Protecting Pure1®

Keeping Fleet-wide Storage Management Secure

Pure1 is the Everpure™ private cloud service used by customers and the company's employees to monitor, manage, and support its products in the field. It is available at no incremental cost to all customers with current Evergreen subscriptions whose products are connected to the Internet. Clients access the service through browsers or a mobile device application.

Pure1 provides:

- Visibility to performance, utilization, and alert information for a customer's entire "fleet" of Everpure systems from a single point.
- AI-based workload simulation for evaluating "what if?" system configuration alternatives.
- "Full-stack" analytics that depict end-to-end I/O performance in VMware environments.
- Secure channels for downloading Purity software upgrades and patches and for conducting hands-on support sessions with Everpure Technical Services engineers.

This brief describes Pure1's capabilities and its benefits to users, summarizes its structure, and shows how it secures access to its facilities by systems and by users.

THE PURE1 VIRTUAL PRIVATE CLOUD (VPC)

Pure1 is Everpure's cloud-based monitoring and management service that enables customers with systems deployed across the world to view up-to-date information about their entire "fleets" (Figure 1), to "drill down" to obtain individual system details, and to perform *self-service upgrades* (SSUs) to Purity software. The applications that comprise Pure1 run in a *virtual private cloud* (VPC) within a larger *Everpure infrastructure cloud* that also hosts several of the company's applications.

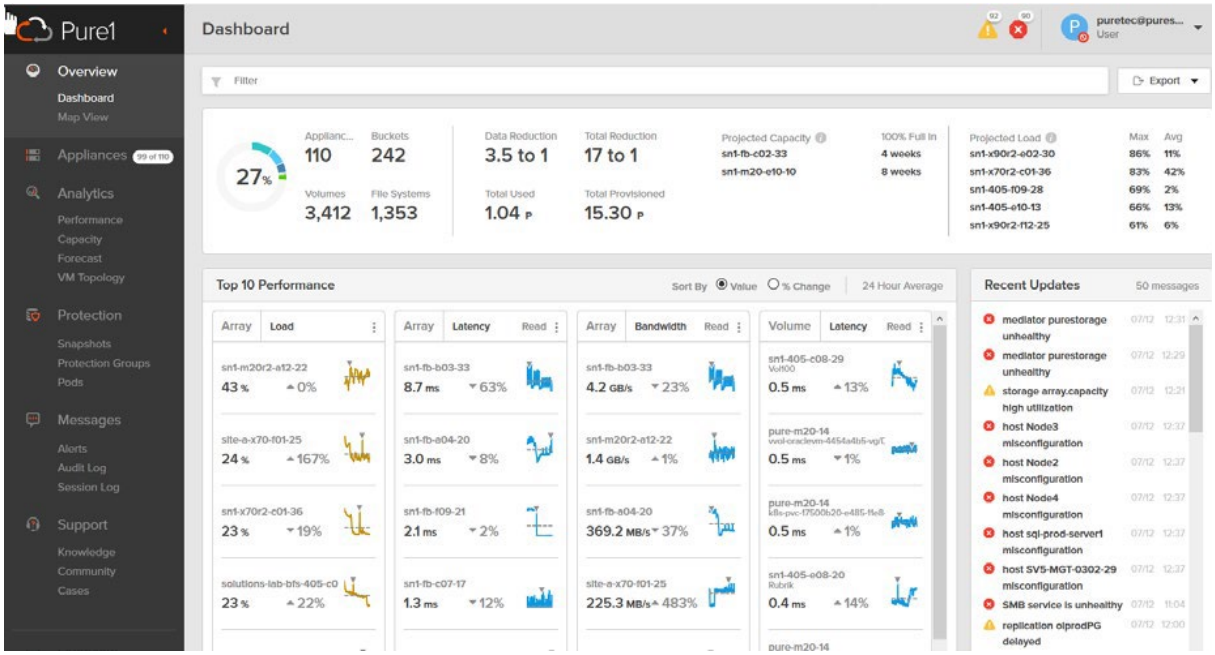

Figure 1: A Sample Pure1 Dashboard

MAJOR COMPONENTS

The Pure1 VPC receives, analyzes, and stores utilization, performance, and "health" information uploaded by deployed systems. It initiates support tickets as necessary and provides secure channels for downloading software updates and conducting hands-on support sessions. The VPC consists of three main components:

PURE1 MANAGE (OFTEN REFERRED TO SIMPLY AS 'PURE1')

A suite of applications that use information from deployed systems to display performance, utilization, and status history for an enterprise's Everpure systems. Users of Pure1 Manage can perform SSUs, initiate and track support tickets, and use AI-based tools to estimate the likely impact of alternative scenarios such as adding or relocating I/O workloads.

