

Secure by Design

Wie XenApp und XenDesktop den Datenschutz, die Zugriffskontrolle und andere kritische Sicherheitsaufgaben drastisch vereinfachen

Die meisten Gespräche über Anwendungs- und Desktop-Virtualisierung konzentrieren sich auf die Kostenreduktion, die Vereinfachung des IT-Betriebs und einen verbesserten Benutzerkomfort für die Mitarbeiter. Diese Faktoren sind zwar äußerst wichtig, aber die IT-Experten sollten auch die gewaltige Auswirkung, die die Arbeitsplatzvirtualisierung auf die Informationssicherheit hat, nicht vergessen. Denn Anwendungs- und Desktop-Virtualisierung bieten wesentliche Vorteile für wichtige Sicherheitsfunktionen wie Datenschutz, Zugriffskontrolle, Anlegen und Löschen von Benutzerkonten und Compliance. Administratoren erhalten zudem eine detaillierte Kontrolle darüber, wie angestellte und freie Mitarbeiter und Geschäftspartner die Anwendungsdaten verwenden und austauschen können.

In diesem Whitepaper erfahren Sie, wie die Citrix XenApp- und Citrix XenDesktop-Lösungen den benötigten Arbeitsaufwand reduzieren, um unternehmenskritische Daten zu schützen. Gleichzeitig erhalten die Anwender einen schnellen, einfachen und flexiblen Remote-Zugriff, der die Unternehmensproduktivität steigert.

Wachsende Herausforderungen für die IT-Sicherheit

Die IT-Abteilungen der Unternehmen stehen einerseits vor der Herausforderung, wichtige neue Unternehmensinitiativen zu unterstützen und den Komfort für Endbenutzer zu verbessern, während gleichzeitig das Budget gekürzt wird und der Druck, die Informationssicherheit zu verbessern, steigt. Zu diesen Herausforderungen gehört auch, dass Computing-Ressourcen unabhängig von physischen und geografischen Grenzen leichter nutzbar gemacht werden müssen. Mitarbeiter fordern Folgendes:

- Ohne Einbußen beim Benutzerkomfort von überall mit PCs, Laptops, Tablets und Smartphones arbeiten zu können
- Dank Bring-your-own-Device (BYOD)-Programmen private Endgeräte in der Unternehmensumgebung verwenden zu können
- Keine starre IT-Sicherheitskontrolle, die die Performance einschränkt und ein produktives Arbeiten verhindert
- Zugriff auf Unternehmensdaten und Auswahl von Anwendungen aus einem Unternehmens-App Store nach Bedarf

In den Schlagzeilen lesen wir von Sicherheitslücken, und auf IT-Webseiten finden wir Geschichten über Cyber-Kriminalität und Hacker, die Zero-Day-Attacken durchführen, neue Arten von Malware und gezielte Attacken auf bestimmte Unternehmen.

Grundlegende Änderungen der Arbeitsweise und ganze Wellen neuer Technologien bringen alte Methoden, die für eine Balance zwischen Mitarbeiterproduktivität und IT-Sicherheit sorgen sollen, aus dem Gleichgewicht. IT-Administratoren sehen sich mit neuen Arbeitsweisen konfrontiert, die die Routineprotokolle und -prozesse zum Schutz der Unternehmensdaten durcheinander bringen:

- Seit 2014 wird von jedem Wissensarbeiter erwartet, dass er sich durchschnittlich mit drei Endgeräten mit seinem Arbeitsplatz verbinden kann.
- Mitarbeiter verwenden ihre privaten Endgeräte. Dadurch wird es schwierig, wenn nicht sogar unmöglich, die Sicherheitsstandards des Unternehmens zu garantieren und durchzusetzen.
- Die IT muss angestellten, freien Mitarbeitern und Geschäftspartnern Zugriff von entfernt gelegenen Niederlassungen, Home Offices, Hotelzimmern und sogar öffentlichen Internet-PCs auf der ganzen Welt ermöglichen.

