CITRIX

Solution Architectures for the General Data Protection Regulation (GDPR)

CITRIX

General Data Protection Regulation (GDPR) Overview

GDPR is a set of data privacy rules that apply broadly to both companies in the European Union (EU) and the usage of data pertaining to EU residents. The GDPR takes full effect on 25th May 2018 across the EU. The official regulation includes several chapters which are further broken down into "articles", or subsections that describe specific provisions, which are referenced frequently by number or title in documents describing how to comply with their requirements.

GDPR seeks to:

- Unify European data protection regulations
- Protect the data privacy of EU residents
- Manage how organizations approach data privacy

Personal data is any information relating to an identifiable person, therefore it is often referred to as personally identifiable information (PII). It could include information such as names, photographs, IP or email addresses, and medical information.

The GDPR applies to:

- Organizations operating within the EU
- Organizations operating outside of the EU who offer goods, services or are involved in 'monitoring the behavior' of EU residents

Privacy considerations for GDPR span the data lifecycle from opt-in collection, to specific or anonymized usage and secured disposal and retirement of data. It covers all personal data relating to your customers, employees, supply chain, partners and anyone else about whom you collect personal information.

Two key GDPR articles will be the focus of this white paper:

- Access control (Article 25) – calls out particular measures which shall ensure that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons.
- Encryption and data protection (Article 32) – calls out:
  - Pseudonymisation and encryption of personal data
  - Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
  - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
  - Protection from accidental and unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed

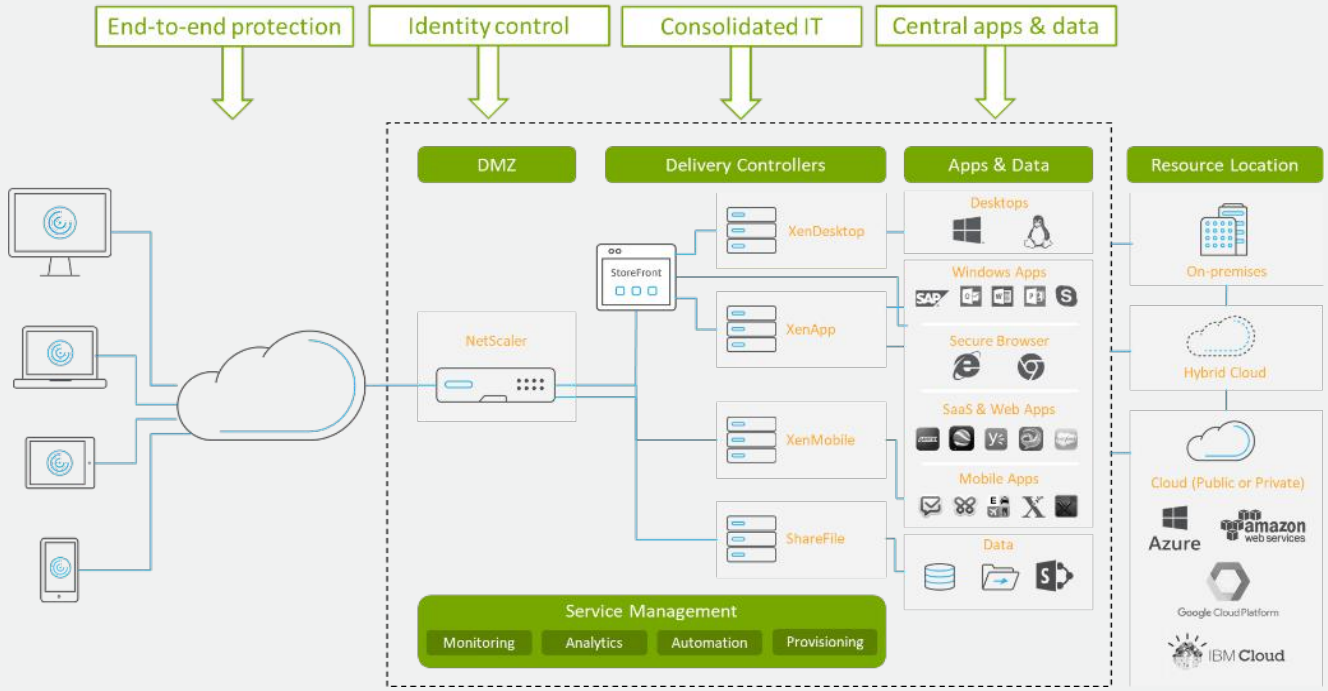
How Citrix can help you with your GDPR compliance initiatives

Citrix Workspace simplifies the management of your systems and data by centralizing services in the data center or cloud as a digital workspace. The goal of this white paper is to describe how it unifies applications, data and desktops into a digital workspace for your teams and allows you to better align with GDPR requirements around data management, data monitoring and information auditing.

Citrix supports clients on their journey to GDPR compliance in 4 key ways:

- By centralizing and enclaving applications and data
- By ensuring data is protected when shared or distributed
- By controlling who has access to data and resources
- By bringing IT together for application and data-specific security

Citrix Workspace – supports your GDPR journey



Data oriented approach to GDPR requirements

Following the GDPR guidelines might be much easier for modern cloud companies than traditional enterprises. While most of the cloud companies have only a few centralized sources where personally identifiable information (PII) is stored, traditional companies potentially have hundreds, if not thousands, of different databases and data sources that need to be assessed, reviewed and updated to meet the latest data privacy standards.

These data sources can range from traditional SQL databases to emails, documents or even physical documents. With the aggressive timelines, many enterprises can be faced with a challenge to prepare everything in time. It is important to understand that the GDPR doesn't affect only active data sources, but also all backups, disaster recovery sites and physical printouts.

The GDPR is all about the maturity of the company when dealing with data and privacy information. Citrix has always been a data and application oriented company, with a proven record of handling complex, often international projects that are dealing with thousands of applications.

The traditional consulting approach is focused on the business processes, identifying people and business requirements, access methods and slowly cascading down to infrastructure and data sources. However, the GDPR requires a more data centric approach. We recommend starting with identifying and assessing various locations where PII data is currently stored and moving higher up the stack to make sure that data sources are properly secured. You can think about this as an inside out approach to security.

Define—Start by defining the criteria of PII data that is in scope of assessment. This phase should help you define what to look for and how to prioritize data sources from a privacy perspective. This should include employees, customers, vendors, and any other entities.

Assess—Analyze all the existing locations where data is stored. Identify the business requirements, data retention and potential challenges to securing the data. Identify not only where the data is stored, but also how it's being collected. Data segmentation is one of the most time consuming and critical phases of the data consolidation projects.

This phase requires a comprehensive approach, critical thinking and well-defined methodology. Organizations mustn't ignore data held in legacy systems, even if there is a program in place to modernize soon or that the data is used only as a backup. It is important to understand that all these legacy systems are covered by the GDPR requirements as well and companies need to take a holistic approach.

Reduce—The goal of this phase is to identify if it is possible to reduce the number of data sources that need to be secured. For example, it is possible to consolidate data sources that are being used by business units – instead of storing client data in multiple locations, a centralized location could be used to maximize effectiveness of security measures. Maybe the data is not even needed at all – the biggest privacy offender might not even be considered critical for the business units. It is also possible that applications are simply collecting too much data ("just in case"). The applications can be modified to stop collecting excessive information and the existing data can be erased. Instead of trying to secure all the possible locations of PII, companies should ask when/where do they actually need to store the data about customers and other parties. As GDPR compliancy is an ongoing process with periodic reviews, minimizing the amount of included data sources can prove to be a very effective long-term strategy.

Remediate—Identify if existing data sources and applications used to access them are following the GDPR guidance, or if changes are needed. If the data source includes PII data and is not secure, identify the possible approaches to solve the situation. A cross departmental GDPR team should also identify, assess, and review not only the data itself, but also access methods, applications used and other factors, such as limiting user and 3rd party access, revisiting requirements and more specifically defining data security measures.

Review – GDPR compliancy is an ongoing process and data assessments need to be performed on a regular basis. It is therefore important to implement a robust, stable, and repeatable process that can be defended if it ever needs to be presented to auditors. The data sources security assessment should be performed and reviewed on a regular basis.

With the large number of data sources that are in scope and limited time available, the goal for most companies should be to choose a few, robust, and proven architectures that can help secure data sources that don't initially meet the GDPR requirements. Trying to create a tailor-made solution for each of the problematic data sources is unrealistic, unless a company has limited data sources and began preparing for the GDPR well in advance. The result is often an environment where a few applications are properly secured, while the majority are left unsecured, with the implementation project being stalled by months or even years and going well over budget. GDPR also presents an opportunity to update privacy architectures across applications and data usage to support evolving global and regional privacy initiatives.

