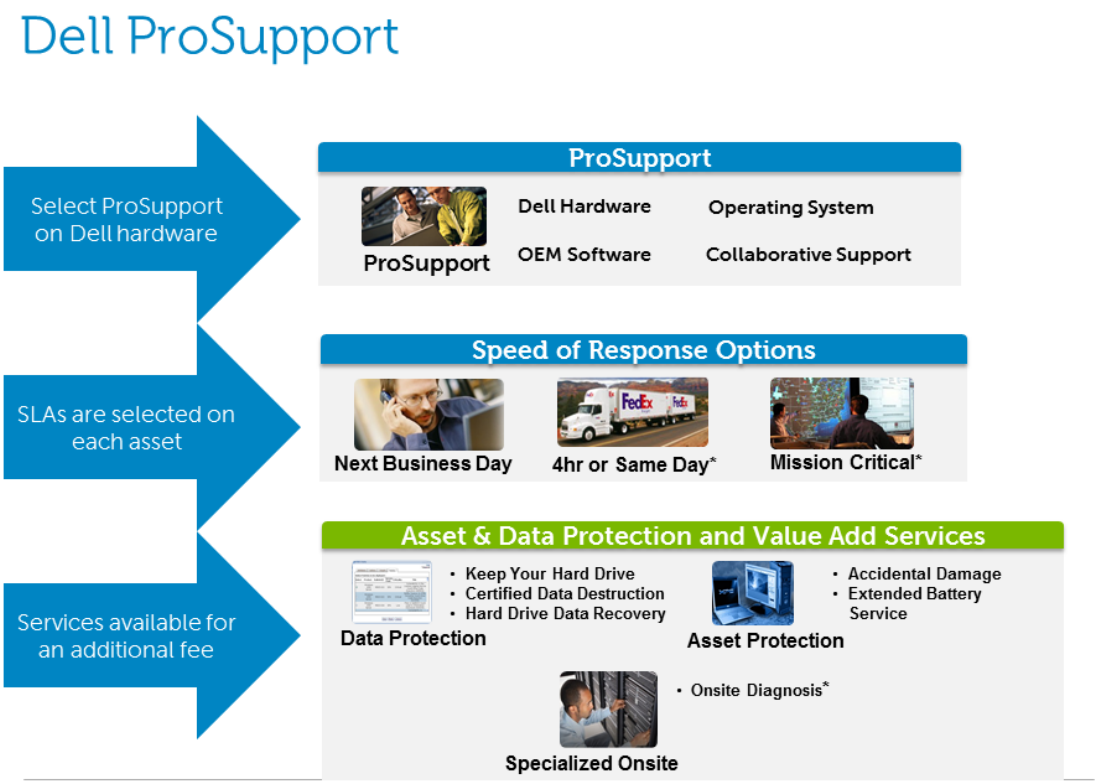
Das Dell MCC Consulting Services Team bietet Unterstützung bei Analyse, Planung und Entwurf einer optimalen Referenzarchitektur, die auf dem ganzheitlichen Verständnis der Anforderungen, IT-Umgebung und Arbeitsabläufe des Kunden basiert. Die Dell MCC Experten arbeiten im Rahmen von Analyse-Workshops vor Ort eng mit Kliniken zusammen, um deren spezifische Anforderungen, Bedürfnisse und Einschränkungen zu ermitteln. Die Experten von Dell unterstützen Kliniken darüber hinaus mithilfe eines Blueprint Assessments bei der Erstellung eines Umgestaltungsentwurfs für die Umstellung vom "Ist-Zustand" auf den "Soll-Zustand". Danach wird ein solider und skalierbarer Entwurf erarbeitet, in dem die detaillierten Hardware- und Softwareanforderungen und der Serviceumfang festgehalten werden. Die Analyse-, Planungs- und Entwurfsservices von Dell unterstützen Organisationen im Gesundheitswesen dabei, herauszufinden, wie sie optimal von der MCC Lösung profitieren können.

Die Dell MCC Implementierungsservices Teams sind verantwortlich für das Projektmanagement und umfassende Integrationsaufgaben, wie beispielsweise Desktop-Virtualisierung, Anwendungsvirtualisierung, Identitäts- und Zugriffsverwaltung, Ausstattung und Konfiguration von Rechenzentren, Clientbereitstellung und andere Aufgaben. Die Dell MCC Services Teams können zudem ein Produktionspilotprojekt mit 50 bis 500 Benutzern implementieren. Organisationen im Gesundheitswesen können anhand eines solchen Projekts die Vorteile der Flexibilität und erhöhten Produktivität der Lösung aus erster Hand feststellen. Wenn ein Krankenhaus zur Implementierung der Lösung bereit ist, helfen die Dell Services Teams beim Entwurf und der Implementierung einer skalierbaren Lösung, die die Vorteile von Dell MCC für Tausende von Benutzern an unterschiedlichen Standorten bereitstellt.