Sicherheit neu entwickeln oder sich für eine „Secure by Design“-Lösung entscheiden

Diese Trends sind ganz offensichtlich nicht mit den derzeitigen Ansätzen für Sicherheit und Remote-Zugriff vereinbar. Wie kann die IT den Zugriff auf Ressourcen vereinfachen, wenn die Bedrohungen immer komplexer werden und sich die Endgeräte, die es zu schützen gilt, vervielfachen? Und es ist nicht allein die Anzahl der Endgeräte, die eine Herausforderung darstellt, sondern insbesondere deren Vielfaltigkeit. Jedes Endgerät – PC, Laptop, Tablet und Smartphone – erfordert andere Sicherheitsprodukte, muss vor anderen Bedrohungen geschützt werden und verlangt nach unterschiedlichen Zugriffsrichtlinien.

Die Lösung besteht nicht darin, eine weitere Ebene an Sicherheitsprodukten hinzuzufügen, die lediglich einen größeren Verwaltungsaufwand bedeuten würde. Es geht darum, den Ansatz zu verändern und ein Computing-Modell einzuführen, das vom Konzept her sicher - „Secure by Design“ - ist. Die Architektur dieser Methode muss grundlegende Sicherheitsfunktionen wie Datenschutz, Zugriffskontrolle, Benutzerkonten-Management und sicheren Remote-Zugriff drastisch vereinfachen.

XenApp und XenDesktop

XenApp ist eine Lösung zur Anwendungsbereitstellung mit der jede Art von Windows®-Anwendung im Rechenzentrum virtualisiert, zentralisiert, gemanagt und sofort standortunabhängig für Anwender mit jedem Endgerät bereitgestellt werden kann. Mit XenApp werden Anwendungen im Rechenzentrum ausgeführt, die an jedem beliebigen Standort sicher aufgerufen und genutzt werden können. Da die Anwendungen und Daten im Rechenzentrum selbst geschützt werden und am gleichen Standort wie die Back-End-Datenbanken gehostet werden, wird die Anwendungs-Performance weiter verbessert, auch wenn von weit entfernten Standorten auf diese Daten und Anwendungen zugegriffen wird.

Die Vorteile durch den Zugriff auf die Anwendungen und die Performance, die XenApp bietet, sind hoch. Häufig aber werden die Sicherheitsvorteile einer zentralisierten Anwendungsbereitstellung nicht als solche erkannt. XenApp stellt eine sichere Architektur bereit, die die Datenmengen, die sich außerhalb des Rechenzentrums befinden, drastisch reduziert – und das ohne die Konfigurierung aufwändiger Sicherheitsfunktionen oder Zusatz-Sicherheitsprodukte. XenApp wurde so entwickelt, dass alle Anwendungen, Daten und Informationen im Rechenzentrum gesichert werden und lediglich Screen-Updates, Mausclicks und Tastenanschläge über das Netzwerk auf das Endgerät des Anwenders übertragen werden.

XenApp sorgt dafür, dass vertrauliche Unternehmensdaten im Rechenzentrum geschützt werden, aber Mitarbeiter brauchen trotzdem einen sicheren Zugriff auf die XenApp-Infrastruktur. Auf Anwendungen, die mit XenApp veröffentlicht werden, kann über Citrix Receiver zugegriffen werden. Das ist ein schlanker Client, der auf jedem Endgerät installiert werden kann, einschließlich iOS, Mac®, Android®, Windows und anderen. Mit dem Citrix Receiver können IT-Administratoren ganz einfach für jedes private oder unternehmenseigene Endgerät einen sicheren Zugriff auf die Anwendungen ermöglichen.

Gleichzeitig ist sichergestellt, dass IT-Sicherheitsverfahren und -prozesse angewendet werden. Citrix Receiver kommuniziert kontinuierlich mit der XenApp-Infrastruktur, wodurch die Identifizierung der optimalen Methode zur Anwendungsbereitstellung für jeden Anwender zum Kinderspiel wird. Als Grundlage für diese Entscheidung werden die Funktionen des Endgeräts, die verfügbare Netzwerkverbindung und besondere anwendungsspezifische Aufgaben herangezogen. Anwender können den Citrix Receiver an jedem Standort herunterladen und sicher auf Anwendungen zugreifen, die mit XenApp veröffentlicht werden. Damit hat die IT die Möglichkeit, den Bedarf der Mitarbeiter zu erfüllen, ohne Einbußen bei den Sicherheitsstandards hinnehmen zu müssen.

