How to Address the Top Five Human Threats to Your Data

The first step in developing a resilient cybersecurity posture is identifying what it is you are trying to protect. For most businesses today, that most valuable asset is data. Customer data, competitor data, internal data – the information you rely on to operate and grow. This makes sense given developments in technology over the last decade. In 2018, the top five largest companies by market value were Apple, Amazon, Alphabet, Microsoft, and Facebook, each of which operates almost exclusively on the ability to collect, manipulate, and share data[1].

It's no wonder then that each of those organizations has been accused of mishandling data. The number is hard to pin down, but estimates are in the billions for the number of people affected by data breaches in 2018. In fact, over 750 million users were affected in the second quarter alone[2]. Overall, cyberattacks increased by almost 50% in 2018 over 2017, and the risks are only expected to rise. Damages related to cybercrime are expected to hit $6 trillion annually by 2021[3]. Besides the economic exposure and threat of regulatory response, these data breaches also lead to a loss of reputation. Can customers trust you to handle their data safely?

Ranking of the Companies Rank 1 to 5	Market Value in Billions of US Dollars
Apple	926.9
Amazon	777.8
Alphabet	766.4
Microsoft	750.6
Facebook	541.5

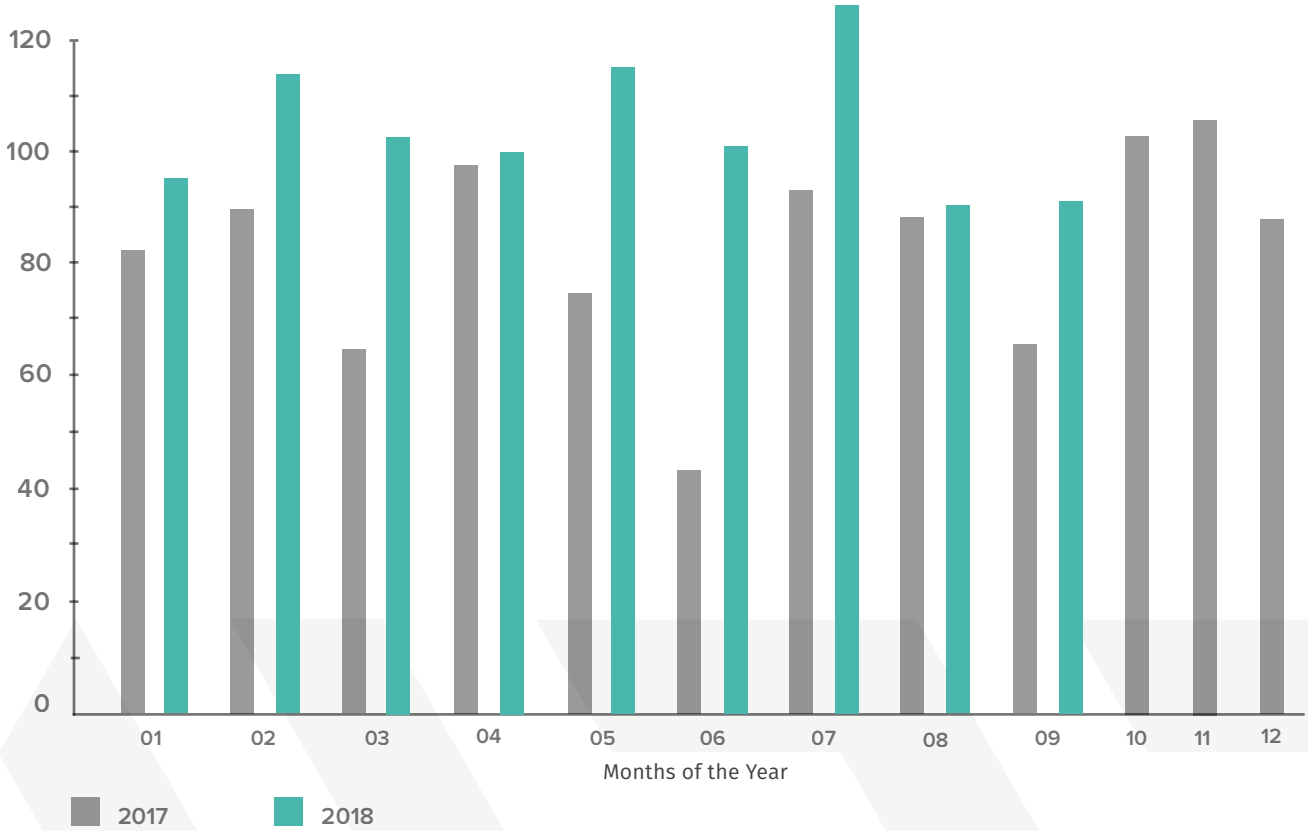
[1] https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/
[2] https://www.ptsecurity.com/ww-en/about/news/293941/
[3] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

What's The Biggest Threat To Data?

