



## **Nirvanix Sets the Standard for Military-Grade Security in Enterprise Cloud Storage**

Surveys of cloud users and potential users, analyst reports, and industry and popular press articles cite security concerns as one of the top barriers to cloud adoption or further implementation. At Nirvanix, we take these concerns seriously and have made the security and integrity of our customer's data and systems our highest priority. In fact, security is baked into our software and processes, not an afterthought. Nirvanix implements unparalleled security safeguards and processes at the user, application, data storage and physical data center levels to protect media & entertainment companies against piracy, prevent unauthorized access to healthcare electronic records, and help financial services companies comply with regulatory requirements for long-term archiving and eDiscovery.

Leveraging advanced technologies and processes Nirvanix has implemented multiple layers of security in its Cloud File System™, Cloud Storage Network™ and data center environments to protect customer data. Customers can now enjoy the superior economics and on-demand flexibility of cloud storage without having to worry about their data regardless of whether they choose the public, hybrid, or private cloud options under the Nirvanix CloudComplete™ portfolio.

This white paper looks at specific external and internal threats posed to cloud storage and at the countermeasures Nirvanix adopts to mitigate them.

## Nirvanix Addresses Threats to Customer Data

Once data is stored in the Nirvanix cloud, data access is limited to customer-authorized personnel and by Nirvanix at the customer's direction or to perform services and maintenance as agreed to by the customer. However, given the very real potential of hacker attacks with the intent of accessing sensitive data or stealing personal and credit card information, Nirvanix has identified a number of external and internal threats and developed a set of countermeasures to prevent them.

### External Threat: Impersonation

To protect customer accounts, Nirvanix requires three credentials that establish the authenticity of the user: the private application key, the username, and the password. A fourth credential exists, the application name, for when the application needs to be referred to over public channels without compromising the application key. To safeguard these credentials, we employ session-based authentication as a means to identify a user for every HTTP request instead of making users send their credentials each and every time they send instructions.

The client initiates a session by logging in with the user's credentials, protected by SSL encryption. Upon successful authentication, the server sends a session token to the client. Subsequently, the client sends back this token with every request to the server as the means to identify the authenticated user and valid session. Thus, the session token acts as a temporary replacement for the actual credentials.

As with any password-protected, session-based system, Nirvanix Web Services could be vulnerable to impersonation attacks when the perpetrator garners enough information to fool the system into believing that fraudulent requests are coming from a legitimate user. The following sections describe these threats and what Nirvanix does to mitigate them.

**Password cracking:** In this scenario, attackers know the usernames of the accounts they want to gain access to and attempt to log in by trying different passwords until they guess the correct one. There are several known techniques employed by hackers, including:

- Personal information—The attackers have personal knowledge of the users who are employing passwords related to themselves in some way, such as a birth date, birthplace, the name of a significant other, etc.
- Dictionary attack—The attackers choose from a list of words that people have a tendency to select as passwords. These include common words in various languages, names of people and places, and frequently used passwords.
- Brute force attack—As a last resort, the attacker tries all possible passwords.

**Countermeasures:** Nirvanix protects users in three different ways.

First, passwords can be strengthened by a password policy that makes users choose more effective passwords. Typically users may be required to include:

- Both upper and lower case letters
- One or more numeric characters
- One or more special characters

Since our Cloud Storage Network is integrated at the end-user level to our customer's online applications, we do not impose any password policy, leaving it up to each application to set the appropriate level of password security for itself. It is our customer's decision to make the trade-off between security and convenience.

Second, limiting the rate at which attackers can submit guessed passwords greatly enhances security. Nirvanix enforces an industry-standard 15-minute lockout on any account following five consecutive failed-login attempts within a span of two hours. This policy is enforced separately for master accounts and child accounts (application owners and their end-users, respectively) but applies to both portal login attempts and web service login attempts.

Finally, Nirvanix requires the application's private key for authentication. As long as the application is not compromised, our services will be secure. If at any time application owners feel that the private key has been compromised, they can regenerate a new key.

**Eavesdropping to steal user's credentials:** In this scenario, the attacker intercepts and logs network traffic to and from the Nirvanix Web Services using a packet sniffer. The attacker can eventually reassemble and decode the captured packets to analyze their content. If the user's credentials are transmitted in clear text, the attacker can easily steal the login information.