Alle Sicherheitsfunktionen von XenApp sind in XenDesktop integriert. Hierbei handelt es sich um eine robuste Plattform für Windows Desktop- und Anwendungs-Virtualisierung, die einen On-Demand-Zugriff bereitstellt. Unternehmen, die XenDesktop verwenden, können das sichere Design von XenApp als Erweiterung verwenden, um vollständige Desktop-Arbeitsplätze bereitzustellen. So können die unterschiedlichen Anwendungen, Daten und Desktop-Funktionen durchgängig im Rechenzentrum geschützt werden. Mit XenDesktop sind virtuelle Desktops „Secure by Design“, konzeptionell sicher, unabhängig davon, wie weit entfernt sich der Anwender befindet oder wie wenig vertrauenswürdig das Endgerät auch sein mag.

NetScaler Gateway

Bereitstellungen mit XenApp und XenDesktop können mit NetScaler Gateway noch weiter verbessert werden. NetScaler Gateway ist eine Lösung für den sicheren Desktop- und Anwendungszugriff, die granulare Richtlinien für Anwendungen und einzelne Endgeräte sowie eine aktive Kontrolle bietet. NetScaler Gateway sorgt für einen sicheren Remote-Zugriff auf die XenApp- und die XenDesktop-Infrastruktur und stellt Anwendern einen sicheren zentralen Zugriffspunkt für veröffentlichte Anwendungen und Desktops über jedes beliebige Endgerät bereit. NetScaler Gateway sorgt für einen sicheren Remote-Zugriff. Dieser wird erreicht, indem eine sichere Citrix ICA Proxy-Technologie zur Verschlüsselung der Daten verwendet wird, ohne dass ein kompletter VPN-Tunnel für die Remote-Endgeräte eingerichtet werden muss.

NetScaler Gateway nutzt die HDX SmartAccess-Technologie, um für die IT ein zentrales Management der Zugriffskontrolle bereitzustellen und die erlaubten Aktionen für die einzelnen Anwender einzuschränken. Dank HDX SmartAccess sind die IT-Administratoren in der Lage, in jeder Situation eine ausgewogene Balance zwischen Sicherheit und Benutzerkomfort für die Endbenutzer zu erreichen. Dies wird durch die Definition exakter Richtlinien erzielt, die Anwender, Endgerät und Standort berücksichtigen. Administratoren möchten beispielsweise Richtlinien erstellen, damit eine bestimmte Anwendergruppe über LAN auf eine breite Palette von Anwendungen und Daten zugreifen kann. Wird von zuhause mit einem Tablet gearbeitet, kann nur noch auf eine Untergruppe dieser Ressourcen zugegriffen werden. Und wenn sich der Mitarbeiter mit einem Smartphone über ein öffentliches Netzwerk verbindet, wird die Gruppe der Ressourcen, auf die er zugreifen kann, noch weiter eingeschränkt. Eine andere, nicht so vertrauenswürdige Benutzergruppe, darf unter allen Bedingungen nur auf eine Untergruppe der Ressourcen zugreifen. Aber die Optionen für Administratoren sind damit noch nicht erschöpft! Sie können die Möglichkeiten von Anwendern in unsicheren Umgebungen einschränken und beispielsweise das Kopieren von Daten, das Versenden von E-Mails oder das Drucken von Informationen einschränken oder das Speichern vertraulicher Dateien auf externen Medien verbieten. Sie können die Möglichkeiten für Nutzer von öffentlichen Internet-Endgeräten darauf beschränken, Daten nur zu lesen.