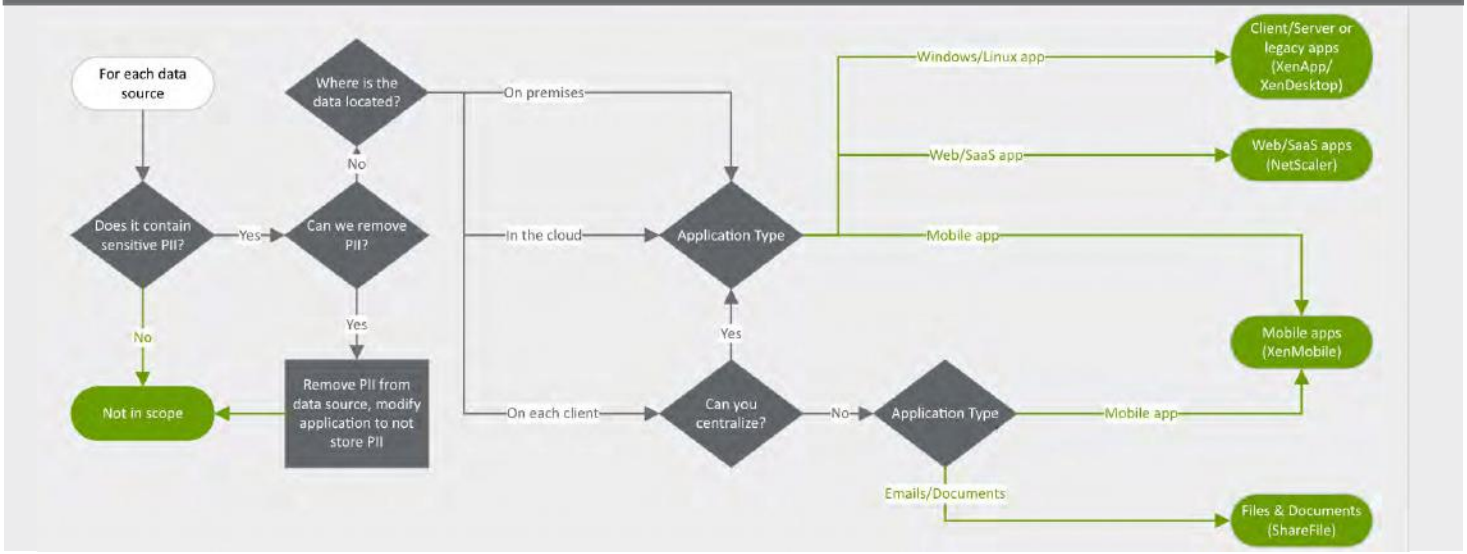
Complexity is considered one of the biggest enemies of security. You want to identify the minimum number of different architectures that could be used to secure the majority of the data sources that have been identified as critical and are storing data included in the GDPR scope.

The Pareto principle (also known as 80/20 rule) is important during this data assessment—and companies should try to minimize the effort required to secure the majority of data sources. Most enterprises have hundreds or thousands of different applications and data sources that are being used and they need to promptly identify those applications that contain critical data and don't meet the GDPR requirements. Automated application assessment solutions can reduce the time required to analyze applications. Citrix AppDNA can help identify applications that can potentially leak personal data with a module that detects vulnerabilities.

Many companies plan to use this mitigation period to transition to a more flexible IT model. While this goal is plausible, it is important to understand the timelines and choose realistic goals. Customers should choose solutions that can be gradually improved without the need for a complete redesign.

In the following few sections, we will present you with a few selected architectures that can provide a universal, secure, and proven solution to secure any type of data, ranging from web-based applications, through legacy client/server applications hosted on Windows or Linux to data stored in various documents or exchanged through emails.

GDPR reference architectures



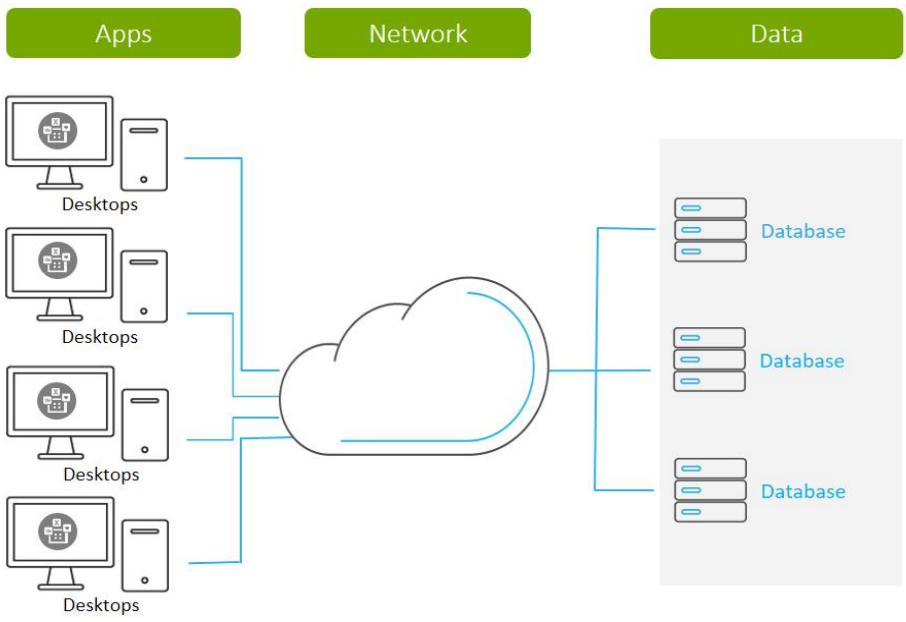
Securing Windows/Linux Applications
Architecture Overview

Trying to secure traditional client/server applications, whether they are running on Windows or Linux operating systems, has been challenging for various reasons.

The traditional approach was to secure each endpoint where these applications are installed. This involves management challenges, such as keeping all the endpoints up to date, encryption of the network traffic, data and workload encryption, implementing multi-factor authentication (MFA) and encryption of the locally stored or cached data. In traditional IT architecture, defenses need to be set up around all endpoints, applications and networks and the whole environment is as secure as the weakest point. This traditional approach to security has been failing with new concepts, like mobile workforce, expansion of security perimeter with cloud computing or BYOD initiatives.

Another common challenge for applications installed on traditional computers it to provide the same security functionality across the whole portfolio. It's common to have a multi-generational IT portfolio residing on a single workstation, from Office-based applications (using Microsoft Access database or custom plugins) through legacy Visual Basic to the latest professionally built applications. Making sure that applications that access sensitive data support encryption, multi-factor authentication and provide enough information for auditors has always been complicated.

Traditional client/server application delivery



Citrix has a long tradition of providing a platform for the secure delivery of these client/server applications. This secure delivery is based on offloading the client application piece onto a dedicated set of servers (XenApp/XenDesktop), specially designed, optimized and secured for application delivery. With decoupling the application and the endpoint, additional security features can be enabled. The advantage of this approach is that security features can be applied consistently, without requiring any changes or access to the source code and even to applications that are no longer actively supported.

In the next few points, we're going to cover how this architecture can help you secure the applications to follow GDPR standards.

Article 25 – Access to Personal Data
There are multiple ways to limit or prevent users from accessing published resources. The most basic method is to simply hide the applications or desktops from users by enforcing Active Directory group membership. This functionality is enabled on the XenApp level and doesn't require any special code changes from applications.

While the use of traditional username/password authentication is decreasing, more secure MFA is increasing. Even for internal networks, more and more companies are enforcing MFA requirements. With Citrix XenApp & XenDesktop and NetScaler, MFA can be applied to any client/server application, even legacy applications that are hard to maintain. The NetScaler appliance provides an extensible and flexible approach to configuring MFA, from time-based one-time tokens, through smart cards, user or machine certificates to biometric authentication (through third party integration).

This access can also be configured based on various other factors – for example the endpoint a user is connecting from, the security state of endpoints such as antivirus or firewall requirements or the network where the user is connecting from. Context-aware policies can be applied, even enforcing a specific geo-location or using more advanced security measures, such as requirements for user and/or machine certificates to access certain resources. You can learn more about context-aware security in the following blog post.

Even more flexibility is available through NetScaler's enhanced MFA feature call nFactor authentication. To learn more about different capabilities of nFactor authentication, refer to the following knowledge base article and one of the many deployment guides: https://support.citrix.com/article/CTX201949

The ability to provide centralized access and authentication is critical to in providing information about users connecting to applications. With Citrix XenApp and XenDesktop, all access to resources is brokered through a controller with historical data saved in a centralized database. This data can be accessed from ODATA API to provide integration with SIEM systems or provide copies for auditors if needed. To learn more about monitoring and reporting, see Comprehensive management and monitoring with Citrix Director and EdgeSight.

Aside from the monitoring and reporting of user access, all administrative changes and activities can be logged to a separate database. It is recommended to enable mandatory logging, where administrative activities are not allowed unless they can be logged in the configuration database first. To learn more, read about Configuration Logging.

Finally, for the most secure-conscious environments, it is possible to create a separate set of user identities and automatically switch to them using the federation and virtual smart card service called Federated Authentication Service. This approach can be used to further minimize the impact of lateral movement and contain the security breach.

Article 32 - Data Encryption in Transit
With XenApp and XenDesktop, only screen pixels are being transferred between the hosted XenApp server and endpoint, while the actual communication is maintained within the datacenter. By providing this additional connection hop (endpoint <-> hosting server <-> database), XenApp can ensure that traffic coming to and from the endpoint is always encrypted, even if the application itself doesn't support encryption. This encryption can be enabled for any application hosted on XenApp server.