**Countermeasure:** Nirvanix requires that all login credentials be transmitted over encrypted channels. All requests containing login information such as login and password change must be sent over HTTPS/SSL.

**Session token manipulation:** Here the attacker tries to manipulate a session token to gain unauthorized access or privileges.

**Countermeasure:** This kind of attack is more of a threat to client-side session management than server-side session management. While the client-side session token contains actual authorization information (and is therefore open to manipulation), the server-side session token merely acts as the ID of the session so that the attacker has no way of changing the property of the session. Nirvanix employs server-side session management with session tokens that are long enough and issued in random sequences to comply with standard principles of session security.

**Session hijacking:** In this scenario, a legitimate user logs in and establishes an authenticated session. The attacker eavesdrops and obtains the session token by decoding and analyzing captured packets. While the session remains active, the attacker uses the session token to access the user's content.

**Countermeasures:** Nirvanix addresses this potential threat in three ways. Most importantly, we associate the user's IP address at login with the session token. Therefore any request using that token which comes from a different IP address is rejected unless the customer explicitly relaxes this security feature. Random attacks of this kind on the Internet are therefore impractical. The attacker and the end-user must share the same public IP address for the hijack to be feasible, limiting attacks to scenarios where the attacker is in the same work offices, school, or Internet café with the user.

A session can also be immediately invalidated with a logout. Nirvanix strongly encourages application developers to implement the best practice of logging out of the service after every transaction. To shorten the window during which the attacker could hijack the session, the application should log out as soon as possible after accessing the content. As a safety net, Nirvanix also forces the expiration of sessions after a period of inactivity.

Last, if security is the top priority, all requests should be made over encrypted channels with HTTPS/SSL. All Nirvanix Web Services are available over HTTPS. Again, because data encryption requires overhead, we leave it up to each application to evaluate the trade-off between security and performance rather than dictating that all communications must be secured.

Note that even if the session is hijacked, Nirvanix login credentials are never compromised. From the session there is no way to retrieve either the application private key or the user password. This limits the damage to one session, and exposure ends with logout.

### External Threat: Eavesdropping to Capture Data

In this scenario, the attacker simply captures network packets to steal users' data as it is being transferred to and from the online storage provider. It is different from the session hijacking threat in that the attacker does not have control of the user's account. However, this type of attack is also much easier to carry out because it does not have the IP address restriction or time constraint of a session. The attacker can log all packets and then analyze them at a later time.

**Countermeasure:** To ensure privacy of the user's data, in those cases when privacy is of the utmost concern, all upload and download requests should be made over encrypted channels. Again, Nirvanix leaves it up to the application to decide between security and performance by making it possible for all web services to be carried out over HTTPS/SSL security.

## External Threat: Database Attack

**SQL injection:** Here the attacker exploits vulnerability in the database layer of the web services. The attacker can cause unintended SQL statements to be executed by injecting them into user input using a carefully crafted sequence of escape characters. This threat is only present when dynamic SQL statements are used and user input is not properly filtered.

**Countermeasure:** All database access from Nirvanix Web Services is made through parameterized stored procedures. Parameterizing input values and type-enforcing them effectively filters user inputs. Furthermore, Nirvanix Web Services are only granted permission to execute stored database procedures, without having access to the actual tables. This keeps them from performing anything other than actions designated by the stored procedures.

## Internal Threats

Here the attacker attempts to break into the storage provider's internal network and steal users' data at the source.

**Countermeasures:** Nirvanix Web Services provide four levels of defense against this kind of attack.

1. All servers are protected by an effective firewall.
  - The servers have no external access other than the specific services they are providing. Database servers are not accessible from the outside.
  - No network management device can be accessed from the outside.
  - IP spoofing is completely eliminated as a threat because the firewall filters ingress and egress and Nirvanix does not employ any host-based authentication measures.
2. Functionality is carefully compartmentalized.
  - Only the exact software components needed to perform the server's role are installed on each server host.
  - Each software component executes as an authenticated process, specifically created for that software role. The permissions given to that process are the bare minimum needed for the component to perform its function. This includes access to databases through Security Support Provider Interface (SSPI).
  - Similarly, each server only has network access to other servers that the software components running on it need to access.
3. Sensitive data is disassociated and separated. Information about user files (file system metadata) and their corresponding physical files (file data load) stored on disks are segregated into separate networks. This separation provides added protection for user data confidentiality in the very remote case that an attacker does manage to break into one network.
4. All customer-sensitive data stored in the database is either strongly encrypted or strongly hashed with secret keys in the very unlikely event that an attacker does manage to break into the database.

