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 Enterprise Security Administrator (ESA) is an intuitive, comprehensive 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
- Centralize 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 with pre-configured high-availability, and 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, central command. By integrating with Protegrity 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, applications 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 & Key Management

At the heart of ESA is the ability to centrally set data security policy (who/what/when/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 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. Protegrity EKM also features the flexibility to integrate with external Hardware Security Module (HSM) systems.

### Manage Data Security Policy

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHAT</td>
<td>Sensitive data to be protected</td>
</tr>
<tr>
<td>HOW</td>
<td>Method(s) of data protection used</td>
</tr>
<tr>
<td>WHO</td>
<td>Users that are authorized to access sensitive data</td>
</tr>
<tr>
<td>WHEN</td>
<td>Time(s)/day(s) when data can be accessed</td>
</tr>
<tr>
<td>WHERE</td>
<td>Systems/applications in which policy is enforced</td>
</tr>
</tbody>
</table>

Centralized Auditing & Reporting

Security teams can capture and report on event logs from Protectors throughout the enterprise in a single, centralized platform. They can also use pre-defined or customized reports with advanced filtering options. Reports can be accessed in a single view in tables, charts, or other formats, saved in various formats such as PDF, CSV, or Docx, and sent automatically to various departments for compliance needs.

Built-in Access Controls with Flexible External Integration

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

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 part of SoD objectives.