Überdies kann der Zugriff in Abhängigkeit des Sicherheitsniveaus des Endgeräts eingeschränkt werden. HDX SmartAccess umfasst eine Analyse-Software des Endgeräts, die in der Lage ist, Remote-Computer zu scannen und festzustellen, ob Sicherheits-Tools wie Anti-Virus-Software, Client Firewalls oder Utilities zur Verschlüsselung der Festplatte installiert sind, laufen und aktuell sind. Werden diese Anforderungen nicht erfüllt, kann der Zugriff für die betroffenen Anwender auf bestimmte Anwendungen und Daten beschränkt werden oder diese werden auf eine Seite zur Problembekämpfung weitergeleitet, um die Sicherheitsdefizite

zu beheben. Da die Anwender zwischen unterschiedlichen Endgeräten, Anwendungen und Standorten hin- und herwechseln, können diese Richtlinien dynamisch angewendet werden.

Administratoren können den Datenschutz und die sichere Speicherung von Daten regeln, um die Compliance durchsetzen. Das ist besonders wichtig für Unternehmen, die bestimmte Vorschriften einhalten müssen – beispielsweise dürfen einige europäische Länder bestimmte Daten über deren Einwohner ausschließlich im Inland speichern. Mit HDX SmartAccess ist eine Organisation in der Lage, sicherzustellen, dass Daten, die sich in einer virtuellen Umgebung befinden, im Inland gespeichert werden. Zusätzlich kann sie Richtlinien erstellen, damit niemand aus dem Ausland (oder durch die Verwendung eines mobilen Endgeräts) auf diese Daten zugreifen kann.

Lernen Sie die Vorteile von „Secure by Design“ kennen

Die Architektur und die wichtigsten Funktionen von XenApp und XenDesktop mit NetScaler Gateway machen es einfacher und zuverlässiger, Sicherheit zu managen. Durch die Entscheidung für eine Secure-by-Design-Lösung lösen sich einige der komplexesten Herausforderungen des Datenschutzes auf Endgeräten einfach in Wohlgefallen auf oder reduzieren zumindest die Komplexität drastisch.

Datenschutz

Mit einer Lösung, die für höchste Sicherheit konzipiert ist, können vertrauliche Daten in Rechenzentren zentralisiert werden und durch eine umfassende Reihe an Netzwerk- und gehosteten Sicherheitsprodukten wie Firewalls der nächsten Generation (NGFW), Intrusion-Protection-Systemen (IPS) sowie Host-Anti-Malware- und Anti-Spyware-Tools geschützt werden. Diese Sicherheitseinrichtungen sind im Allgemeinen viel stärker und effektiver als lokale Firewall- und Anti-Virus-Produkte, die auf Endgeräten bereitgestellt werden. Überdies sind sie weitaus einfacher zu aktualisieren.

Mit XenApp und XenDesktop werden Daten niemals über ein Netzwerk übermittelt. Wenn die Richtlinien allerdings eine Datenübermittlung erlauben, werden diese stets verschlüsselt. So bleiben geistiges Eigentum und vertrauliche Daten vor Lauschangriffen, Man-in-the-Middle-Angriffen und anderen Bedrohungen, denen Daten bei einer Übertragung ausgesetzt sind, geschützt.

Eine Anwendungs- und Desktop-Virtualisierung mit XenApp und XenDesktop vereinfacht überdies den betrieblichen Aspekt des Datenschutzes. Datenbanken und Dateien, die zentral verwaltet werden, können viel einfacher überwacht und gesichert werden als solche, die sich auf vielen unterschiedlichen Endgeräten befinden. Mitarbeiter können einfach vor Datenverlust durch Hardware- oder Software-Fehler, Unfällen oder menschlichen Fehlern geschützt werden. Bei einem Ausfall oder einer Katastrophe können Daten schneller wiederhergestellt werden.

Zugriffskontrolle

Es ist eine große Herausforderung, den Zugriff auf Anwendungen und Daten zu kontrollieren, die auf Endgeräten gespeichert sind. Das gilt insbesondere deshalb, weil die verfügbaren Tools für das Management dieser lokalen Daten sehr stark variieren – je nach Art des Laptops, Tablets und Smartphones.