SUPPORT INFRASTRUCTURE

Everpure Technical Services' primary tool for:

- Identifying potential problems from uploaded system logs and initiating remediation.[1]
- Identifying system configurations that match *fingerprints* of known product and environmental issues to identify and avert potential problems.
- Providing secure bidirectional communication between the company's support engineers and customer systems that require hands-on service.

PURE EDGE SERVICE (PES)

A secure communication path between VPC applications and deployed systems. At publication time, PES is used only for downloading software for Purity SSUs.

THE VALUE OF PURE1

Pure1 enhances the supportability of Everpure's systems.

FOR CUSTOMERS

Pure1 simplifies customers management of their storage by:

- Providing a single point for monitoring and managing their entire "fleets" of Everpure systems, estimating future storage requirements, and assessing the impact of potential operational changes (e.g., workload relocations).
- Eliminating the need for on-premises storage management servers.
- Assisting Everpure *Technical Services engineers* (TSEs) with problem diagnosis, fingerprint development, and analytics and planning algorithm refinement.
- Providing secure communication paths for hands-on support by TSEs and for self-service Purity software upgrades.

FOR THE COMPANY

Pure1 databases are a constantly updated repository of current and historical information about the company's entire installed base of systems. The databases speed issue identification and resolution and make preemptive support possible. Continuous feedback from deployed systems helps TSEs create fingerprints of potential issues that are common to multiple systems so they can be remediated before becoming problematic and helps identify needs for additional product capabilities.

[1] Historically, Pure1 has initiated over half of all support tickets autonomously, usually before customers become aware of issues.

THE PURE1 VPC STRUCTURE

Figure 2 illustrates the major components of the Pure1 VPC and their interactions with deployed systems, users of Pure1 Manage, and Everpure Technical Services engineers.

The applications represented in the figure are implemented as auto-scaling clusters whose instances start and stop based on client load. Load balancers (not shown) regulate client access and spread load across active application instances. The applications illustrated are:

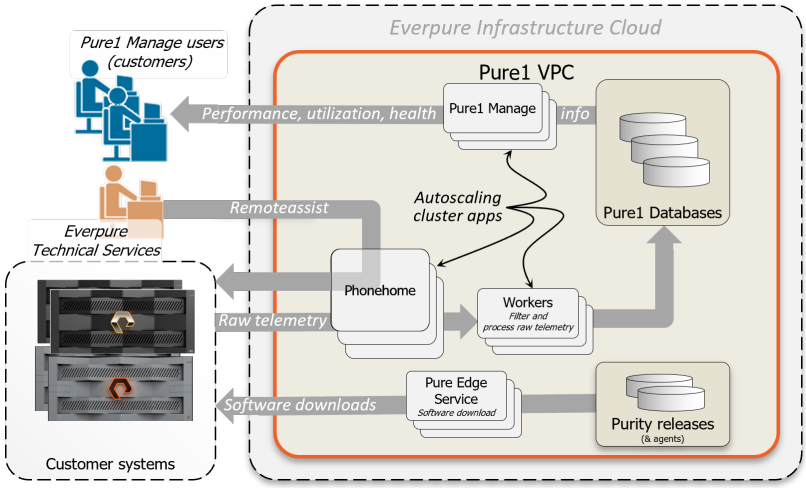

Figure 2: The Pure1 VPC Structure

PHONEHOME

Secure connections used to receive periodic utilization, performance, and "health," reports from deployed systems and by Everpure TSEs to interact directly with customers' systems during *RemoteAssist* (RA) sessions.

WORKERS

Filter and process information received from deployed systems. Workers store raw information in Pure1 databases, create extracts for Pure1 Manage, format system logs for Everpure Technical Services, analyze alerts to identify issues, and initiate support tickets.