This architecture supports end-to-end encryption between all components. You can read more in End-To-End Encryption with XenApp and XenDesktop whitepaper.

Article 32 – Data Encryption at Rest
While XenApp can help with the encryption between user and application, the backend itself remains out of scope for this solution. However, XenApp can be used to isolate unencrypted traffic and data during the transition period utilizing secure zones – making sure that all data is encrypted is a long-term process and encapsulating this data in an isolated enclave can provide the required security while the migration project is underway. You can read more about secure zones in this blog post: "Unsinkable": The Myth of Foolproof IT Security.

As for encryption on the endpoint, it is important to minimize data exposure at the endpoint and control data remanence. Data residing on the endpoint should be restricted, delivering only the minimum amount of data necessary, virtualizing all access to PII and ensuring that residual data, keystrokes and screen data are managed and protected. To learn more, read this blog post about Citrix ICA client footprint.

Article 32 – Data Isolation and Protection
Contrary to traditional desktops, XenApp servers usually have a much more restricted scope of operation – they are used to host a group of well defined, centrally managed applications with predictable behavior and centralized configuration options.

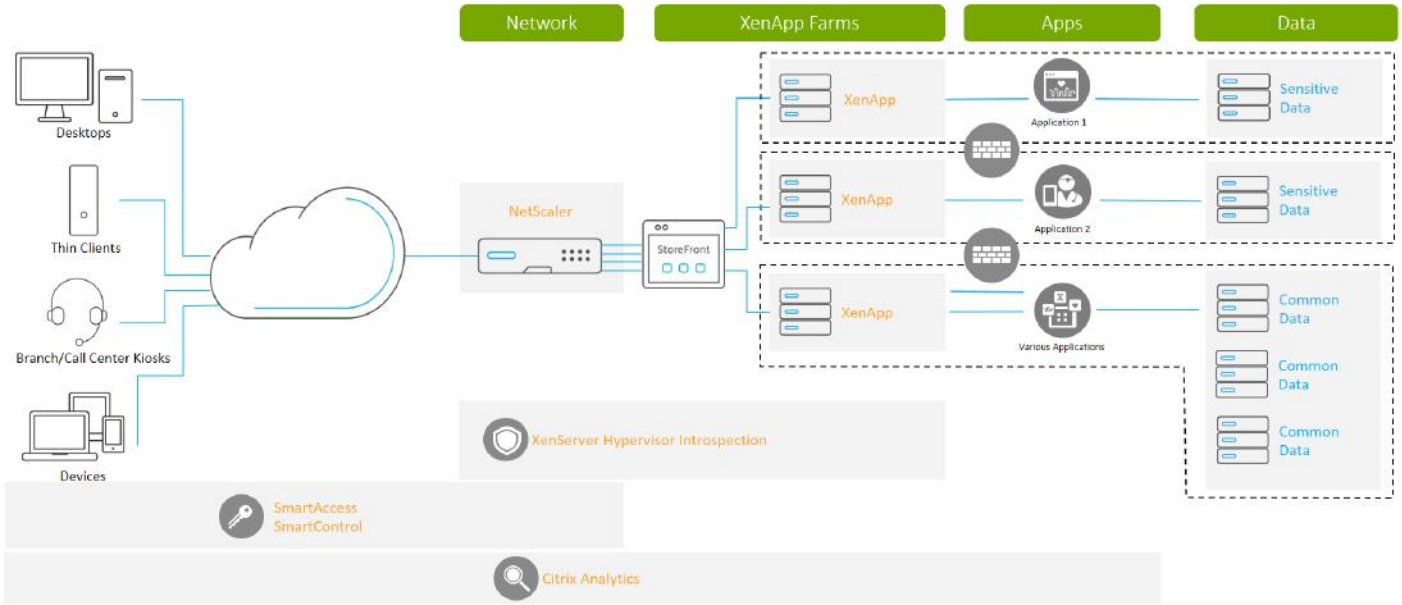
There are different ways how data and applications can be protected and isolated from each other. With aggregation of resources from multiple servers, it is possible to create groups of separated servers to host different applications with different trust levels.

Even if applications are hosted on the same server, it is common practice to isolate and secure them. XenApp servers are used to host well defined, centrally managed sets of applications. This means that these servers can support more restrictive security hardening than traditional workstations. Application whitelisting solutions such as WEM Application Security are much more useful with servers built for specific applications rather than general workloads. Allowing only specific white listed executables is much simpler on these special-purpose build servers than general workstations.

Security can be further enhanced by application of granular Citrix policies. These policies provide control over many aspects of the workspace: available printers, ability to access network drives or use clipboard and many more. A special template for "Security & Control" is included with all the best practices and recommended settings.

To learn more about hardening of XenApp or XenDesktop machines, you can read the System Hardening white paper.

Aggregation of applications with different trust levels



Securing Web/SaaS Applications
Architecture Overview

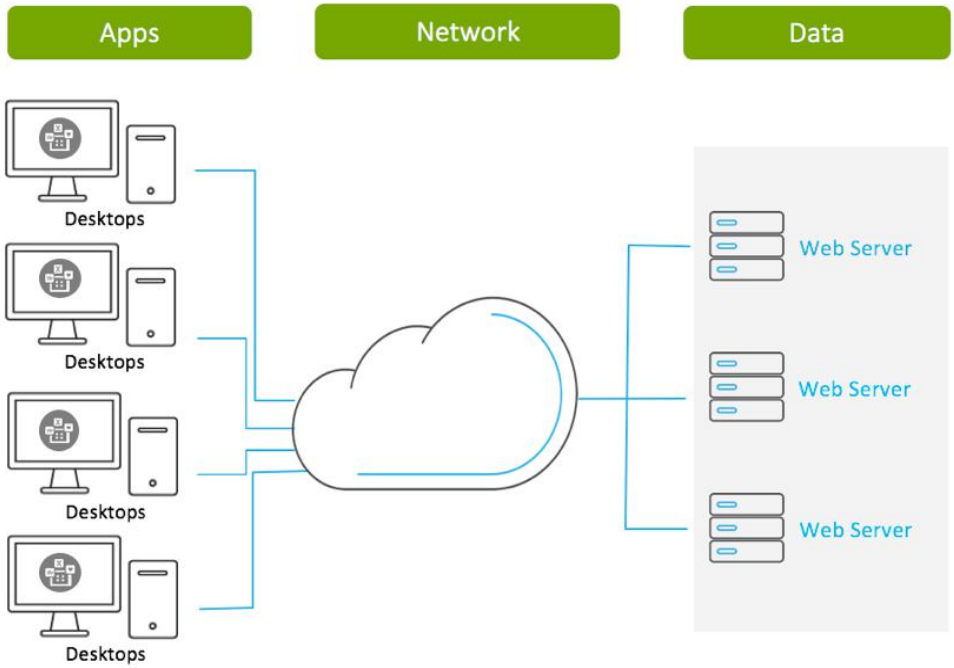
Web apps are architecturally different than client server apps but also similar in many ways – including suffering from security challenges. With web apps, a specific client is replaced with a single corporate standard or multiple general-purpose web browsers, with varying capabilities and dependencies. Although somewhat simplified, the same management challenges apply – keeping the browser up to date against vulnerabilities, encryption of traffic, and implementing multi-factor authentication.

The demands for legacy application support and modern capabilities for SaaS have driven conflicting requirements. There are two types of web apps – the born-on-the-internet-apps and webified apps-custom and legacy web apps that support the business. The born-on-the-internet apps drive the requirements on security and architecture – load balancing, scalability, failover, and performance. While the webified apps drive the requirements on supportability - browser plugins, extensions, and validating browser updates can break functionality.

At the core, the functional goal is for the end user to interact with web apps and manipulate data – including personal and sensitive data regardless if running in legacy environments or on SaaS apps pushing the limits of HTML5. Gartner recommends a two-pronged strategy. This is when an organization uses a legacy browser for running legacy applications, but also employs modern browsers for use with all other applications or sites, including general web surfing. That's where Citrix helps – tying together the user experience and security requirements for hybrid or bimodal web environments.

For the enterprise, maintaining multiple versions of multiple browsers, plugins, and applets while at the same time simplifying authentication and access is a pain point addressable with XenApp by building a remote browsing solution to separate internet and intranet web traffic from each other and the endpoint.