Weiter erschwerend kommt hinzu, dass viele Unternehmen unterschiedliche Zugriffspunkte und Authentifizierungsverfahren anwenden, um die verschiedenen Szenarien zu unterstützen. Unter Umständen sind drei unterschiedliche Gateways und ebenfalls drei unterschiedliche Authentifizierungsverfahren nötig, um folgende Szenarien zu bewältigen: Ein Mitarbeiter verbindet sich über einen PC im Büro, ein zweiter über ein Tablet von zuhause und ein freier Mitarbeiter über ein Smartphone am Flughafen.

Mit XenApp und XenDesktop können Administratoren ein Tool-Set verwenden, um für alle Anwender einheitliche Richtlinien zur Zugriffskontrolle zu erstellen und durchzusetzen –

unabhängig von deren Standort und dem Endgerät, das sie verwenden. Sie können auch alle Windows- und Legacy-Anwendungen sofort durch Multi-Faktor-Authentifizierung ergänzen, einschließlich dynamische Token, RADIUS, Kerberos, SmartCard und Biometrieverfahren.

Die gleichen Zugriffskontrollen und Authentifizierungsmethoden können verwendet werden, um den Zugriff auf alle Ressourcen zu verwalten, die über XenApp und XenDesktop bereitgestellt werden. Gleichzeitig steht ein Unternehmens-App-Store mit Self-Service zur Verfügung, über den Anwender schnellen Zugriff nach Bedarf auf Windows-Anwendungen und Anwendungs-Updates erhalten. Durch die Bereitstellung eines Unternehmens-App-Stores bietet die IT Anwendern hohe Flexibilität und entlastet Mitarbeiter in den Bereichen IT-Betrieb und Support. Diese müssen nicht mehr länger die Anwendungen für jeden Mitarbeiter einzeln bereitstellen. Zusätzlich ist eine verbesserte Sicherheit möglich: Die Anwender erhalten einfachen Zugriff auf Anwendungen, die vom Unternehmen genehmigt und geprüft wurden. So müssen die Mitarbeiter nicht mehr länger potentiell infizierte Anwendungen aus zweifelhaften App-Stores und von gefährlichen Webseiten herunterladen.

Steuerung des Benutzerzugriffs

Die Steuerung des Benutzerzugriffs der Mitarbeiter kann für IT-Administratoren sehr arbeitsintensiv sein. Es ist besonders komplex, den Zugriff auf Anwendung und Daten für interne und externe Mitarbeiter und andere Personen zu sperren, wenn diese aus dem Unternehmen ausscheiden bzw. die Zusammenarbeit beendet wird. Geschichten von ehemaligen freien Mitarbeitern, die auch noch Monate nach Abschluss ihrer Arbeit für das jeweilige Unternehmen Zugriff auf die Unternehmensanwendungen haben oder von gekündigten Mitarbeitern, die Kundenlisten und geistiges Eigentum mitnehmen, gibt es häufig.

Mit XenApp und XenDesktop kann für neue Anwender der Zugriff auf Anwendungen mit ein paar Mausklicks bereitgestellt werden. Ebenso schnell kann der Zugriff auf Anwendungen und Daten auch wieder deaktiviert werden, beispielsweise wenn ein Mitarbeiter das Unternehmen verlässt. Und wenn gekündigte Mitarbeiter ihre privaten Laptops oder mobilen Endgeräte verwenden, sind vertrauliche Daten außerhalb ihrer Reichweite in Rechenzentren und nicht auf ihren privaten Geräten gespeichert.

Reaktion auf Vorfälle und Disaster Recovery

Auch die Reaktion auf Vorfälle und die Disaster Recovery ist mit Anwendungs- und Desktop-Virtualisierung um vieles einfacher. Zentral verwaltete Daten können einfacher überwacht und analysiert werden, als Daten, die auf unterschiedliche Systeme verstreut sind. Schwachstellen können zentral gepatcht oder behoben werden und es müssen nicht hunderte Remote-PCs und -Endgeräte individuell behandelt werden.