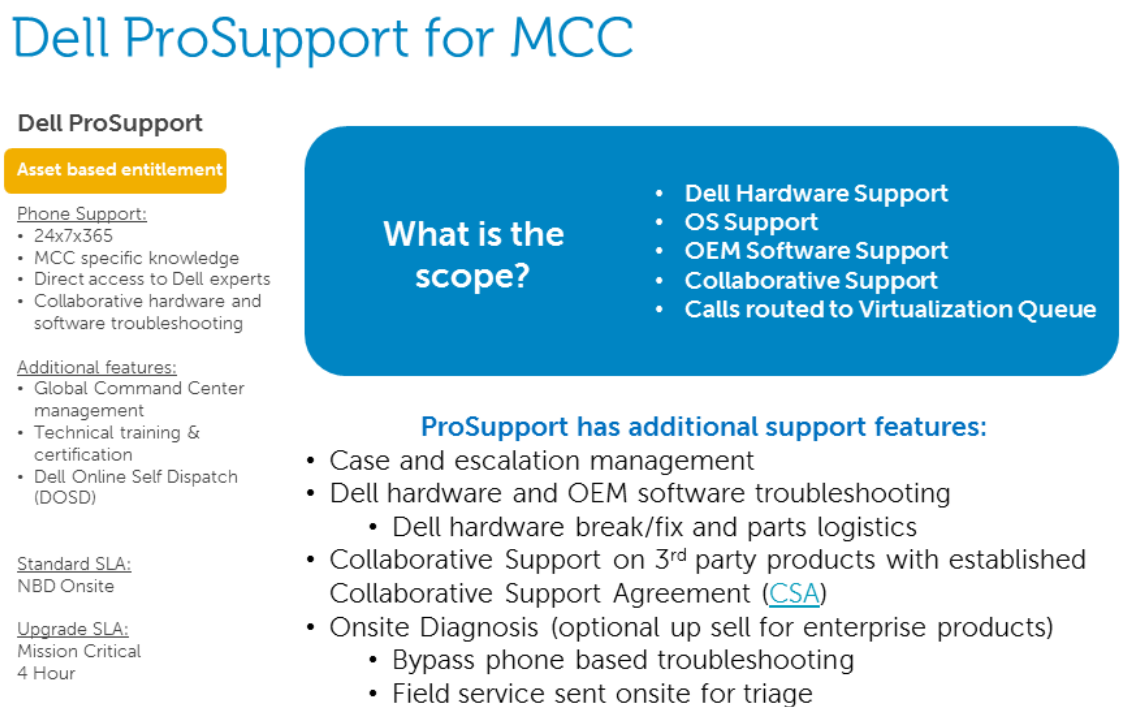
Dell ProSupport

Dell ProSupport™ ist ein Portfolio an weltweit verfügbaren, rund um die Uhr zugänglichen erstklassigen Support-Services für Hardware, Software und Lösungen. Mit den Dell ProSupport Services können Kliniken ihre internen Support-Prozesse vereinfachen und Lücken im internen IT-Support, ihren Systemressourcen und dem organisationsinternen Fachwissen abdecken. Ressourcenausfälle können somit vermieden werden und die Erfüllung von Benutzeranforderungen wird gewährleistet. Gleichzeitig verfügen Kliniken dank koordinierten kooperativem Support für mehrere Anbieter inklusive Eskalationsverwaltung über einen einzigen, zentralen Ansprechpartner.

- Ein einziger, zentraler Ansprechpartner mit hoch qualifizierten Experten
- Vor-Ort-Service am nächsten Arbeitstag mit optional vier oder acht Stunden Reaktionszeit bei Ersatzteilen/Arbeitsleistung
- Kooperativer Drittanbietersupport für Hardware- und Softwareprobleme, der auf der Beziehung zwischen Dell und führenden Softwareanbietern aufbaut
- Eskalationsverwaltung mit Optionen für kundenseitig festgelegte Dringlichkeitsstufen
- Lösungsbasiertes Support-Know-how für spezifische Anwendungen und Software, die in der Lösung enthaltene Desktop-Virtualisierungssoftware inbegriffen
- Zugang zum zentralen Dell Global Command Center für die Bereitstellung von aktuellen Statusinformationen im Hinblick auf die Verfügbarkeit von ProSupport™ Technikern und die voraussichtliche Ankunftszeit von Ersatzteilen, rund um die Uhr



Die Dell ProSupport™ MCC Helpdesk-Techniker und MCC Techniker vor Ort sind hoch qualifizierte Experten, die mit sämtlichen Komponenten der im Labor geprüften MCC Lösungskonfigurationen vertraut sind. Hierzu zählen Hardware und Software der Enterprise-Klasse, Endgeräte, Desktop-Virtualisierungssoftware und Software für die Identitäts- und Zugriffsverwaltung. Unsere Techniker verfügen über Zertifizierungen für VMware vSphere und VMware View, Imprivata und Wyse und werden fortlaufend geschult.



