FLASHARRAY™ ACCESS SECURITY

This brief describes how Pure Storage™ FlashArray systems protect against unauthorized local and remote access

FLASHARRAY ACCESS POINTS

A FlashArray system connects to its environment in four ways:

Storage network
Fibre Channel, iSCSI, or NVMe-oF links between arrays and storage networks or host computers

Replication network
TCP/IP connections between FlashRecover asynchronous replication source and target arrays, and between ActiveCluster synchronously replicating *partner* arrays

Array administration
TCP/IP connections between an array and a GUI or CLI running on a workstation or mobile device, or administrative applications that use the Purity//FA REST interface

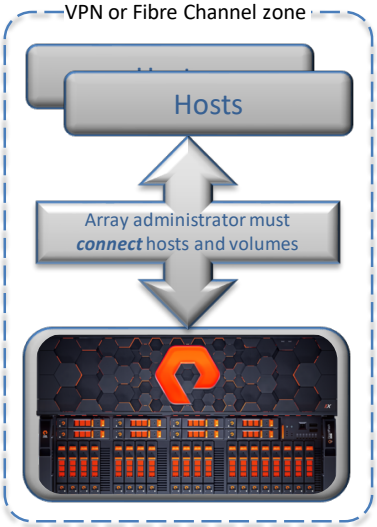
Support
TCP/IP connections for transmitting logs to the Pure1® cloud-based support framework and for conducting RemoteAssist diagnosis and remediation sessions with Pure Storage Support Engineers.

This brief describes how FlashArray protects against threats of misappropriation, alteration, or destruction of stored data on each of these access paths.

SECURING ACCESS TO STORED DATA

FlashArray presents *volumes* to hosts via Fibre Channel or Ethernet (NVMe-oF or iSCSI) storage network fabrics. Many fabrics are entirely internal to the data center and so are physically secure. For routed connections, however, as well as to prevent access by unauthorized hosts, users should configure zones or VLANs to restrict access to data in transit.

Regardless of storage network type, FlashArray administrators must *connect* volumes to hosts, effectively whitelisting them, before arrays will respond to their I/O commands. Internally, FlashArray represents hosts as *host object* data structures—lists of the hosts' storage network addresses. Arrays only respond to commands from storage network addresses associated with hosts that an administrator has connected to the volumes they address.[1]



Data Access Security

Pure Storage Technical Brief TB-160201 describes how FlashArray protects the data at rest in an array from misappropriation.

SECURING COMMUNICATIONS BETWEEN ARRAYS

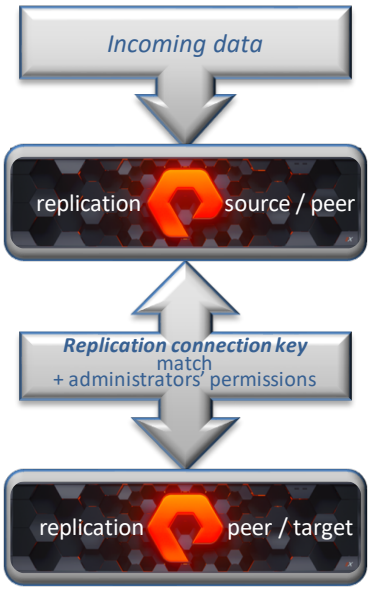
Because the usual reason for replicating data between arrays is disaster protection, replication often takes place over routed connections that pass through firewalls. FlashArray encrypts locally stored data, but does not encrypt replicated data during transit. Where "on the wire" encryption is required, it is performed by network gateways and/or VLANs. Network

1 For iSCSI connections, array administrators may additionally configure *Challenge Handshake Authentication Protocol* (CHAP) to prevent an unauthorized host from impersonating an authorized one.

administrators must permit TCP/IP connections through firewalls for the ports that arrays use to make replication connections and to transfer data.