Traditional web application architecture

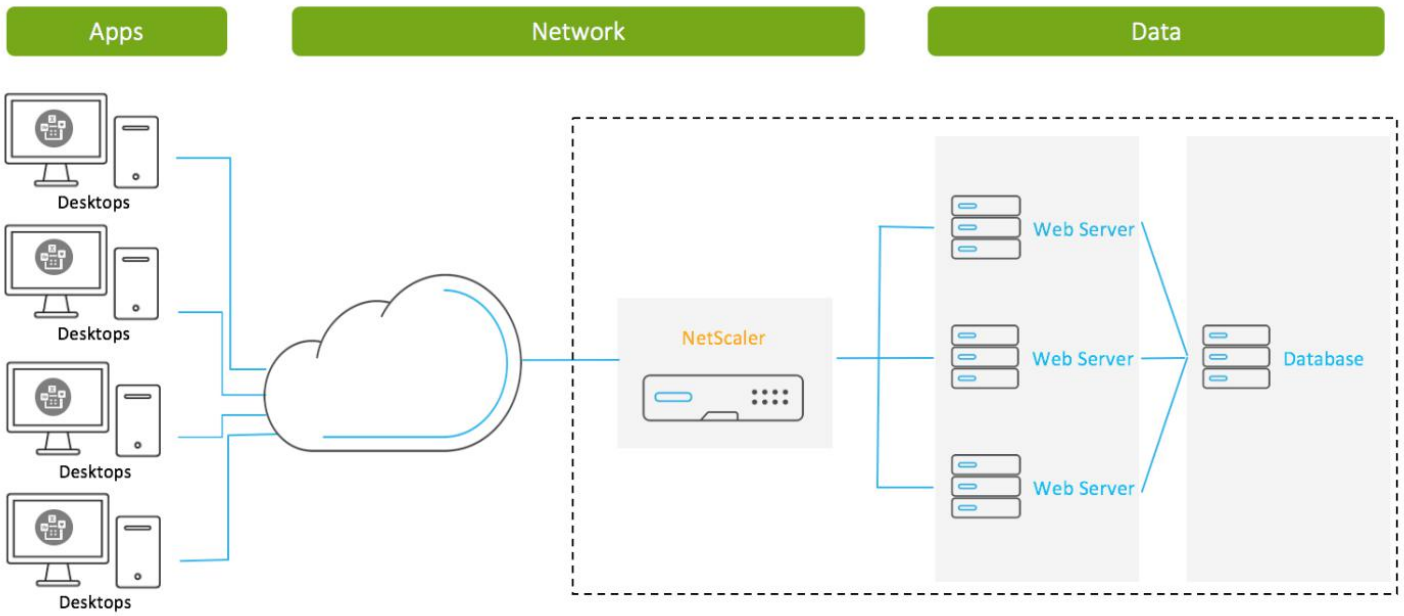


The second challenge has been to provide unified security features across the wide range of SaaS and cloud applications that typical enterprise is using – effectively giving back some IT control – especially in BYOD and mobile environments. An example is providing a unified multifactor authentication solution across all apps instead of a fragmented user experience.

Citrix has a long tradition of providing platform for secure delivery of web apps applications. This secure delivery is based on NetScaler as an Application Delivery Controller (ADC). NetScaler secures the session between the browser and the web app – by encrypting data in transit, maintaining strict access control, and data protection. This is largely based on its design as a reverse proxy that brokers connections coming from the browser to web app servers. And, with its position between the client and the server, additional security features can be enabled.

We're going to cover how this architecture can help you secure the applications to follow GDPR standards. These technical measures fall largely under the requirements or Article 25 and 32 where controllers are required to "implement appropriate technical and organizational measures."

Web application architecture with NetScaler



Article 25 – Access to Personal Data
Authentication, Authorization and Auditing are all core to controlling access to personal data. As an AAA proxy, NetScaler consolidates, extends, and enhances the traditional authentication schemes even in scenarios where the web apps do not natively support MFA. NetScaler supports authentication using username/password, multi-factor (MFA), time-based and one-time tokens (NetScaler has native OTP support), smart cards, user or machine certificates and biometrics. While this is especially important for internet facing web apps, some organizations with a zero trust networking approach are moving to require MFA for "internal" access.

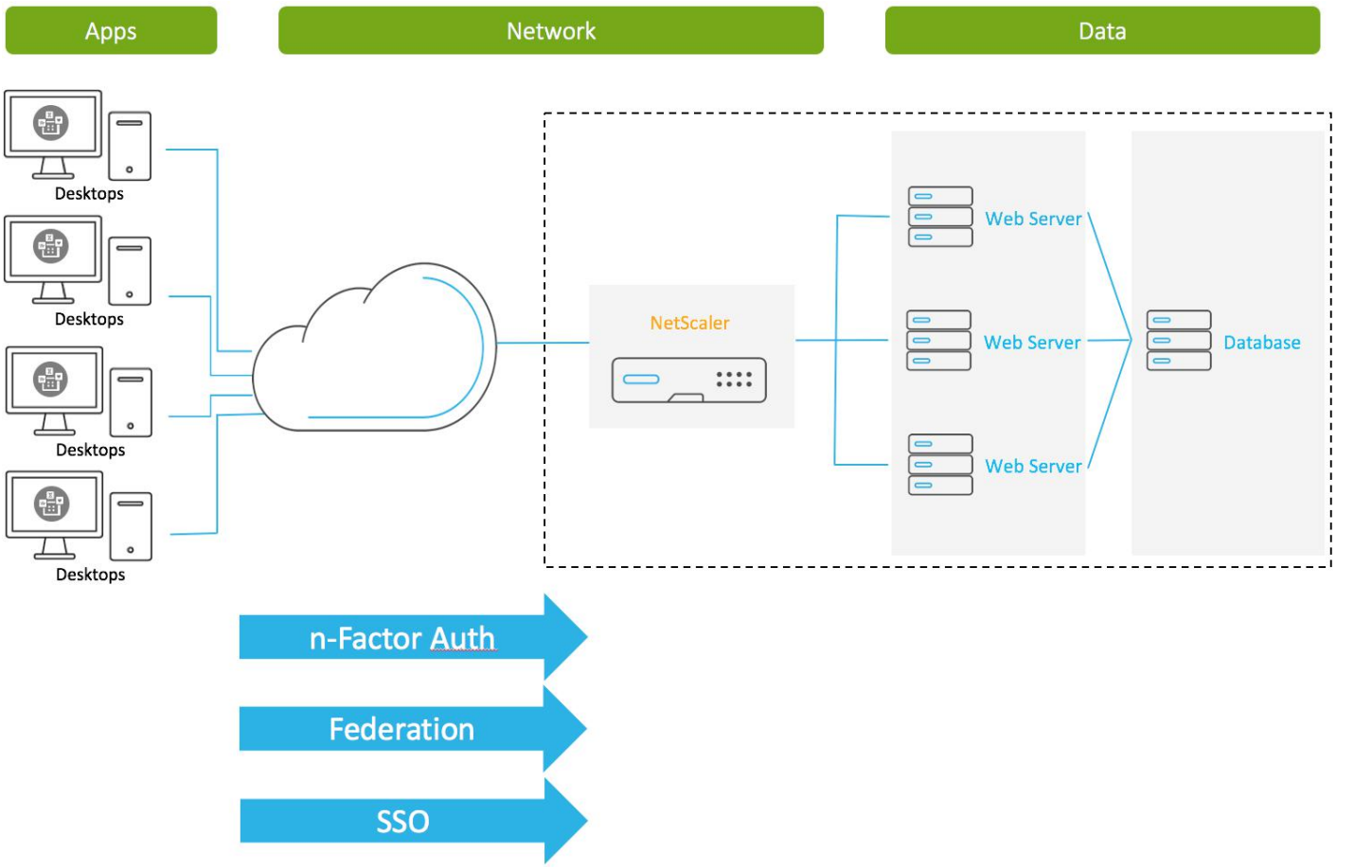
NetScaler's enhanced MFA called nFactor authentication takes into account capabilities such as SAML, client certificates, group extraction, and multiple passwords. Federation and SSO also provide and additional level of security and ease of use.

To learn more about different capabilities of nFactor authentication, refer to the following knowledge base article and one of the many deployment guides: https://support.citrix.com/article/CTX201949. A side note here is that SMS based MFA is not recommended as it has been deemed insecure by NIST.

Logging and visibility are provided through NetScaler Management and Analytics System (MAS). By capturing telemetry from NetScaler MAS provides:

- Security Insight against application layer attacks leveraging the application layer firewall
- SSL Insight for visibility into the security ciphers in use
- Gateway Insight for visibility into failed logins and End Point Analysis scans

