Work from home Data Security

(the new normal)

Now that the Covid-19 virus has forced company employees to work remotely, it's more important than ever to make sure your data security monitoring practices are effective. Office and home security measures are much different, and hackers are not standing down during this pandemic. IBM has several products to help, IBM Guardium Data Protection can help spot hackers and Guardium Data Encryption will encrypt your files to protect them from theft.

Guardium Data Protection

IBM Guardium Data Protection not only provides data discovery, classification and activity monitoring, but it also contains data driven cognitive analytics to discover unusual behavior and identify risky users use of sensitive data. It protects against unauthorized data access by learning regular user access patterns and can provide real-time alerts on suspicious activities.

Guardium Analytics uses machine learning algorithms and outlier mining to looks for patterns and behaviors that deviate from the norm based on factors such as time of day, client program and client/ destination IPs, and may suggest an anomaly or risk. These identified anomalies or risks are placed into either:

- **Active Threats Analytics to identify common attack vectors**
- **User risks via Risk Spotter**

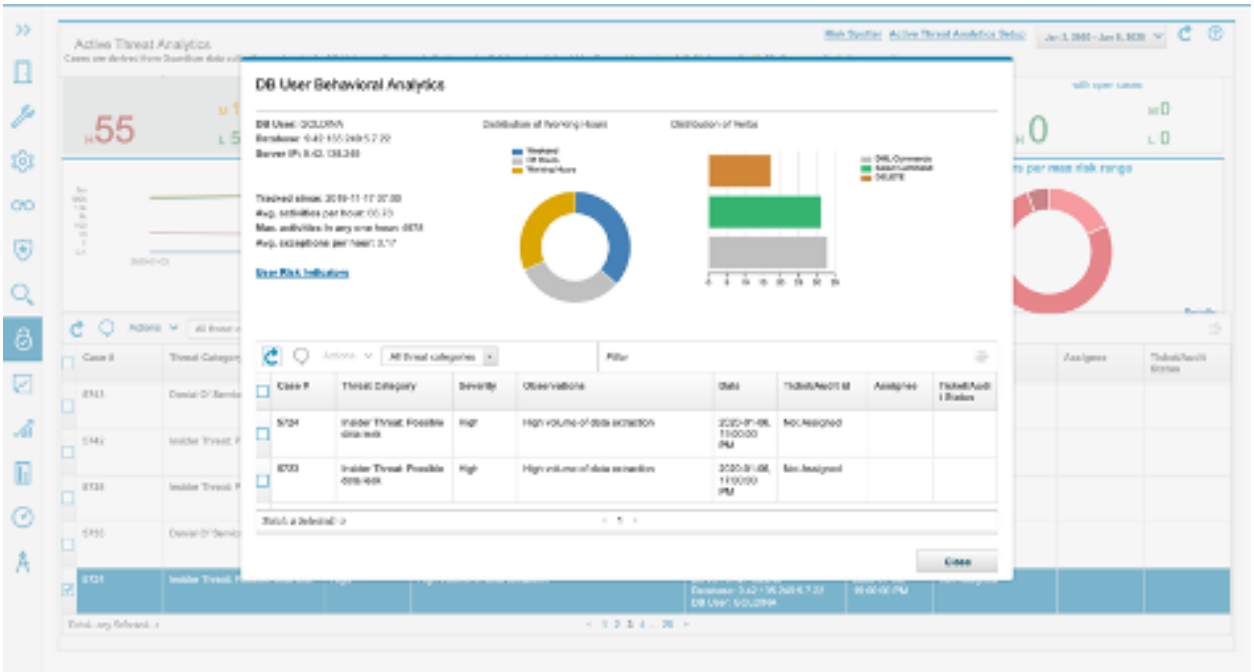
Smarter Data Security

Active Threats Analytics vectors:

- **Insider threat: data leak**
- **Account Takeover**
- **Data Tampering**
- **Denial of Service**
- **Massive grants**
- **Schema tampering**
- **Anomaly - user behaviors**
- **SQL Injection**
- **Malicious Stored Procedure**
- **SQL Injection: Tautology**
- **SQL Injection: Side channel**

The Active Threat Analytics screen below displays events by source, severity and category.

