SOLUTION BRIEF

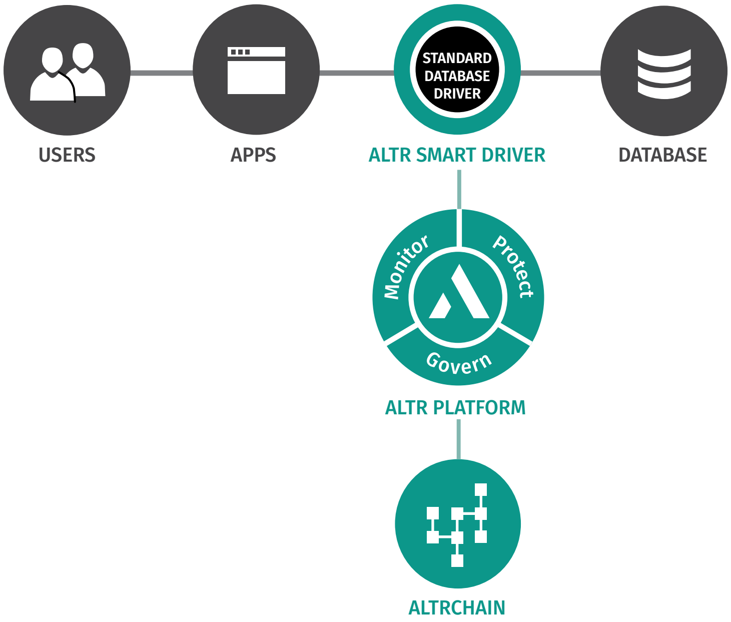
MANAGE AND PROTECT YOUR ENTERPRISE DATA WAREHOUSE WITH ALTR

ALTR Provides Next-Generation Data Monitoring, Governance, and Protection to Address Today's Security, Privacy, and Compliance Concerns

DATA GOVERNANCE

Problem:

Granular data governance through popular data visualization tools (e.g. Power BI, Qlik, and Tableau) is cumbersome, if even possible. Once access is provisioned, limiting what data can be seen by which users requires significant IT involvement, delivered on a user by user basis. Further, no policy engines exist to limit where data can be accessed from, when it can be accessed and most importantly, how much data can be consumed by which users. The result is once a user has access, they have near free reign to view whatever they want without any limits on consumption.



The ALTR Platform installs using a smart database driver into the critical path of data access.

Solution:

ALTR's smart driver sits in the critical path between the user and the data, directly within the data visualization application on each end users' machine. From this position, ALTR logs all data access immutably out to private, permissioned blockchains, creating a single view of the truth of all data access and actors. Further, using ALTR's policy engine, accessed through ALTR's cloud hosted management console, a non-technical user can quickly invoke very granular data governance policy by user and user group, which is seamlessly and automatically effected through ALTR's smart drivers.

DATA PRIVACY & SECURITY

Problem:

Financial Institutions that do core data dumps into their EDWs create toxic data pools that contain voluminous amounts of personally identifiable information, PCI data, and even data subject to GDPR, CCPA and other pending privacy regulations. Standard data encryption methods (e.g., TDE, key-based encryption and tokenization) protect data at rest from remote access users, but do not offer adequate protection from administrative users with direct data access privileges, like DBAs and developers. Further, in its unencrypted form, these data find their way into many desktop applications and spreadsheets, which creates data sprawl issues that are unmonitored, not governed and generally unprotected.

Solution:

ALTR Protect removes sensitive data from the EDW, fragments it, then scatters those fragments across private and permissioned blockchains. Within the EDW, the data itself is replaced with a token value that simply references where the first bits of data exist in the blockchains. When a user requests data from the EDW that is protected by ALTR, tokens are returned to the ALTR smart driver installed in that user's application, and only if access is granted will that value be reassembled and delivered to the application. The sensitive (and previously "toxic") data does not exist anywhere in its full form. Within the EDW, the sensitive columns contain only tokens, protecting it from any users with direct access, while also rendering it useless for any bad actors in the event of a breach or exfiltration. With ALTR, if any users try to access protected data through applications without an ALTR smart driver, then only tokens are returned and those users must self-identify to enterprise IT that their applications need ALTR drivers

COMPLIANCE REPORTING

Problem:

Once data is delivered to EDWs, no effective means for logging all data access and actors exist. This leads to compliance issues where Financial Institutions cannot holistically and completely identify exactly what users accessed what data, when and from where. Further, if (and more appropriately, when) data is breached, determining who had previously accessed that data is impossible. Finally, existing syslogs and other "monitoring" technologies can be turned off or taken offline, and the log file themselves can be altered or erased.

Solution:

Sitting in the critical path between the users and the data, directly in the user's desktop application, ALTR smart drivers asynchronously log all data access and actors immutably to private and permissioned blockchains. Further, anytime a protected value is reassembled, the user who accessed it goes on blockchain record as having rebuilt a protected value – in essence the FI gets a read receipt for any protected data values that were viewed. When combined, this provides a single view of the truth of all data access and actors, stored immutable on a highly secure distributed ledger and accessible immediately, as an order one lookup. Should any sensitive data appear in other applications, or be found elsewhere (like in spreadsheets), it can be traced back to exactly what users reassembled it, when, how and from where. Unlike syslogs and other monitoring tools, ALTR smart drivers cannot be turned off, nor can their logs be changed, thanks to the write forward property of blockchains. Lastly, this level of compliance reporting on data access helps to significantly advance an Financial Institutions Cybersecurity maturity as measured by both the FFIEC CAT and the FSSCC Profile.