ENTERPRISE SECURITY ADMINISTRATOR

Unified, consistent security management across all data assets

PROTEGRITY

Data Sheet

As data continues to amass exponentially in the enterprise, so too does the risk generated by unsecured sensitive data. This data can often be found (or hidden) within multiple heterogeneous systems, applications, and platforms inside and outside of the enterprise, making consistent data security and visibility extremely challenging.

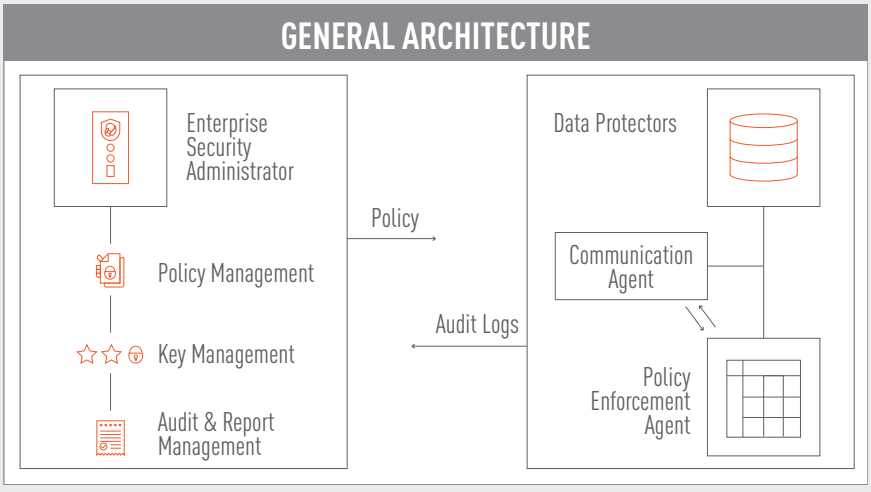
Protegrity's Enterprise Security Administrator (ESA) is an intuitive, comprehensive management interface for centralized, visual administration of data security policies, key management, auditing and reporting of sensitive data assets across the enterprise. Delivered as a soft appliance and hardened for high security, ESA comes equipped with built-in backup and restore functions, granular access controls and separation of duties.

Key Benefits

- Improve security, governance and visibility for all sensitive data across the enterprise from a single interface
- Centralized policy and key management, auditing and reporting
- Monitor all services and activities on sensitive data in a single pane of glass
- Utilize advanced access controls and security features, including separation of duties
- Dependable as a highly resilient platform with built-in backup and restore

Enterprise-Wide Platform Support

ESA makes it easy to manage the security of various systems across the enterprise from a single, centralized console. By integrating with **Protegity Data Protectors** located at various endpoints, ESA enforces consistent, efficient security enterprise-wide, and unifies all auditing and reporting into a single interface. Protectors can seamlessly secure big data, databases, cloud applications, file servers, application and more.



Visual Administration & Management

ESA allows security administrators to manage and monitor servers, services and key system metrics, like CPU, memory, logs and disk usage, in a single pane of glass. Users can also create, schedule and manage tasks, backup or visually restore, with a pre-defined frequency or time period, and receive real-time notifications on the dashboard, or email/HTTP alerts, based on the rules set.

Unified Policy, Governance, and Key Management

ESA provides the ability to centrally set data security policy (who/what/where/how) and deploy to Protegrity Protectors located at various endpoints in the enterprise. Policies enable different users to access only the data they are entitled to, based on the roles defined. ESA offers federated data governance to allow enterprise wide data security posture that is consistent globally, while also being able to accommodate local/regional laws and privacy policies (like data residency.)

ESA also offers integrated, comprehensive enterprise key management (EKM) capabilities. Keys can be managed from a single, centralized repository for various protection points across the enterprise. ESA offers key state management including key-encryption key (KEK) handling and rotation. Protegrity EKM also features the flexibility to integrate with external Hardware Security Module (HSM) systems and supports the NIST 800-57 standard.

MANAGE DATA SECURITY POLICY

Aspect	Definition
What	Sensitive data to be protected
How	Method(s) of data protection used
Who	Users that are authorized to access sensitive data
Where	Systems/applications in which policy is enforced

Built-in Access Controls with Flexible External Integration

Security administrators can manage users and roles inside ESA with a built-in LDAP directory service and integrate with external LDAP or Active Directory services. Advanced security is provided in the form of a two-factor authentication, where users have to take an additional step to authenticate, using standard mobile devices, such as Android or iPhone.

Separation of Duties (SoD)

ESA enables organizations to prevent unauthorized technologists, such as DBAs, programmers, or system engineers from accessing sensitive data in the clear by segregating security duties from systems administration with the data security policy. Security administrators can also be prevented from viewing sensitive data as a part of SoD objectives.

PROTEGRITY

For over 15 years, Protegrity has set the standard in precision data protection, helping enterprises secure and use a perpetually growing store of sensitive data. Through granular protection and intelligent role-based empowerment, Protegrity helps companies focus on growth, development and optimization. By securing their internal and customer data, companies can embrace new ways to share while remaining compliant.

Protegrity USA, Inc.
(Global Headquarters)
1165 E Wilmington Avenue
Suite 200
Salt Lake City, Utah 84106
1.203.326.7200
1.650.431.7000

Protegrity (Europe)
1 St Katherine's Way
London, E1W 1UN
+44 1494 857762

FOR MORE INFORMATION, EMAIL INFO@PROTEGRITY.COM