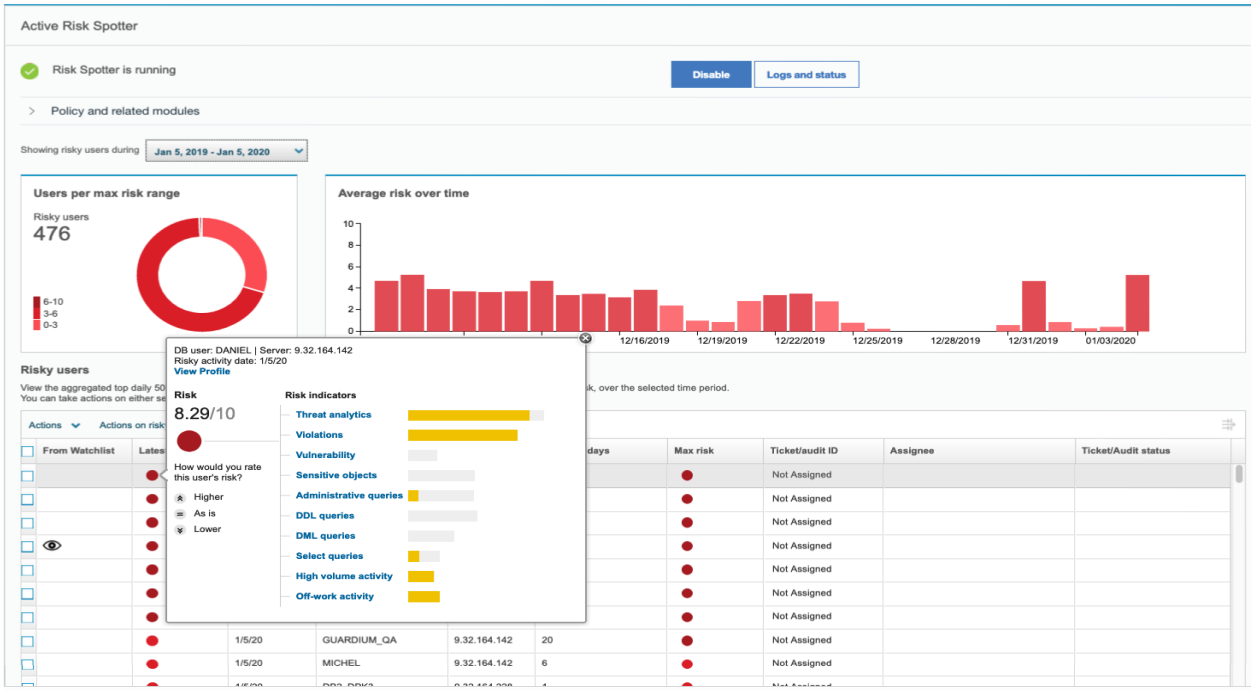
Further drill down provides more details about the incident:



Risk Spotter Indicators

- **Threat Analytics - Identified high and medium potential risks**
- **Violations - number of high and medium severity violations related to the DB user**
- **Vulnerability - number of failed vulnerability assessments for a user**
- **Sensitive objects - number of queries on sensitive data**
- **Administrative queries - relative number of administrative queries**
- **DDL queries - relative amount of DDL queries**
- **DML queries - relative amount of DML queries**
- **Select queries - relative number of select queries**
- **High volume activity - DB Users that have high volume activity**
- **Off-work activity - Activity related to the DB user that occurred in non-work hours**

Risk Spotter helps you identify users and provides the detail information on how the risk score was determined.



Guardium Data Encryption

IBM Guardium Data Encryption (GDE) provides encryption capabilities to help protect file and database data from misuse. In addition to file and database encryption, GDE also supports separation of duties, so that administrators do not have free access to sensitive data. Encrypting file and database data helps organizations meet government and industry compliance regulations (including PCI, GDPR, etc.).

IBM Guardium Data Encryption not only provides transparency but also minimizes performance impacts by only encrypting the contents of a file, not the file system metadata. By leaving the file system metadata in the clear, GDE provides transparency to access requests generated by application and database solutions which rely on the metadata for the location of storage blocks that comprise a file, as well as other critical file attributes. This offering performs encryption and decryption operations with minimal performance impact and high scalability for heterogeneous environments.