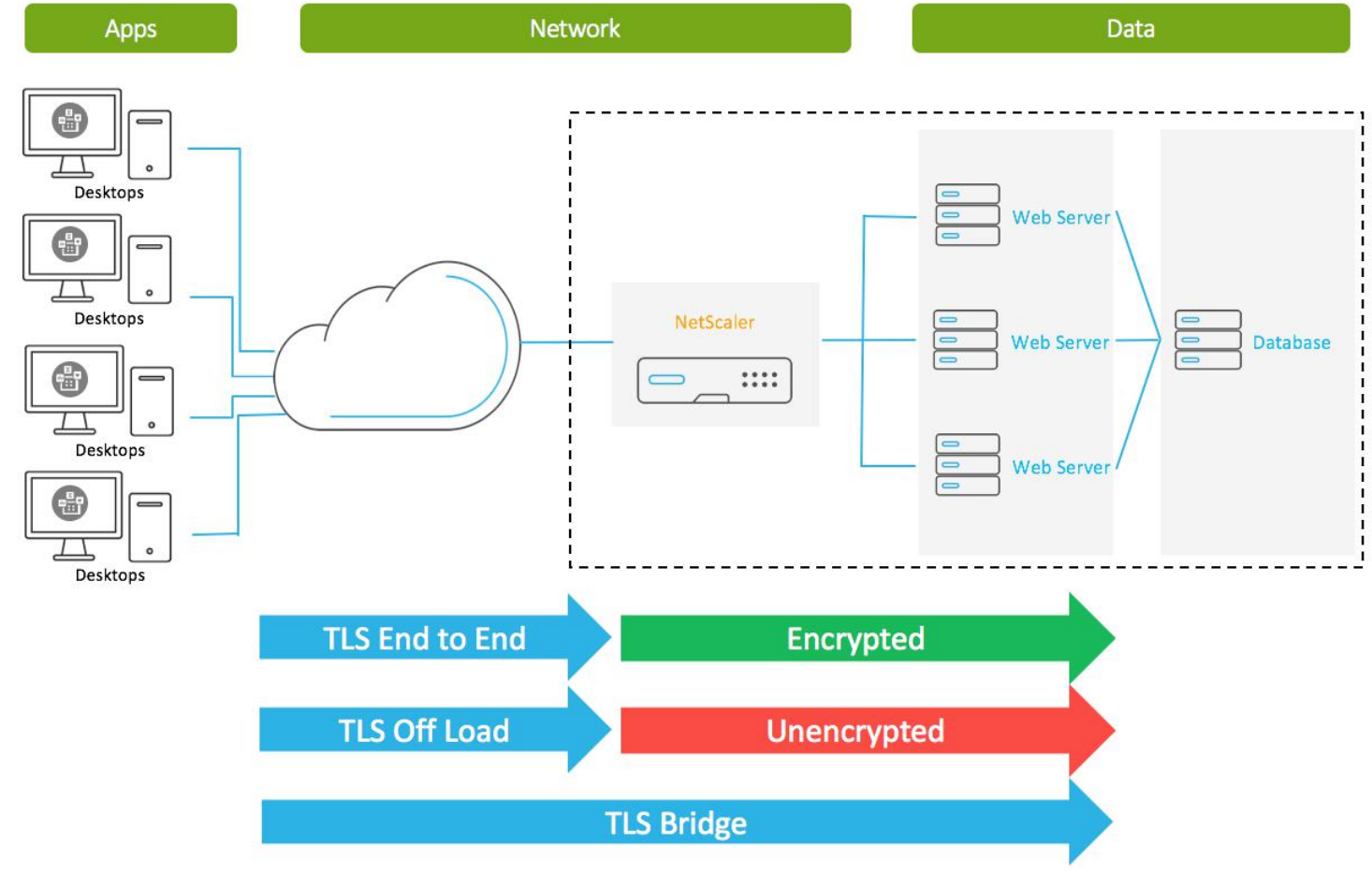
NetScaler authentication options



Article 32 – Data Isolation and Protection
NetScaler is a reverse proxy and as such it benefits from its placement in the network architecture, typically in a DMZ or security zone where it accepts the front-end user connection, creates a secure connection to the backend server, and has full visibility into requests and responses. Additionally, NetScaler can change the logic of the web traffic on the fly without requiring updates to the backend application. This includes encryption of not only packet header but body as it does deep packet inspection and rewrite.

NetScaler can ensure that traffic coming to and from the browser is always encrypted, even if the web server itself doesn't support encryption. This encryption can be enabled for any site proxied through the NetScaler. SSL offloading leverages the NetScaler to perform the resource intensive SSL/TLS handshakes thereby offloading them from the backend servers. For scenarios requiring end-to-end encryption, NetScaler can re-encrypt the connection to the backend. This allows the NetScaler to inspect and apply security policy to the traffic. SSL bridging is available for when requirements demand that NetScaler plays no part in terminating the connection. Using NetScaler with NetScaler Management and Analytics System (MAS) allows administrators to keep central configuration and visibility of the cipher suites in use, helping prevent negotiation of outdated ciphers.

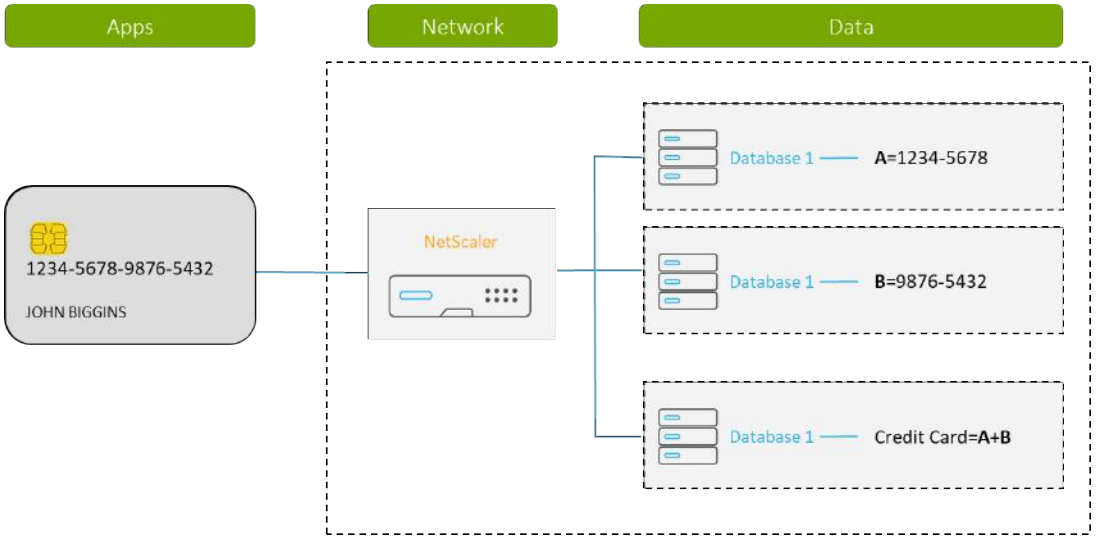
NetScaler encryption options



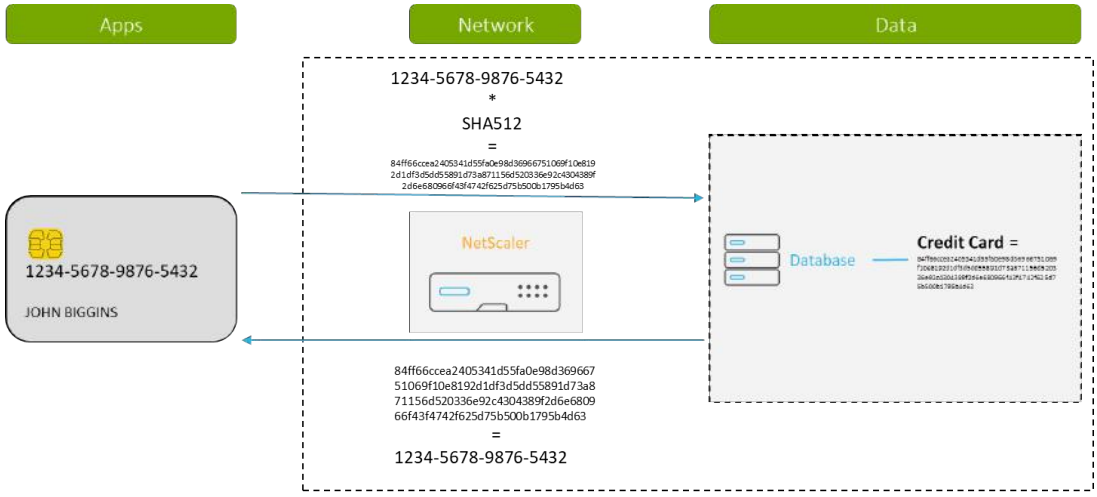
As a proxy between the browser and the web app, NetScaler protects the data flowing through it. That includes protecting from attacks against databases, attacks against the web app, and other users using its built-in application firewall. NetScaler protects against common web attacks including SQL Injection and XSS. You can read more about NetScaler App Firewall in our whitepaper Web application firewall – delivering must-have protection for the modern enterprise.

Protecting data also includes maximizing availability through Denial of Service (DoS/DDoS) attack protections. Combination attacks hit at all layers—so NetScaler provides Application layer defense (Layer 7), Transport layer defense (Layer 4) and Network layer defense (Layer 3). NetScaler not only provides a multilayer approach to DDoS protection but it is coupled with a built-in IP Reputation service which is an extremely effective tool in identifying the IP address that is sending unwanted requests. Since most malware comes from compromised sites, you can use the IP reputation list to preemptively reject requests that are coming from the IP with the bad reputation. NetScaler's forward proxy, Secure Web Gateway, filters out connections going out to the internet based on reputational risk - enforcing security policies on all outgoing web traffic, while blocking access to inappropriate sites on a per user/group basis.