PURE1 MANAGE

Provides monitoring, analytics, and support case management for interactive users and customers' data center automation frameworks.

PURE EDGE SERVICE (PES)

Provides a secure bidirectional communication path between systems and the VPC. At publication time, PES is used for downloading and installing self-service Purity software upgrades. Its capabilities may support additional applications in the future. Technical Brief TB-211001 describes the Pure Edge Service in more detail.

Keeping PURE1 Secure

Pure1 VPC applications access customers' systems for administration and support. They do not enable access to stored data. Nevertheless, communication between systems and the VPC must be secure and access to Pure1 Manage and SSU must be restricted to authorized actors. The remainder of this brief describes how Pure1 information flows are protected against intrusion.

SYSTEM COMMUNICATIONS WITH PURE1

Deployed systems transmit status information to the VPC every few seconds over a secure channel called *Phonehome*. Systems and VPC authenticate each other using mutual TLSv1.3 prior to transmitting information.

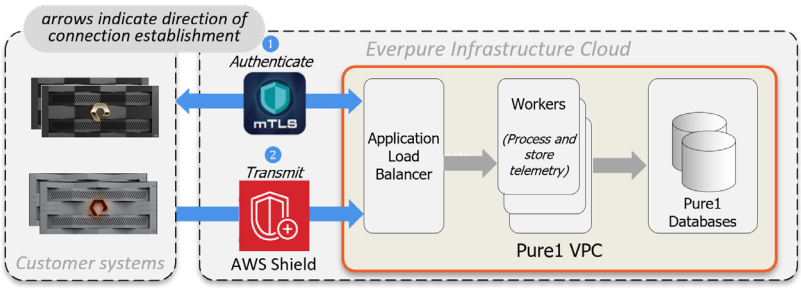

Figure 3: Securing the Phonehome Channel

At publication time, the Amazon Web Services *AWS Shield* service protects Phonehome against *distributed denial of service* (DDoS) attacks. Reporting is unidirectional (systems → Pure1). Systems encrypt all transmissions, and Everpure monitors the service for suspicious activity.

INFORMATION TRANSMITTED VIA PHONEHOME

Systems upload configuration (hostnames, network addresses, etc.), performance, storage utilization, event log, and alert information to the VPC in the form of:

FREQUENT DIAGNOSTICS (EVERY 30 SECONDS)

Configuration, hardware and software status, performance, utilization, and alerts.[2]

LOGS (HOURLY)

Logs of administrator actions and other significant events (e.g., free space below 20%).

When a system is installed, Everpure issues a unique certificate to it. Systems use these to authenticate to the VPC. The company automatically refreshes certificates at least annually. Users whose policies prohibit outgoing network connections must whitelist the Pure1 DNS name (pure1.purestorge.com) or IP addresses in their firewalls to enable Phonehome.

[2] Customers with active support agreements can view the Frequent Diagnostic message content list at https://support.purestorage.com/FlashArray/FlashArray_Security/FlashArray_Security_Reference/Phone_Home_Contents.

ACCESS TO PURE1 MANAGE

Pure1 makes historical performance, storage utilization, and information used for VMware analytics available to Pure1 Manage users for a limited period.[3] Pure1 Manage derives the information it presents to users from Phonehome uploads, not directly from the systems.

PURE1 CLIENT ACCOUNTS

Pure1 limits user access to resources owned or controlled by a user's *company* (customer). Its authentication database contains at least two objects for every Everpure customer of record:

- A *company* object that identifies the customer.
- A *Pure1 client account* object associated with the company object.

Customers can create additional Pure1 client accounts to enable access by more users.

Each Pure1 client account has either *viewer only access* to information or *full control* of the company's Pure1 client accounts and self-service upgrades (SSUs). Clients with full control can create, manage, and delete Pure1 client accounts within their companies.

During system installation, Pure1 creates a *system* database object associated with the customer that owns or controls the system. The system and company objects determine a Pure1 client's access to system information and ability to perform SSUs.

With customers acquiring more and more Everpure systems, a more granular approach to Pure1 client access is necessary. For example, a customer's IT might be organized by geography, product line, business function, or other criteria. Within an organization, different teams might manage subsets of its IT resources.