Whether through intentional malicious acts or simple negligence, the people with access to this data are the biggest threat to data security and privacy. The so-called "insider threat" is very real; in fact, according to the 2018 Insider Threat Report, 90% of organizations believe they are vulnerable to insider attacks. Companies are shifting their security focus towards these threats, with 64% reporting a focus on insider threat detection, 58% on deterrence, and 49% on deploying post-breach analysis and forensics. The majority of respondents – over 80% – are in the midst of developing and deploying insider threat programs[4].

90% of organizations believe they are vulnerable to insider attacks

As companies expand their internal cybersecurity operations to protect the critical data on which they thrive, many become overwhelmed. Data security threats seem to be everywhere and growing. Even the most hardened, off-the-grid security experts acknowledge that it is impossible to be 100% secure. Instead, experts suggest developing a security strategy that focuses on the most significant – and most likely – threats to your business. Addressing these top threats to your data is the first step in building a layered, data-centric approach to data security and privacy, which is vital in a world where data is currency in the bank and it seems everyone has a key to the vault.



Number of Cyberattack Incidents per Month in 2017 and 2018

[4]https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

The Top 5 Human Threats to Your Data

#1 Guessed and Stolen Credentials

Obtaining user passwords is one of the most common ways cyber criminals breach security defenses. The 2017 Verizon Data Breach Investigations Report found the number of data breaches involving weak or stolen passwords rose to 81%, up from 66% in 2016 and 50% in 2015[5]. Using brute force or dictionary attacks – or simply peering over someone's shoulder – hackers essentially "guess" user passwords based on their knowledge of password habits and open source intelligence. This is especially true for weak passwords, which are, unfortunately, still used frequently across multiple applications and platforms. According to over 1000 surveyed individuals in the US, more than half used the same password for multiple online logins[6]. This makes the hacker's job easy.

81%
of data breaches involve weak or stolen passwords

1.	123456	6.	12345
2.	password	7.	1234
3.	12345678	8.	111111
4.	qwerty	9.	1234567
5.	123456789	10.	dragon

Most Common Weak Passwords

Even strong passwords can be compromised. Cybersecurity expert Troy Hunt, who maintains the Pwned Passwords database, notes that once a password or passphrase is exposed by a data breach, it is no longer secure. His database includes over half a billion compromised passwords, some of which are demonstrably "strong"[7]. Unfortunately, any password exposed is a password compromised. Attackers hoard the information exposed in these breaches and engage in credential stuffing, testing the combinations on unrelated sites. And, since so many individuals use the same password on multiple platforms, the hackers invariably find success.

Cyber criminals are also adept at manipulating credentialed users into giving away passwords through phishing and spear-phishing campaigns. That email from the CEO asking to reschedule the quarterly board meeting? It might not be all it seems. This popular phishing campaign identified in January 2019 is just one way malicious entities attempt to steal credentials from those with access to organizational data[8].

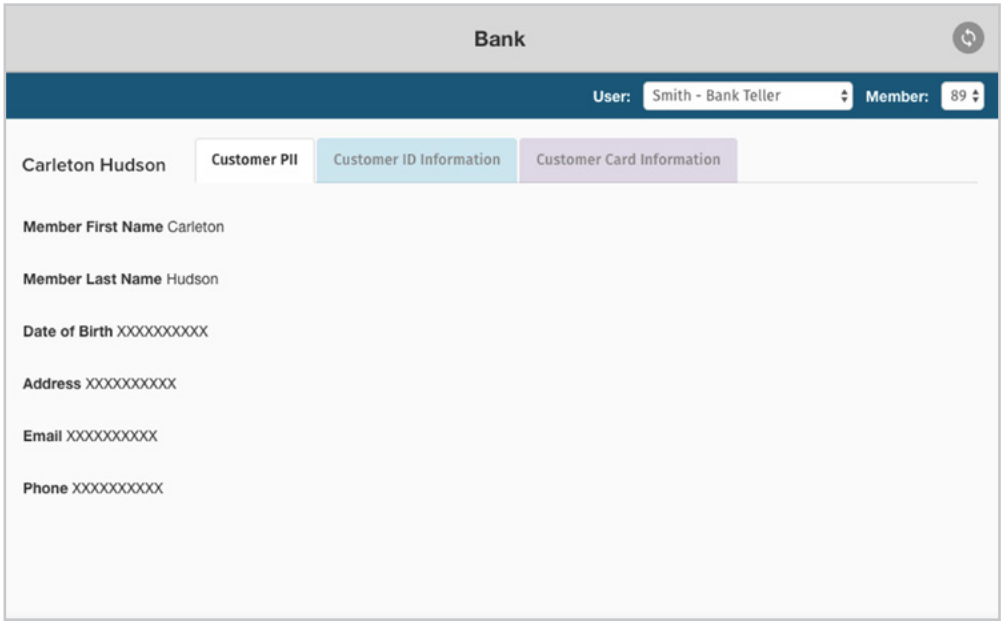
Securing passwords is no easy task. Attackers put a great deal of effort into these campaigns, making the phishing websites look almost identical to their legitimate models. Even after security awareness and phishing identification training programs, users still click on phishing emails almost 25% of the time[9]. Security "strength" indicators are also weak tools for measuring actual password strength. In one stunning example shared by System and Security Administrator Aaron Toponce, the password geyps5aykj0q71c637n9g14ycg is considered weak, while Password123! is considered strong!