Tokenization with NetScaler

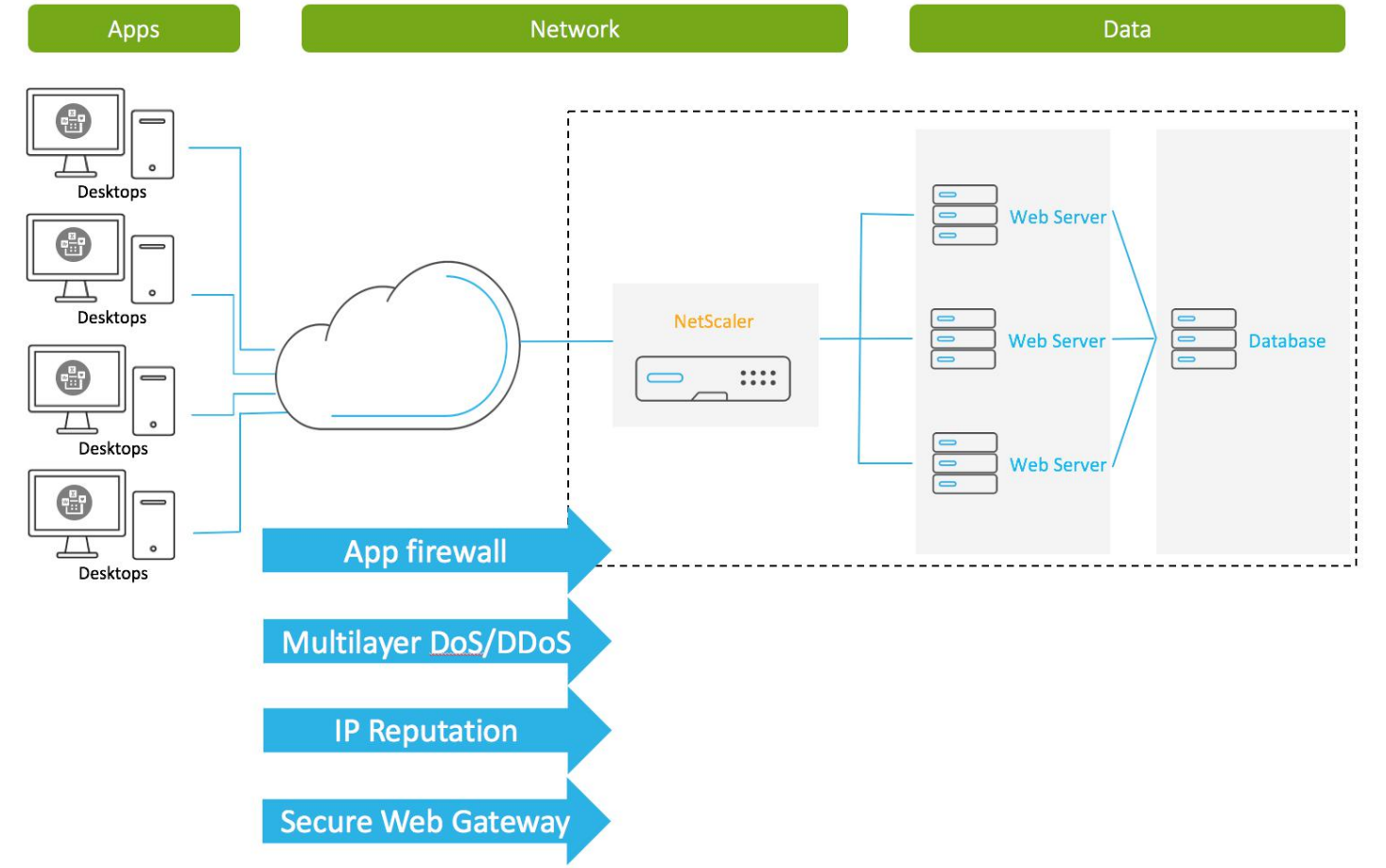


Pseudonymization with NetScaler



Pseudonymization is another control mentioned in Article 32. Conceptually, it's a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. This makes storing personal data more secure in the event of a breach – by using data segmentation. An example is tokenizing or hashing sensitive data that NetScaler parses for web-application traffic – i.e. hashing personally identifying data while transmitted between a controller and a processer. This is done in PCI-DSS regulated environments. For example, for cardholder data, tokenization guidelines are specific for the Primary Account Number (PAN). Tokenization replaces the PAN with a surrogate value called a token. De-tokenization is the reverse process of redeeming a token for its associated PAN value. The security of an individual token relies predominantly on the infeasibility of determining the original PAN by knowing only the surrogate value. Applications may not need the same level of security protection as associated with the use of PAN. For GDPR, storing tokens instead of PII is one alternative that can help to reduce the amount of personal data in the environment, potentially reducing the effort to implement GDPR requirements.

NetScaler data protection



Securing Mobile Applications
Architecture Overview

Mobile devices, particularly with BYOD ownership, present many challenges to enterprises trying to secure data. Their use in Enterprise has driven the inception of technologies to securely manage mobile endpoints. Used beyond the borders of Enterprise DMZs, on any public or private network, at any time, with apps from a variety of sources, mobile devices present special risks to companies seeking to secure their personal data.

- The GDPR controller must secure personal data used by corporate mobile apps despite the fact they're hosted on a user owned mobile device.

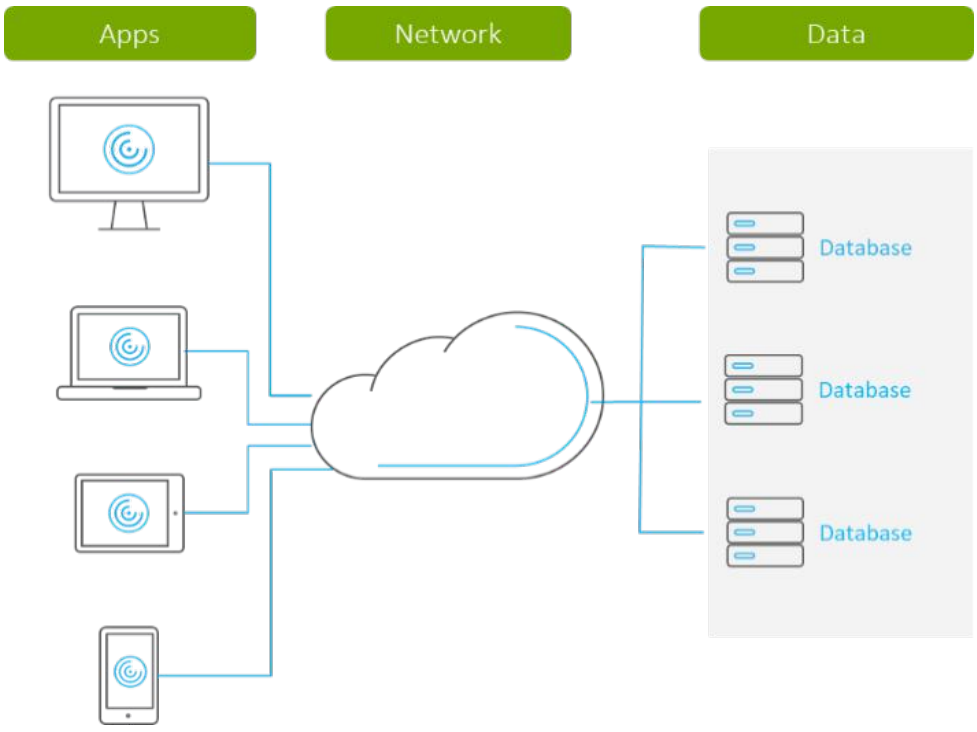
- Not only must the GDPR controller ensure the confidentiality, integrity, and availability of the personal data during its use, it must ensure that when a user exercises their right to erase that no artifacts are left behind and exposed to other apps or users, etc.

- Controllers must support file sharing and collaboration securely between enterprise mobile apps and be able to erase files from the device in a moment's notice.

- They need to help protect the platform OS, mitigate the risk of malware, and enforce device security and pertinent policies to control device functions that make data vulnerable to loss.

- Controllers need to provide Unified Endpoint Management across multiple platforms including control of critical software patches that include updates to address vulnerabilities.

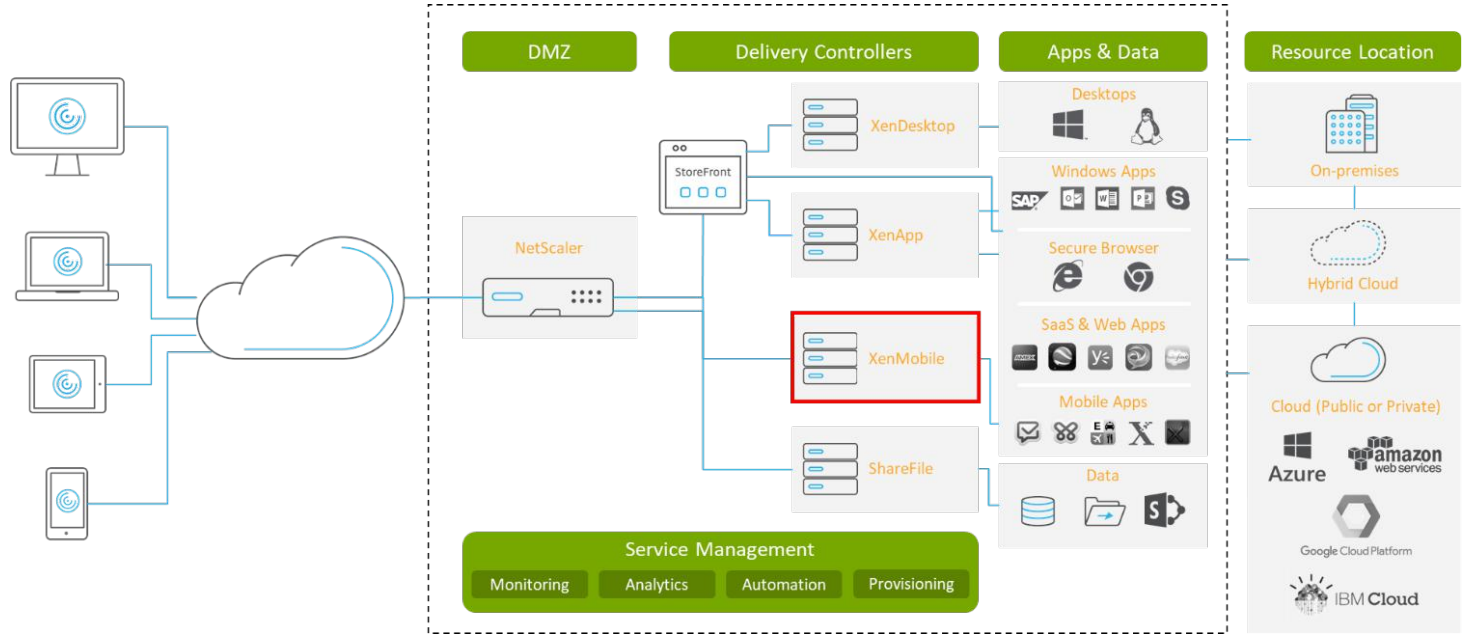
Traditional mobile device application architecture