To minimize the possibility of a remote computer impersonating a replication target or peer array and misappropriating data, pairs of replicating arrays exchange a credential called a *replication connection key* before establishing the replication TCP/IP connections. One array's administrator uses the FlashArray CLI or GUI to generate a replication connection key and communicates it (securely) to the other administrator, who installs it in the partner array. Either administrator can establish a replication connection between arrays with matching keys.

Once replication connections are established, both arrays' administrators must explicitly permit replication to occur. With FlashRecover, for example, source array administrators *enable* replication; target administrators *allow* it. Either administrator can stop replication at any time. These protections help administrators limit exposure to network breaches, and in addition they make it possible to suspend replication temporarily, for example if network load becomes too high or a FlashRecover target array's available storage becomes dangerously low.



Replication Security

SECURING ADMINISTRATIVE ACCESS TO ARRAYS

Administrators interact with arrays using either a command line interface (CLI) accessed from a virtual console such as PuTTY or ssh, a Graphical User Interface (GUI) in a web browser, or a mobile device application. In addition, Purity//FA supports a REST API for software-based administration and VMware's *vStorage APIs for Storage Awareness* (VASA).

CLI access is validated either by a *public/private key* (PPK) pair or an account name and password. GUI access uses account name and password for validation. Arrays may validate passwords themselves, or they may optionally be configured to query an Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) service for validation.

Array administrators generate account-specific API tokens used to validate REST exchanges.

With VASA, vCenter administrators manage FlashArray systems in vSphere environments using interfaces with which they are familiar. FlashArray administrator credentials validate an array's first interaction with vCenter; thereafter, certificates generated and validated by vCenter authenticate interactions.

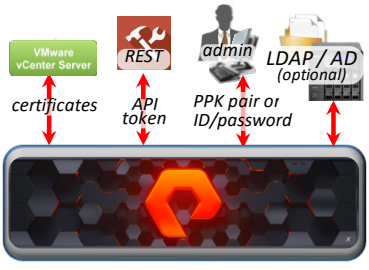
Each FlashArray account is associated with one of three roles:

- **Array:** all administrative actions permitted
- **Storage:** volume-related actions permitted
- **Read-only:** only monitoring actions permitted.

Arrays come with a pre-installed **`pureuser`** account having the array role. The **`pureuser`** account password can be changed, but its role cannot, and it cannot be deleted.

Administrators, REST applications, and vCenter use secure connections between arrays and workstations, mobile devices, and management servers to create, resize, group, copy, and destroy storage volumes, to manage host-volume connections, to schedule snapshots and replications, and to monitor array performance and storage utilization.

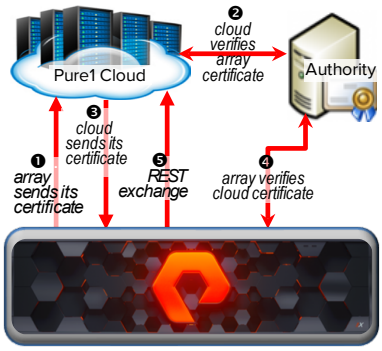
Arrays log all administrative interactions, including successful and unsuccessful logins, *indelibly* in a circular buffer that overwrites the oldest



Administrative Access Security

entries with the newest ones when it fills. Logs are only deleted when a Pure Storage Support Engineer resets an entire array. Administrators can view logs via the GUI or CLI, and can optionally configure arrays to send them to syslog servers.

None of the FlashArray administrative interfaces provides access to stored data. Purity//FA software has no facilities for an administrator to read stored data or to write data to an array's volumes. While an administrative access breach might enable an attacker to masquerade as an array or storage administrator and obliterate data by eradicating volumes, it would not enable data alteration or other misappropriation. Purity//FA provides robust mechanisms for limiting access to arrays to authorized administrators, but it is incumbent on array owners to manage administrator authorizations.



TLS Mutual Authentication

SECURING ACCESS FOR SUPPORT

Except where it is technically infeasible or prohibited by user policy, arrays regularly use a REST API to upload performance, utilization, log, and alert information to Pure1, a feature colloquially called *phonehome*. Pure Storage Support uses phonehome information for diagnosis and remediation, fingerprint analysis and development, and for routine monitoring and statistics collection.