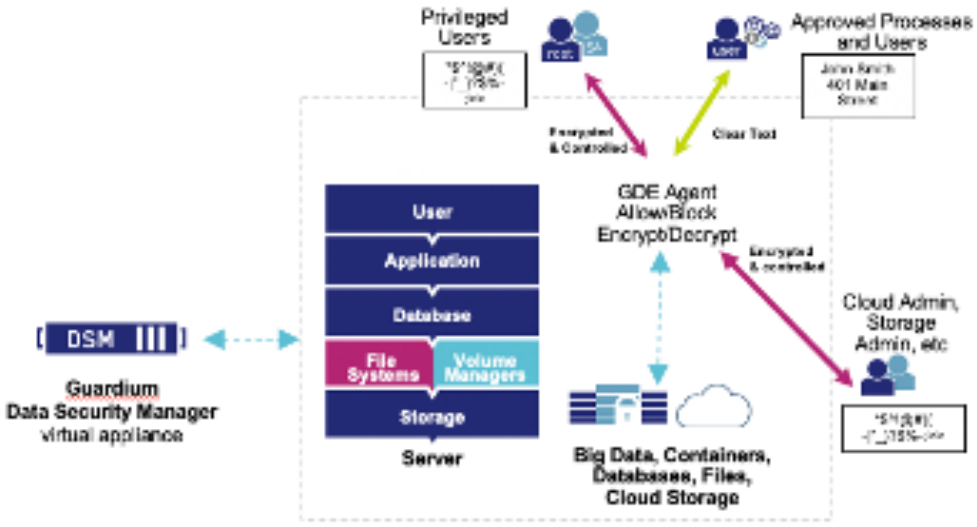
IBM Guardium Data Encryption offers a secure solution for protecting structured and unstructured data through the enforcement of policy-based encryption and centralized encryption key management that enables organizations to keep data private and compliant.

GDE Transparently protects file system, volume data-at-rest

- **No changes to applications or workflows required**
- **Encryption and Key Management – Lock down data**
- **Fine-grained access controls – Only decrypt data for authorized users and processes including system, Active Directory/LDAP, container (OpenShift and Docker) and Hadoop users**
- **Detailed data access audit logs integrate easily with SIEM systems to detect attacks in process**

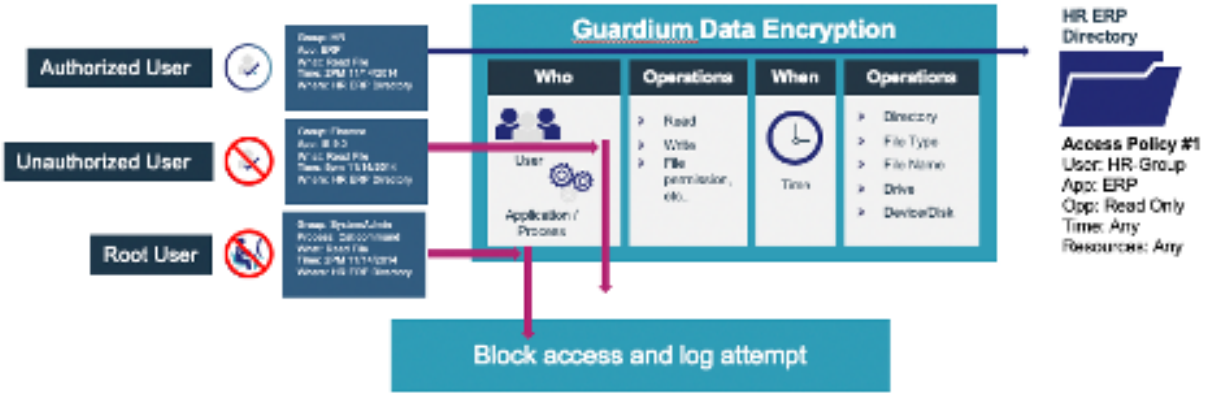
Smarter Data Security

Guardium Data Encryption



Guardium Data Encryption - Granular Access Controls

Process and user aware file access policies



File access polices can be very granular. User access can be controlled by application, allowed operations, time and the file or resource they attempt to access.

Supports controls for users and groups from the System level as well as LDAP/AD, Hadoop and Container environments – Including Privileged users

The IBM Guardium portfolio provides all the building blocks you need for a vigilant enterprise data security solution. If you have any questions about either IBM Guardium Data Protection or Guardium Data Encryption, please contact IBM.