For such customers, Pure1 implements the client access hierarchy illustrated in Figure 4. Customers with multiple IT teams that manage separate resources can use Pure1's *Identity and Access Manager* (IAM) to create and manage subordinate *organization* objects as needed. In turn, an organization may contain multiple *resource group* objects, each including one or more *system* objects.

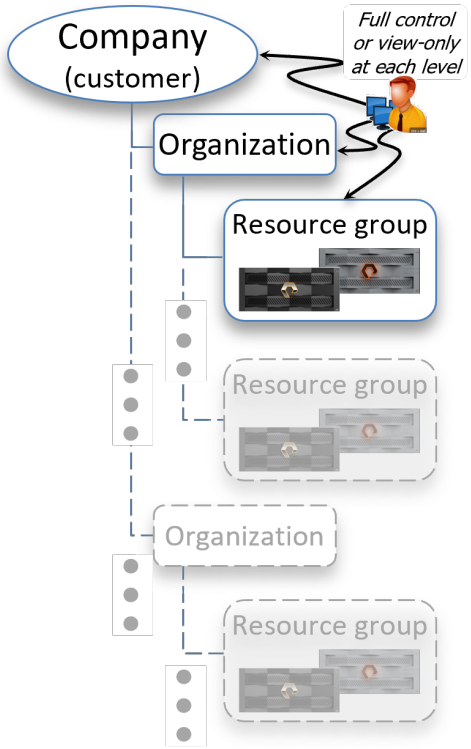

Figure 4: Pure1 Access Hierarchy

[3] At publication time, Pure1 makes about 35 days of performance history, 13 months of storage utilization history, and 7 days of VM Analytics data available to clients. A premium *VM Analytics Pro* option retains VM Analytics data for up to three years. Everpure retains some information indefinitely for internal problem resolution, fingerprint development, and other research.

With this structure, each Pure1 client account has either a company, organization, or resource group *access scope* of viewing or full control. For example, an account with organization scope can view or update only the systems in its organization's resource groups.

For customers with flat IT organizations or only a few systems, the hierarchy shown in Figure 4 effectively collapses to a company object with one organization containing one resource group. As a customer's IT becomes more complex, a Pure1 full access client account with company scope can use IAM to expand the Pure1 access hierarchy.

User Authentication

During installation of a customer's first Everpure product, Pure1 registers its *identity provider* (IdP). It uses the identity provider to authenticate subsequent Pure1 client account logins. For customers who do not use an IdP, Everpure maintains a salesforce.com account for use in Pure1 client authentication (Figure 5).

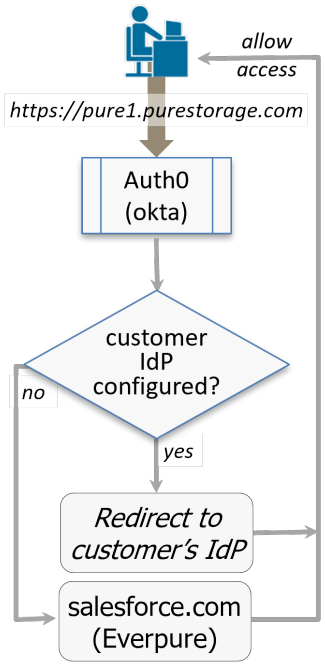

Figure 5: Pure1 Manage Authentication

Multi-factor Authentication

Pure1 requires a type of *multi-factor authentication* (MFA) for operations that alter system states.[4] To perform such operations, a user requests that Pure1 temporarily "step up" account access. Pure1 generates a time-based random code and requests that the mobile device registered in the user's profile[5] generate a corresponding code. The user enters the code from the device; Pure1 compares it to the code it generated and only allows the operation if the two agree.

SafeMode™

SafeMode prevents snapshot deletion and schedule changes. In an emergency (e.g. low acailable space), changes can be made by an Everpure TSE in a RemoteAssist session. Such sessions must be requested by pre-designated customer representatives, and requests must be verified by at least one additional pre-designated customer representative.