Citrix XenMobile is a market leading Unified Endpoint Management (UEM) component of the Citrix Workspace. XenMobile securely manages a variety of mobile endpoints platforms ranging from iOS, Android, Windows and Mac to rugged mobile devices and IoT devices. XenMobile also manages a variety of mobile apps on endpoints and supports various delivery mechanisms including virtualized, web & SaaS, public app store, native enterprise mobile app and containerized mobile apps.

In the following sections, we will discuss how this architecture can help you secure PII on mobile endpoints. Also find a comprehensive general Citrix XenMobile Security whitepaper here.

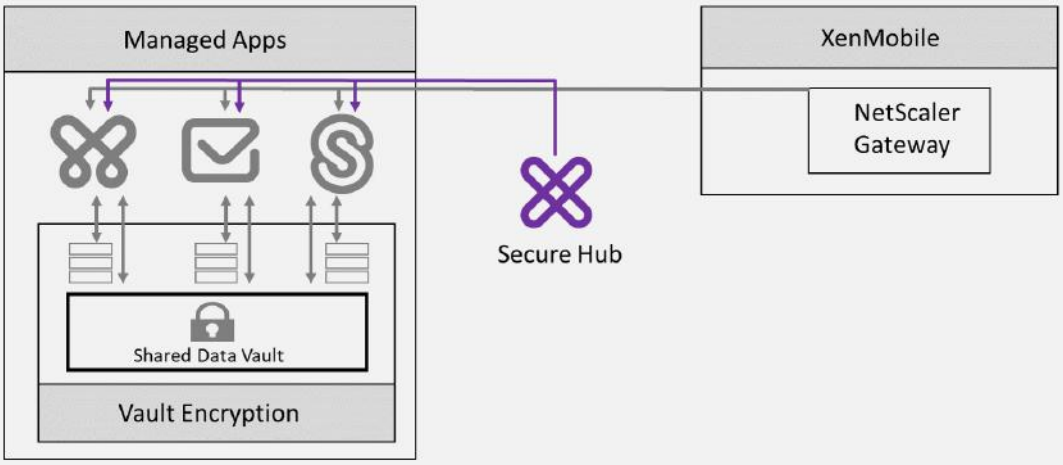
Citrix Secure Digital Workspace – mobility architecture



XenMobile MDX, the XenMobile MAM container technology, is a key part of the XenMobile solution to protect data. It provides end-to-end security maximizing protection of personal data, mitigating the risk of loss, by encrypting apps and data and managing secure transfer of data through 70+ MDX policies, including functional areas such as Authentication, Device Security, Networking, Encryption, Access Thresholds, App Interaction, App Restrictions, and other XenMobile App specific polices all applied on a per-app basis to mitigate the risk of PII loss. XenMobile MDX technology uses its own encryption libraries to host apps securely on iOS and Android platforms on top of platform encryption provided by the iOS keychain or device hardware encryption modes on Android which may or may not be active (depends on device encryption and passcode policies).

MDX Technologies help provide end-to-end protection by managing encrypted data transfers between device and intranet data stores, as well as between managed apps. Once these apps are installed, Secure Hub, a mobile app that provides access to desktops, apps and data, ensures that the desired policies are continuously enforced, always keeping IT in control of the enterprise content on users' devices. MDX also includes "microVPN", a per-app VPN that technology that integrates with Citrix NetScaler Gateway. It can be utilized seamlessly by managed apps to encrypt data traffic to and from the Enterprise intranet.

XenMobile MDX
end-to-end protection



Article 25 – Access to Personal Data
XenMobile provides a variety of enrollment methods to validate user identify prior to initiating Mobile Device Management and or Mobile App Management and subsequently access to secure data. For example, a two-factor solution can include One-time PIN (OTP) enrollment invitations in conjunction with Active Directory domain credentials. For environments with the highest security requirements, enrollment invitations may be linked to a device by SN, UDID, EMEI to uniquely identify the hardware.

XenMobile also provides a variety of multi-factor authentication options to validate the identity of enrolled user device/(s) including combinations of domain username and password, Radius, Azure Active Directory, certificate, or derived credentials (a high security federal standard based on government issued personal identity verification cards). Certificate and domain authentication used in conjunction with XenMobile pin is a popular secure combination that provides a great user experience.

Through these links learn more about XenMobile enrollment methods and multi-factor authentication options through Secure Hub. Also find deployment guidance based on security posture.

Article 32 - Data Encryption in Transit
XenMobile supports Data Encryption in Transit through several methods such as:

- Containerized with embedded VPN when apps utilize the XenMobile SDK
- Platform based utilizing a Citrix NetScaler VPN client
- Through policies to utilize native platform OS VPN functionality

The XenMobile SDK, or MDX technology, with microVPN which provides secure per-app VPN functionality to encrypt data in-transit between the mobile endpoint and intranet backend. It works in conjunction with Secure Hub and Citrix NetScaler to ensure MDX app traffic is directed over a dedicated encrypted VPN. It is unique Citrix XenMobile technology that provides seamless encryption of data in transit. Microsoft is adopting Citrix XenMobile microVPN for its mobile apps such as Intune Browser.

For more information see this microVPN FAQ; configuration of Android platform per-app VPNs using Citrix VPN for Android or iOS; or the configuration of platform per-app VPNs using native functionality.

Article 32 – Data Encryption at Rest
XenMobile supports Data Encryption at Rest through XenMobile MDX with Citrix-provided encryption libraries, or through platform level encryption directly or indirectly in conjunction with partner containerization solutions.

XenMobile can provide encryption at rest on any supported mobile device independent of platform encryption. The XenMobile secure app container technology, MDX, uses its own software applied data encryption using FIPS compliant algorithms making the risk of data loss is virtually impossible.

Device level encryption varies by platform. Apple's iOS features a file system with the OS information and user data written to flash memory. It also uses a factory-assigned device ID and group ID with the device user's passcode so only that passcode can unencrypt data on the phone or tablet. Android also provides encryption, although not every device manufacturer creates hardware that supports it and users can turn encryption off accidentally or deliberately with a factory reset on Android devices.
Find more information about the MDX Toolkit, MDX policies, and integrating with MDX in Citrix documentation.