Pure Storage Support Engineers use the *RemoteAssist* (RA) facility to perform hands-on diagnosis and remediation. Array administrators must *enable* RemoteAssist and initiate RA sessions. Sessions are often accompanied by phone calls with the Support Engineer, whose every action is inelibly logged by the array.

Phonehome and RA do not access user data. Nevertheless, their communication paths between array and Pure1 must be secure to avoid exposing tangential information such as volume properties, utilization, I/O activity, storage network addresses, host identities, snapshot and replication schedules, and so forth.

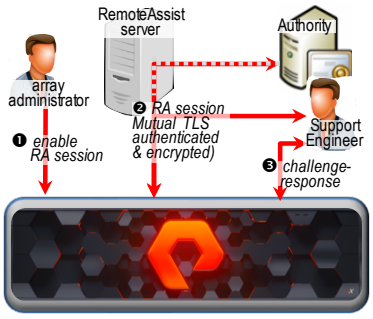
When an array is installed, generates a *public-private key* (PPK) pair and signs and sends its public key securely to a Pure1 database. Pure1 uses the array's public key to verify its identity in subsequent interactions.

The array also creates a generic self-signed digital certificate. When a GUI user attempts to connect to the array through a browser, the array confirms its identity by presenting its certificate for validation. Administrators in the array role can change certificate attributes and import additional certificates from recognized signing authorities. For optimal access security, Pure Storage strongly recommends the latter. Arrays update their digital certificates automatically when necessary, for example shortly prior to expiration.

At time of publication, current releases of Purity//FA software secure phonehome exchanges and RA sessions with TLS Mutual Authentication and HTTPS encryption. With TLS Mutual Authentication, encrypted message exchanges are not susceptible to to the "man in the middle" SSL interception that some organizations use to audit traffic leaving their internal networks. (With earlier versions of Purity//FA that did not use TLS Mutual Authentication, interception was possible.)

SECURING REMOTEASSIST SESSIONS

When an array administrator initiates an RA session, the array and a remote Pure1 server perform TLS Mutual Authentication. The array then generates a one-time password which it sends to the Support Engineer via a secure network path (separate from the path used by the session). The Support Engineer echoes the password to the array, thus verifying his or her authenticity. Communication during the session uses ssh within



RemoteAssist Authentication

an HTTPS encrypted tunnel. As with phonehome exchanges, interactions between Support Engineers and arrays cannot be intercepted. Arrays log every Support Engineer action.

FlashArray administrators control RA sessions. Arrays automatically terminate sessions after 48 hours of inactivity, but an administrator can terminate a session at any time by disabling RemoteAssist with the CLI or GUI. RA sessions enable Support Engineers to view internal array information for diagnosis and to perform certain maintenance operations not available with any of the administrative roles.

SECURING USER ACCESS TO PURE1®

Pure1 Manage (often referred to simply as Pure1) is a is a comprehensive management platform for Pure Storage products. It is a distributed cloud application available to FlashArray owners with current support agreements at no incremental cost. It. With Pure1, array owners' authorized representatives can use artificial intelligence-based models to forecast the storage capacity and I/O performance needs of indvidual workloads, analyze full-stack performance down to the virtual machine level, manage volume group snapshots stored either locally or in a public cloud service, view the utilization, performance history, and alert status of their arrays, and manage support cases through a browser or mobile application.

Pure1 distills information from the logs it receives from arrays; it does not access the arrays directly.[2] The information visible to Pure1 users includes array and host object names, alert and support case status, volume properties, replication schedules and status, historical and projected utilization and performance, and so forth, *for their arrays only*.

When a Pure Storage product is installed, a company representative creates a record of the array's security certificate in a Pure1 private database. Pure1 uses the database to restrict organizations' access to information about their own arrays.

