SECURITY NIGHTMARES:
Six Steps to Address Your Worst Security Fears

LAYER UP The best defense involves applying multiple layers of security defense mechanisms. If a single control point is compromised or fails, business-critical data will still be protected.

1 Vulnerability Management

Like an impervious bunker, the first step is to harden your servers (data warehouse or any enterprise environment) against known vulnerabilities so attackers can't break in.

2 Secure Authentication

Most breaches start with credential theft, which is why it's critical to require more than a username and password. Multi-factor authentication ensures only users who should be in the system are.

3 Strong Access Rights Control (RBAC, RLS, CLS)

What can users do on your system? Role-based access control and filtering to create row or column level restrictions means individual users can't explore where they don't have access.

4 Data Protection

Masking, hashing, encryption, and tokenization are ways that apply security directly to sensitive data itself so it's protected at rest at all times and rarely, if ever, unprotected.

5 Audit Logging, Monitoring and Alerting

What are users really doing on your system? Monitor application and database access and usage for continuous visibility, timely alerts, and reporting to detect the good from the bad activity as it occurs.

6 Advanced Threat Detection

An intrusion can happen in milliseconds, but the real damage occurs after hackers extend their foothold. If someone attacks, you have a fighting chance to learn about it before they can steal high-value data.

Don't let data security give you nightmares. **Learn more.**

TERADATA.