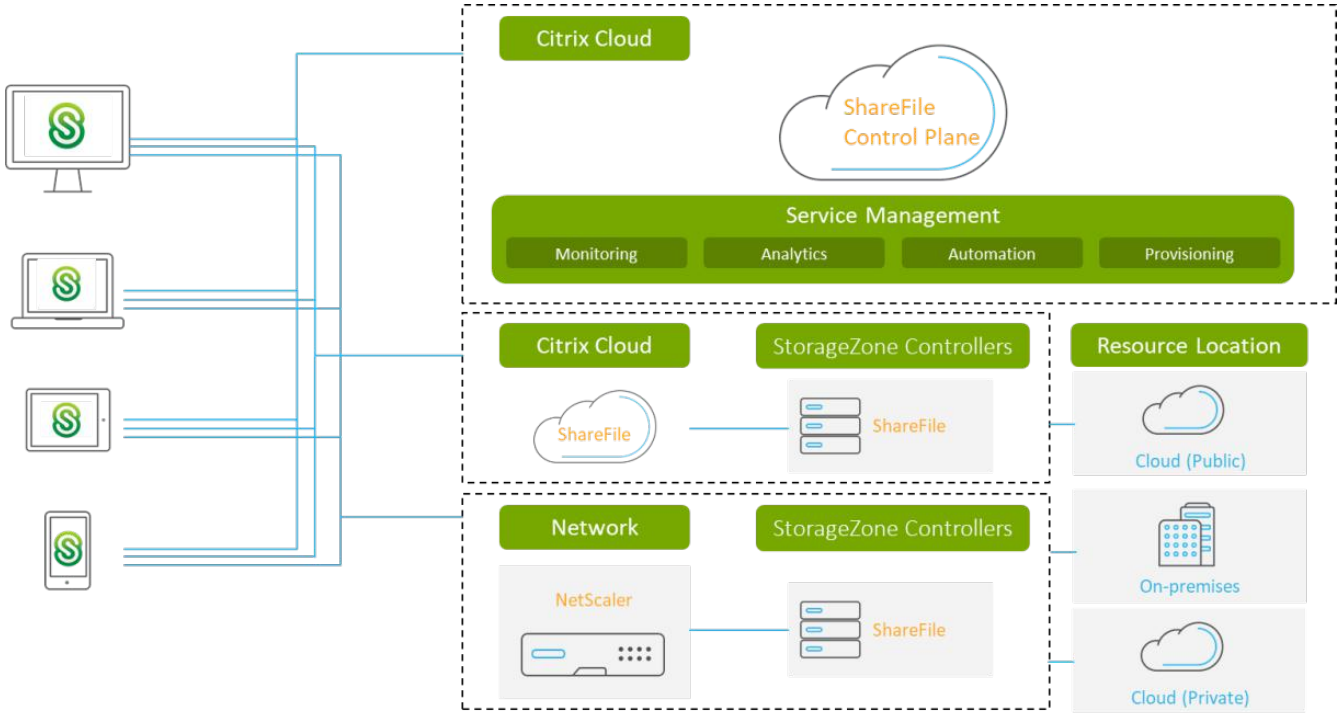
Article 32 – Data Isolation and Protection
Containerization enables mobile BYOD programs in corporate environments empowering users to use mobile endpoints as an enterprise device and personal device simultaneously by separating apps and data. It helps enterprises prevent malware, intruders, system resources or other applications from interacting with the application and any of its sensitive information. XenMobile enables containerized native mobile apps through MDX technology, and it also integrates with several partner container solutions providing value-add by integrating many broad app and device management capabilities.

Securing Files with Workflows
Architecture Overview

Many of our daily workflows consist of the creation of files and collaborating on those files with others. In many cases those files contain personal data, such as name and address, Social Security numbers or credit card details. Unfortunately, there are many examples of data leakage occurring, from lost USB drives filled with files containing personal information to phishing attempts to access files on secured systems with employee permissions. Under GDPR it is necessary to not only secure and control this information in every step of the process, from storing these files inside a repository to internal and external collaboration and providing context-based access to the files, but also to monitor for irregular activities and report on who has which permissions to which files.

Citrix ShareFile provides a range of controls to help organizations become and remain compliant under GDPR. This starts by having a choice on the location where files are being stored, either inside one of the Citrix-managed StorageZones in different global regions or in a StorageZone managed by the customer in their own datacenters or private cloud. Multiple locations can be used, allowing for the optimal location to store each individual file. By leveraging the StorageZone Connectors technology to access existing repositories, such as network file shares or SharePoint document libraries, all file related activities are done through a single platform. This makes auditing the activities easier, as well as making sure that the correct permissions are in place.

ShareFile StorageZones with global regions



Collaboration on files has not changed much over the past years. Most of these workflows use email to send files to a group of recipients, gather the feedback from each of those recipients as separate emails to the thread, then update the files and start this cycle again. As such, multiple messages and copies of the same document are stored inside the email platform, which makes it more difficult to comply with GDPR policies. By leveraging the ShareFile Feedback and Approvals workflow to collaborate on documents, all feedback and document revisions are stored in a single place, making it easier to comply with such regulations.

Many paper-based workflows in an organization contain PII data in some form. For instance, the workflow to hire people involves multiple steps where personal information needs to be recorded and shared. All this information needs to comply with GDPR regulations, centralizing and digitizing these workflows have a positive impact. ShareFile Custom Workflows allow this personal information to be securely captured, securely stored inside ShareFile and, where needed, to be completed with an electronic signature. All information is stored together in a single location and is audited for who accesses and modifies this information, providing a practice that allows to stay compliant with GDPR.

Article 32 - Data Encryption in Transit
All connections between ShareFile clients and the ShareFile SaaS Control Plane, between ShareFile clients and ShareFile StorageZones, as well as between ShareFile SaaS Control Plane and ShareFile StorageZones are TLS 1.1/1.2 and encrypted with up to AES 256-bit encryption.

ShareFile clients for iOS and Android which are managed by XenMobile can also leverage the embedded VPN capabilities provided by the XenMobile SDK. See "Data Encryption in Transit" in the Securing Mobile Applications section of this document for additional details.

Article 32 – Data Encryption at Rest
ShareFile offers a flexible architecture which provides customers the choice of where files are stored at rest. These repositories are called ShareFile StorageZones and are managed by either Citrix or the customer.

For StorageZones managed by Citrix, hosted in either Amazon AWS or Microsoft Azure, files are stored at rest with 256-bit AES encryption. The encryption key is a shared key for all files stored across all ShareFile tenants. Alternatively, this can be a customer-managed encryption key, configured in Amazon Key Management Service. When the StorageZone is managed by the customer, per-file encryption can be enabled inside the StorageZone configuration. When enabled, all files are encrypted with 256-bit AES encryption.

Files are not only stored at rest inside the repository in the data center or cloud, but also on the devices being used by employees. As a best practice, it's recommended to always use full drive encryption on Windows and macOS devices. On top of that, ShareFile allows controls for both corporate-owned and BYOD devices. ShareFile allows for a remote wipe of the ShareFile files, removing only the corporate files and not touching the personal files of the employee. When a remote wipe is initiated, the ShareFile client will send back all file activity that has occurred offline between the wipe command and the actual wipe of the ShareFile repository, which occurs when ShareFile logs on to the ShareFile SaaS application tier.

Similar safeguards are in place for ShareFile for iOS and Android. All files at rest are encrypted by using the device keychain and encryption capabilities. When using a XenMobile managed version of ShareFile, the encryption key is stored inside Secure Hub. And because ShareFile provides a robust rendering and editing engine for Office files and PDF documents as part of the mobile ShareFile clients, files don't have to leave the ShareFile applications to be reviewed or edited. ShareFile offers multiple mobile device management to secure the files, for instance by blocking access from jailbroken devices and blocking opening files in other applications. When using XenMobile, additional advanced policies for more granular control are available.

Article 25 – Access to Personal Data
Authentication to ShareFile is either controlled by a username and password (ShareFile credentials) or by using corporate credentials through a SAML Identity Provider.

When using ShareFile credentials, the password for the user is subject to the password policy that has been configured. This password policy controls the requirements for the password in terms of complexity, history and how often it must be changed. The password is stored hashed and salted inside the ShareFile SaaS application tier, which makes it impossible for anyone to retrieve the password in clear text from the platform.

SAML based authentication is commonly used for authentication to cloud services. Instead of authenticating directly to the enterprise directory, e.g. Active Directory, the authentication is done against an Identity Provider. This removes the need to expose the enterprise directory directly to ShareFile, but still allows users to authenticate with their enterprise credentials. The Identity Provider controls how the user must identify and authenticate itself, based on the context of that authentication attempt. This allows for additional security measures like multifactor authentication for authentication attempts from outside the corporate network and SSO based on the Windows authentication token for domain-joined devices.

Article 32 — Data Isolation and Protection
ShareFile integrates with market-leading Data Loss Prevention products for customer-managed StorageZones and Cloud Access Security Broker services for any type of ShareFile StorageZone, enabling content-aware restrictions. Documents stored inside a ShareFile StorageZone are examined by the same policies that are already set up for other repositories and based on those scanning results, files can be blocked to be downloaded or shared with others.

Sharing files is a key component of modern workflows. This makes controlling the access and permissions to documents containing privacy related information a priority, especially when the files are outside the direct control of your own security policies. With ShareFile Information Rights Management (IRM) documents are encrypted when the files are downloaded, controlling who can open the file. This prevents sensitive information from being seen by unauthorized people, even when the authorized person sends on the file to someone else. With the ShareFile IRM policies you can also control what permissions the recipient has when opening the file. This can range from View Only access to the ability to edit and print the document.

ShareFile uses versioning to store different versions of the same file. This is not only very convenient to review changes made to documents, but this can help when recovering from a malware or ransomware attack. By restoring the files to the state before the attack, data loss can be minimized, and the recovery time can be reduced by automating the restore to previous versions by using the ShareFile PowerShell cmdlets.

For customers requiring all files to be archived for compliance purposes, ShareFile offers this capability. When a user deletes a file, or when the file is automatically deleted by a retention policy, the file is stored inside an archive instead of being fully deleted from ShareFile. Dedicated auditors can review the contents of the archived files, including access permissions, during an investigation.

Summary

Citrix Workspace simplifies the management of your systems and data by centralizing services in the data center or cloud as a digital workspace. It can help Citrix customers with their journey to GDPR compliance by ensuring applications are centralized and enclaved, data is protected when shared or distributed, access to data and resources is controlled, and IT is brought together for application and data-specific security.

To learn more about security and compliance with Citrix secure digital workspace solutions, please visit https://www.citrix.com/it-security/.

About the Authors and Contributors

Matthew Brooks
Florin Lazurca
Rob Sanders
Martin Zugec

A special thanks to the reviewers of this Security Whitepaper:
Daniel Feller
Chris Mayer
Kurt Roemer
Stephen Twynam

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States