Pure Storage representatives create a *Pure1 administrative user* (Pure1 Admin) accounts for each of their customers. Users with Pure1 Admin accounts can create and delete additional accounts, including Pure1 Admin ones, for their organization. Pure1 supports single sign-on (SSO) access through any recognized identify provider that supports the *Security Assertion Markup Language* (SAML 2.0). For organizations that do not use SSO, Pure Storage uses a recognized credentialing authority[3] to authenticate Pure1 logins. Users create and delete additional Pure1 Admin accounts (e.g., when an employee's role no longer requires Pure1 Admin access) upon customer or partner request.

PURE STORAGE AND PARTNER ACCESS TO PURE1

Pure Storage employees whose job functions require Pure1 data have access to information pertaining to the entire installed base. Pure Storage extends Pure1 access, except for support case information, to its *Authorized Service Providers* (ASPs) automatically. Organizations that acquire their arrays through other partners can create accounts to enable partners to access Pure1 information about their arrays. Partners and ASPs can only access information pertaining to arrays for which they are responsible.

In addition, Pure Storage sales engineers and account executives regularly use Pure1 information for capacity planning and preemptive diagnosis.

Pure1 makes about a month of performance history and a year of storage utilization history available to users. It retains certain information indefinitely for internal use to resolve problems, to develop "fingerprints" of issues for preemptive diagnosis and remediation, and to conduct research leading to product improvements and enhancements.

[2] Pure1 does provide one-click access to arrays' GUI login pages, from which administrators can log in with their credentials and manage their arrays directly.

[3] At the time of publication, Salesforce.com, Inc.

FLASHARRAY AND COMMON CRITERIA

The Common Criteria Recognition Arrangement (CCRA) is an international agreement that defines criteria for specifying and evaluating security in information technology products. Published under the aegis of CCRA, the *Common Criteria for Information Technology Security Evaluation* (commonly known as CC) and related specifications define product profiles, security features, and testing criteria. Each CCRA signatory is represented by a national agency whose brief is IT security. The United States, for example, is represented by the National Information Assurance Partnership (NIAP, https://www.niap-ccevs.org/). These agencies approve security evaluation laboratories,[4] which test IT products and issue certificates of compliance with criteria specific to product classes. Under the CCRA, signatory nations agree in principle to recognize each others' certifications, effectively making CC compliance an international IT product security certification.

Increasingly, organizations are using CC compliance to assure that the equipment in their data centers meets consistent, well-defined standards for securing data and access to it. Some, especially in the public sector, require that all IT products they acquire be CC-certified. Recognizing the importance of CC to its customers, Pure Storage engages independent laboratories certified by NIAP,[5] to evaluate FlashArray hardware and Purity//FA software for compliance to current CC profiles. Evaluations have thus far resulted in certification of most current FlashArray models and Purity//FA software versions against the Common Criteria Network Device Protection Profile, Version 1.1.[6] Certification of newer array models, Purity//FA versions, and CC Profile versions is constantly in progress.

CC COMPLIANCE AND FLASHARRAY DEPLOYMENT

Strict CC compliance requires that certain FlashArray facilities, such as phonehome and RemoteAssist, be restricted or disabled. Thus, although all FA-400 and FlashArray//M arrays that run Purity//FA version 4.7 are certified CC-compliant, a Pure Storage or Qualified Partner representative must configure an array for full compliance when it is installed. After installation with full compliance configured, phonehome and RemoteAssist, can be enabled by an array administrator, but complete relaxation of CC-compliance requires engagement with Pure Storage Support or with a Qualified Partner.

[4] In the United States, laboratories are certified by the NIST National Voluntary Laboratory Accreditation Program.

[5] For example, UL (https://ims.ul.com/common-criteriaiso15408) is one such laboratory.

[6] https://www.niap-ccevs.org/Product/Archived.cfm?par303=Pure%20Storage%2C%20Inc%2E contains a partial list of certified FlashArray models. Certification documents for other models are available from FlashArray Product Management.