Für die Disaster Recovery können Administratoren eine „Zwei-Rechenzentren“-Konfiguration einrichten, um Anwendungen und Daten zwischen zwei Standorten zu spiegeln. Fällt ein Standort aus, können die Anwender schnell zum anderen wechseln, ohne dass Daten verloren gehen oder die Produktivität eingeschränkt wird. Wenn Laptops oder andere Endgeräte zerstört werden oder im Katastrophenfall nicht verfügbar sind, können die Mitarbeiter von sicheren Standorten über andere Endgeräte auf ihre Anwendungen und Daten zugreifen.

Compliance

XenApp und XenDesktop können Audits und die Einhaltung von Compliance-Anforderungen vereinfachen. Prüfer können einen umfassenden zentralisierten Audit Trail verwenden, um festzustellen, wer auf welche Anwendung und Informationen zugegriffen hat. Es ist nicht mehr erforderlich, umfangreiche Protokolle von Remote-Endgeräten zu sammeln.

Fazit

Dieses Dokument beschreibt, wie XenApp- und XenDesktop-Lösungen von Citrix Anwendern mehr Möglichkeiten und Flexibilität geben, um von überall und über jedes Endgerät sicher auf Anwendungen und Daten zuzugreifen. Überdies werden einige Möglichkeiten dargestellt, wie die Anwendungs- und Desktop-Virtualisierung komplizierte und zeitintensive Sicherheitsaufgaben der IT vereinfacht. Dazu gehören:

- Datenschutz
- Zugriffskontrolle
- Richtlinienerzwingung
- Steuerung des Benutzerzugriffs
- Reaktion auf Vorfälle und Disaster Recovery
- Compliance
- Sicherer effizienter Remote-Zugriff.

Die XenApp- und XenDesktop-Lösungen sind „Secure by Design“, konzeptionell sicher. Sie verringern die Arbeit, die benötigt wird, um eine bessere Sicherheit bereitzustellen. Sicherheitsverbesserungen gehen mit einer virtualisierten Architektur sowie einer zentralisierten Anwendungs- und Desktop-Bereitstellung einher. Das bedeutet: Die Organisation kann die Vorteile einer einfacheren und zuverlässigeren Sicherheit nutzen, ohne neue und komplexe Sicherheits-Tools zu implementieren und zu managen.

Erfahren Sie mehr auf citrix.de/xenapp und citrix.de/xendesktop



Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, Indien

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, Großbritannien

EMEA Headquarters
Schaffhausen, Schweiz

Pacific Headquarters
Hongkong, China

Über Citrix

Citrix (NASDAQ:CTXS) ist ein Anbieter von Virtualisierungs-, Netzwerk- und Cloud Computing-Infrastruktur, die Menschen bei neuen Formen der Zusammenarbeit unterstützt. Citrix-Lösungen helfen IT-Abteilungen und Service Providern beim Aufbau, der Verwaltung und der Absicherung virtueller und mobiler Arbeitsplätze: Damit lassen sich einzelne Anwendungen oder gesamte Desktops sowie Daten und Dienste jederzeit auf jedem Endgerät und über jedes Netzwerk bereitstellen. Mehr als 330.000 Unternehmen und über 100 Millionen Anwender setzen weltweit auf Technologie von Citrix. Der jährliche Umsatz in 2013 betrug 2,9 Milliarden US-Dollar. Weitere Informationen unter www.citrix.de.

Copyright © 2014 Citrix Systems, Inc. Alle Rechte vorbehalten. Citrix, Citrix Receiver, ICA, XenApp, XenDesktop, NetScaler Gateway und HDX sind Marken von Citrix Systems, Inc. und/oder seiner Tochtergesellschaften, die u. U. in den USA und anderen Ländern registriert sind. Weitere in diesem Dokument genannte Produkt- und Unternehmensnamen sind Marken ihrer jeweiligen Unternehmen.