Pure1 uses the step-up technique described above to validate SafeMode requests by sending requests to all designated customer representatives. Two or more correct responses are required to create a support case requesting a RemotAassist session in which a TSE performs the requested operations. Multi-party verification minimizes the opportunity for a rogue customer employee or other malicious actor to perform unauthorized operations on stored data.

[4] At publication time, Purity Self-Service Ugrade is the only application that alters system state.
[5] Everpure recommends registering mobile devices in Pure1 account profiles when they are created.

Partner Access

Everpure's *Authorized Service Providers* (ASPs) have Pure1 access with company scope for their customers' systems. Customers of other distributors and resellers can create Pure1 client accounts to provide Pure1 access to their systems for service technicians. Everpure's partner management and legal organizations vet all ASPs, distributors, and resellers, and only allow Pure1 access by entities named on sales and service contracts.

Everpure Employee Access

Everpure's company-wide identity provider, okta.com, controls employee access to Pure1. Employees whose job functions require access, including account executives and sales engineers, are authorized to view Pure1 Manage information for their customers' systems.

SECURING ACCESS TO PURE1 MANAGE

Pure1 Manage executes requests from customers' storage administrators and data center automation applications. At publication time, it uses AWS Shield to detect and prevent DDoS attacks from overwhelming the application. In addition, an *AWS Web Application Firewall* (WAF) configured by Everpure ensures that only valid requests reach the application. Finally, validated requests are routed through a reverse proxy service that provides an additional layer of *defense in depth*.

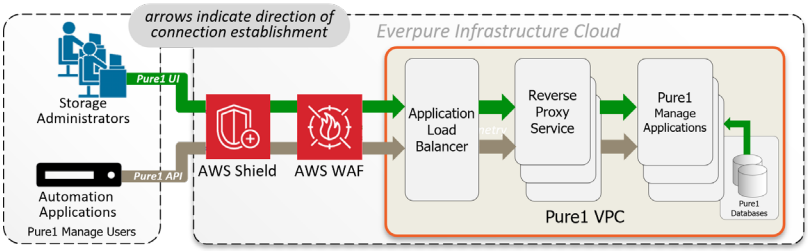

Figure 6: Securing Pure1 Manage Sessions

SECURITY FOR REMOTEASSIST

RemoteAssist sessions provide Everpure TSEs with a level of access to customer systems that enables diagnosis, remediation, software installation, and other assistance. Customers control the sessions. Before a TSE can access a system, a customer representative must enable RemoteAssist on it. The representative can terminate a session at any time by disabling RemoteAssist. Sessions terminate automatically after 48 hours.

Identifying Systems Uniquely

Each Everpure system ships with a pre-installed security certificate that is used to establish a temporary trust relationship between its built-in **`puresupport`** account and the company's *Secure Shell Certificate Authority* (SSH CA). During installation, a system registers with the CA and obtains a new certificate with its unique *appliance-id* as a principal. Thereafter, when its appliance-id appears as a SSH certificate principal, the *Pure1 Support Infrastructure* grants the

system's **`puresupport`** account SSH access. This prevents inadvertent use of a system's certificate to access a different system.

Securing Access to RemoteAssist Sessions

All RemoteAssist communication occurs via a Phonehome channel and the Pure1 VPC. Figure 7 illustrates the steps in initiating and conducting a session:

1. An authorized customer representative enables RemoteAssist on the *target system* (system needing service).
2. The target system and Pure1 use mutual TLSv1.3 to authenticate each other.
3. A TSE connects to a *RemoteAssist Client* in the VPC, either from an Everpure facility or via the company VPN using Everpure's identity provider to authenticate to the VPC. The TSE obtains a SSH certificate that grants access to the required VPC features.
4. RemoteAssist Clients route TSE communications through a firewall to a *RemoteAssist Service Bastion* in a separate account and from there through another firewall to the VPC's RemoteAssist Service. The Bastion isolates the TSE from direct contact with the RemoteAssist Service and the target system.
5. The TSE conducts the session by communicating with the target system via the path described above.