Referenzen

Dell Mobile Clinical Computing Lösung
www.dell.de/mcc

Informationen und White Paper zu in BVIT Tests nachgewiesenen Ergebnissen für die Dell Mobile Clinical Computing Lösung
www.dell.de/mcc-ergebnisse und
www.dell.com/downloads/global/casestudies/DELL-MCC-WHITEPAPER-GERMAN.pdf

DVS Enterprise Referenzarchitekturen: Mobile Clinical Computing
http://go.us.dell.com/dvsmcc

Anhang 1.0

Beispiele für in den einzelnen Regionen verwendete kontaktlose Chipkarten:

Großbritannien, Frankreich, Deutschland, Niederlande

Lesegeräte: MIFARE Lesegerät, wie beispielsweise das externe RF IDeas USB-Lesegerät, das OMNIKEY® 5321 CR USB-Lesegerät oder das Gemalto ProxDU Lesegerät
Kontaktlose Chipkarten: Kompatible Protokolle: HID® iCLASS® und MIFARE® sowie ISO 14443 A/B und ISO 15693

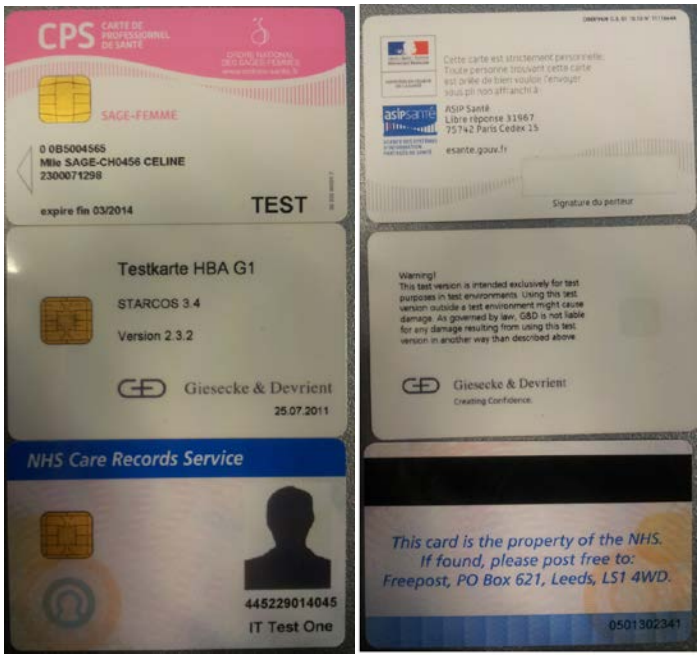
Beispiele für in den einzelnen Regionen verwendete Smartcards:
Nachstehend finden Sie Beispiele für in den jeweiligen Ländern derzeit verwendete Smartcards:

Großbritannien
Smartcard: NHS V5 Smartcard
Lesegeräte: Integriertes Smartcard-Lesegerät für kontaktbasierte Smartcards in der Dell Tastatur, MIFARE Lesegeräte, wie beispielsweise das externe RF IDeas USB-Lesegerät

Frankreich
Smartcards: CPS V3 Smartcard (Kombination aus kontaktloser Chipkarte und Smartcard)
Lesegeräte: Gemalto GemPC Smartcard-Lesegerät für Smartcard-Authentifizierung. Verwenden Sie für die Authentifizierung von kontaktlosen Smartcards das OMNIKEY 5321 Lesegerät oder das Gemalto ProxDU Lesegerät.

Deutschland
Lesegeräte: OMNIKEY® 5321 Desktop-USB-Lesegerät
Karten: Kompatible Protokolle: HID® iCLASS® und MIFARE® sowie ISO 14443 A/B und ISO 15693

Niederlande
Lesegeräte: OMNIKEY 3121 USB-Lesegerät
Kartentyp: UZI-pas


CPS
CARTE DE PROFESSIONNEL DE SANTÉ
SAGE-FEMME
0 0B5004565
Mlle SAGE-CH0456 CELINE
2300071298
expire fin 03/2014
TEST
Testkarte HBA G1
STARCOS 3.4
Version 2.3.2
Giesecke & Devrient
25.07.2011
NHS Care Records Service
445229014045
IT Test One
Cette carte est strictement personnelle.
Toute personne trouvant cette carte
est priée de bien vouloir l'envoyer
sous pli non affranchi à :
ASIP Santé
Libre réponse 31967
75742 Paris Cedex 15
esante.gouv.fr
Signature du porteur
Warning!
This test version is intended exclusively for test
purposes in test environments. Using this test
version outside a test environment might cause
damage. As governed by law, G&D is not liable
for any damage resulting from using this test
version in another way than described above.
Giesecke & Devrient
Creating Confidence.
This card is the property of the NHS.
If found, please post free to:
Freepost, PO Box 621, Leeds, LS1 4WD.
0501302341