## Highly-secure Data Centers

From a physical integrity perspective, all Nirvanix storage nodes are located globally in Tier III facilities that use financial-grade physical and biometric procedures to secure access to the nodes and your data. In addition, Nirvanix has undergone a Big 4 security audit and has certified control processes via the Statement on Auditing Standard 70 (SAS 70) Type II. Physical security of the data centers is provided by on-site 24x7 security combined with CCTV digital camera coverage of the entire center, including cages, with detailed surveillance and audit logs, as well as integrated with access control and alarm system. The buildings themselves are protected by concrete bollards/planters as outer perimeter boundaries and bullet-resistant exterior walls.

## Highest Data Availability and Integrity

**High-Availability Distributed Node Architecture:** The Nirvanix Cloud File System was built for 99.999% availability with a clustered node architecture that allows Nirvanix to provide enhanced levels of service and data protection. One key feature of the Nirvanix architecture is dynamic load-balancing of traffic by replicating content in adjacent storage servers, thus eliminating resource contention for best-user experience during peak loads. Sudden traffic peaks do not affect end-user experience for files stored in the Cloud File System. The node architecture in the Cloud File System also supports intelligent routing of files to the closest global location for accelerated performance. Files may be moved permanently or temporarily to a geo location to address local demand for that content. As Nirvanix deploys additional nodes around the globe, the architecture balances localized demand from users in a geo-location by moving content to the closest storage node available.

**Robust Infrastructure:** Nirvanix offers guaranteed quality-of-service levels, not best efforts, to meet our customers' data availability and disaster recovery needs with offsite data protection, policy-based geo-replication, and data integrity checking. Using Nirvanix's policy-based data replication, guaranteed SLA ranges from the standard 99.9% for one copy, to 99.99% for two copies or 99.999% for 3 or more copies. These SLA levels are backed by superior customer support and 24x7 monitoring across 7 layers in our Network Operations Center (NOC).

Data availability and integrity are ensured through an architecture that includes RAID-6 Protected Data Storage, RAID-10 Protected File System, fully redundant infrastructure, data backups, multi-homed bandwidth, and hardware standardization in order to minimize variability. The service's highly scalable infrastructure allows Nirvanix to maintain high performance levels even as customer data (and Nirvanix customer base) grows, media files increase, bit-rates and media quality increases and content libraries expand. Our superior bandwidth capacity allows Nirvanix to support traffic peaks associated with unexpected circumstances or special events.

## Conclusion

Protecting customer data in the Nirvanix cloud is a top priority. We take every precaution and preventive measure to safeguard the integrity of our enterprise customers' data. In some areas where trade-offs can be considered, we offer a flexible model to let each application choose the appropriate level of security while never leaving data exposed to external or internal threats.

## The Time to Move to Nirvanix Cloud Storage Is Now

With multiple layers of security in place, Nirvanix customers can enjoy the superior economics and on-demand flexibility of cloud storage without having to worry about their data. The Nirvanix CloudComplete portfolio of cloud storage solutions is enterprise-ready now.

Visit [www.nirvanix.com](http://www.nirvanix.com), call 619.764.5650 x330, or e-mail: [info@nirvanix.com](mailto:info@nirvanix.com) to get started.



---

9191 Towne Centre Drive, Suite 510 | San Diego, CA 92122  
Tel 1.619.764.5650 | Fax 1.619.374.7469 | [info@nirvanix.com](mailto:info@nirvanix.com) | [www.nirvanix.com](http://www.nirvanix.com) | [twitter.com/nirvanix](https://twitter.com/nirvanix)

Visit our web site at [www.nirvanix.com](http://www.nirvanix.com).

© Copyright 2011 Nirvanix, Inc.  
All rights reserved. Nirvanix, CloudComplete, Cloud Storage Network, Cloud File System and One Click to the Cloud are trademarks and CloudNAS is a registered trademark of Nirvanix, Inc. #NWP-SCSE-1111a