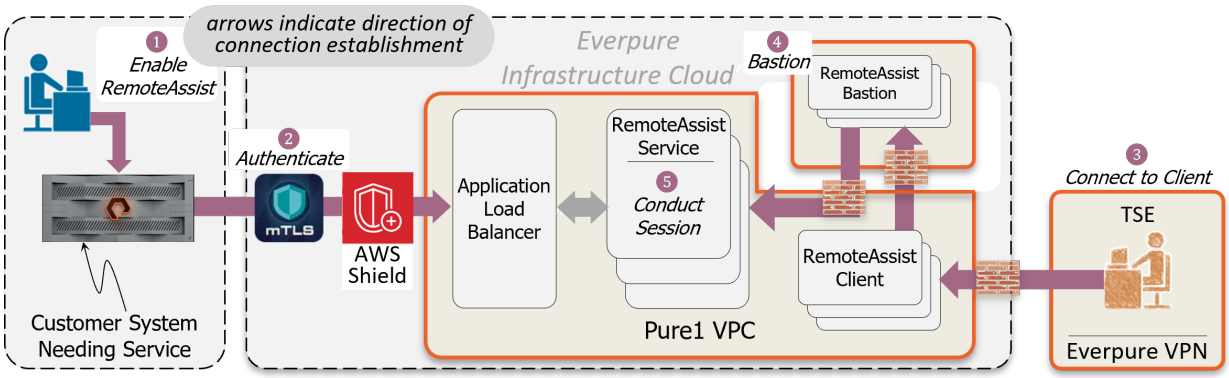

Figure 7: Securing Remote Access Sessions

TSE Access to the Pure1 Support Infrastructure

Once connected to the VPC, TSEs use its SSH CA to gain access to the Pure1 Support Infrastructure. The CA issues ephemeral SSH certificates with authenticated engineers as principals to enable login to the Support Infrastructure within a few minutes of issue.

The SSH certificate does not enable access to a RemoteAssist session. To join a session, the TSE requests the CA to add the target system's appliance-id to the certificate's principals.[6] With

[6] ASP support engineer access is limited to the ASP's end customers' systems.

the augmented certificate, the TSE must log in to the target system's `puresupport` account within two minutes. Once logged in, a TSE can conduct sessions of up to 48 hours' duration.

The Support Infrastructure logs all RemoteAssist session activity. Everpure makes RemoteAssist session logs for their systems available to customers on request.

MAINTAINING THE PURE1 CLOUD INFRASTRUCTURE

SECURING ACCESS TO PURE1 CLOUD RESOURCES

Pure1 VPC servers and databases are managed centrally through a *Pure1 Support Dashboard*. Access to the Dashboard is limited to authorized individuals and is only possible from Everpure's internal network. The company's okta identity management system authenticates employees authorized to access the Dashboard. The identity management system is linked to the company's human resources system, so Dashboard access is automatically revoked if required by employee role and status changes.

TSEs and development engineers are the only users of the detailed event histories in Pure1 databases. They use a *playback GUI* that displays sequences of administrative actions and system responses to assist with diagnosis. Developers use automated systems to update cloud software and maintain cloud databases.

SECURING THE PURE1 CLOUD AGAINST INTRUSION

Pure1 implements the security guidelines and best practices recommended by its cloud provider as well as additional monitoring tools for identifying suspicious activity and resource abuse. The tools flag potential issues, both in security (e.g., access rule violations), performance (e.g., approaching service limits), and availability (e.g., application crash) for remediation, which usually occurs before issues impact service to clients.

Everpure's Corporate Security Team monitors recognized external sources of computer security alerts including the *United States Computer Emergency Readiness Team* (US-CERT) for potential threats, exploits, and vulnerabilities and prioritizes preemptive remediation based on severity. All security remediation tasks are tracked by the company's support ticketing system to maintain constant awareness of the status of security issues.

PURE1 DEVELOPMENT AND MAINTENANCE SECURITY

DESIGN REVIEW AND PENETRATION TESTING

At least annually, Everpure engages recognized third-party firms to perform independent design reviews and penetration tests of the Pure1 VPC. The company prioritizes any critical or high-risk vulnerabilities discovered for remediation, based on likelihood of occurrence and potential technical and financial impact. If critical issues (outages or security incidents) occur, its Security and Site Reliability Engineering (SRE) Teams conduct after-analyses to identify root causes to prevent future occurrences of similar issues and/or mitigate their impact.

The Pure1 Enhancement and Change Control Process

The Corporate Security Team uses the company's support ticketing system to track changes and feature enhancements to Pure1 Cloud software. The process for introducing a change is:

1. The Security Team reviews developer proposals for software enhancement to eliminate design flaws, potential security issues, and unnecessary complexity.
2. Developers create the proposed software (amended if necessary) and submit the code for peer review. Reviewers verify that the design fulfills the proposal.
3. Developers implement and test the software and stage the result in an internal cloud test bed.
4. The SRE team verifies the staged implementation and agrees with the developers on a communication, deployment, and maintenance plan.
5. Developers put the verified software into production, audited either by other developers or by SRE delegates.

Appendix: Security Posture at a Glance

USING PURE1 TO EVALUATE ORGANIZATIONAL DATA SECURITY

The **Assessment** view of the Pure1 Dashboard (example in Figure 8) provides an overview of a customer's Everpure systems' data protection, sustainability, and disaster recovery postures at the organization[7] level.

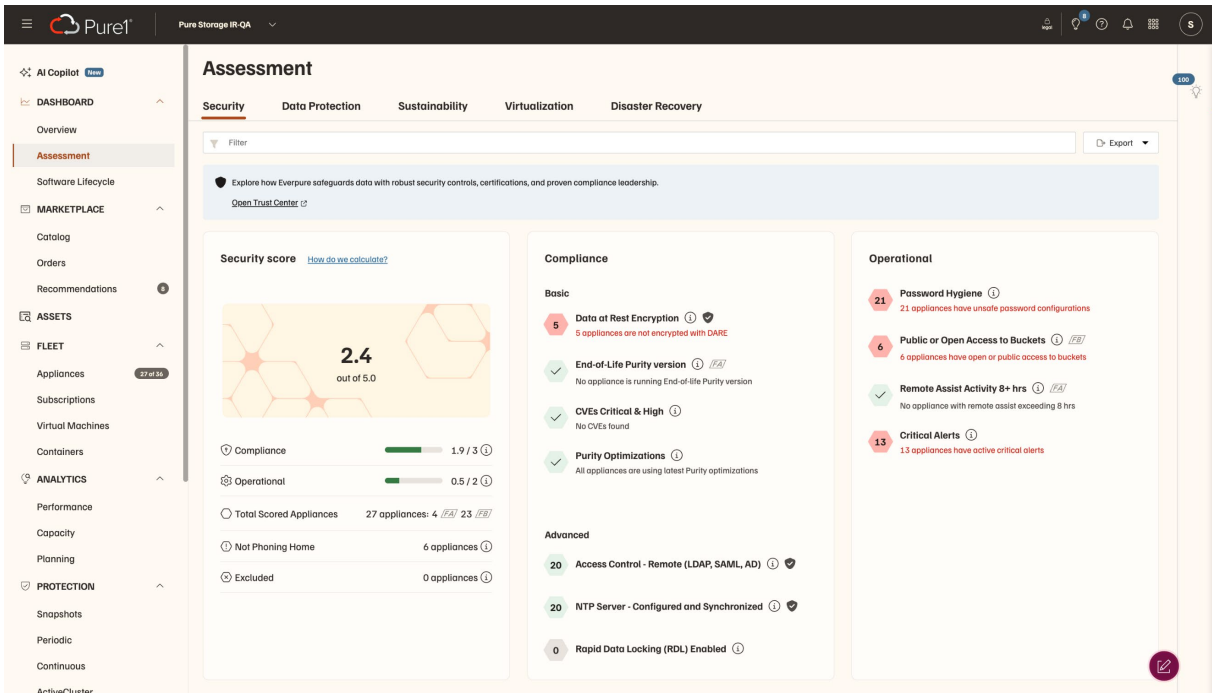

Figure 8: The Pure1 Security Assessment

In the example **Security** pane shown, Pure1 examines all systems that belong to the selected organization for compliance with Purity management best practices and identifies potential security weaknesses at the operational level. The **Security** pane displays an overview of the organization's security status. Users can "drill down" to discover which systems are flagged for potential vulnerabilities and take steps to correct them.

[7] As defined on page 5