To overcome this threat, businesses are increasingly turning to technology that recognizes unusual behavior when it comes to data consumption by users, instead of relying entirely on passwords to secure data. This is a key aspect of what ALTR Govern, the data governance product inside of ALTR's platform, provides. ALTR Govern provides businesses with the ability to prevent breaches in real-time by slowing down or blocking the flow of data when consumption of that data exceeds set thresholds at the application or user role level. This data-centric method enforces protections at the data level to protect against scenarios when password protection fails. In addition, ALTR Monitor creates a completely tamperproof audit log of all data anomalies, administrative actions, and resolutions inside of an ALTRchain, a high-performance private blockchain.

[5] https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
[6] https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/
[7] https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/
[8] https://www.zdnet.com/article/this-password-stealing-phishing-attack-comes-disguised-as-a-fake-meeting-request-from-the-boss/
[9] https://enterprise.verizon.com/resources/reports/DBIR_2016_Report.pdf

#2 Private Data Exposure

The supply chain of the 21st century is far more complex than those of previous eras. Businesses today rely on their relationships with contractors, vendors, and partners to ensure every facet of their organization is optimized, from heating and building infrastructure to website development and big data analytics. Finding trustworthy partners is key to moving the business forward.



Example Application with Masked Data

Yet without proper tools to secure data, even trustworthy partners may see more than they should. Lacking the proper controls, the unintended exposure of private or regulated data is likely. Take, for instance, the risk posed by third-party application developers. Oftentimes, in an effort to use realistic datasets to build and maintain applications, developers end up accessing private data. This puts the development partner and the business at increased risk – of private data exposure and reputation loss. Improper data exposure with partners is common, and everyone from HVAC vendors to medical transport providers is seeing more than they should.

Unfortunately, the most common current method for protecting private data is controlling access at the application level. IT departments typically focus on who has access to what and use access-management tools to do so. For example, IT makes sure the finance department has access to payroll applications and marketing has access to a content management system. This creates gaps in data governance. All too often, private data is simply left exposed.

What these solutions fail to do is focus on what it is that needs protection: data. In essence, these controls are about users, not about data. Newer developments use data classification groupings, such as GDPR data or HIPAA data, to enable data-centric controls by the business. By associating these data classifications with user groupings, businesses can protect against data exposure. Data classifications give IT more control over data flow and protect against data exfiltration.

With ALTR's platform, ALTR Monitor allows organizations to understand the relationships between user groups and data classifications. ALTR Govern then allows for the enforcement of locks that provide format-preserving dynamic masking of data when it is accessed by unauthorized groups. For instance, a social security number (345-21-8678) might be replaced by "XXX-XX-XXXX" as it flows out of the database for users who should not have access to it. By understanding who is accessing what data, and enforcing rules concerning who should have access, businesses are better able to secure private data before it is exposed without having to re-engineer applications.

#3 Theft Using Privileged Database Access

Insider threats are growing across every industry. According to the 2018 Insider Threat Report, privileged administrators pose severe security risks to organizations[10], with more than half of respondents identifying this pool as high-risk. Those with privileged database access, such as database administrators (DBAs) or IT leadership, have access to database servers, encryption keys, and tokenization maps. These users are able to easily bypass governance.

Unlike excessive privileges given to regular employees or vendors, privileged database access refers to legitimate access abuse, where users access private data for unauthorized purposes. In this case, users with deep credentials may access confidential business information, privileged account information, sensitive personal information, or intellectual property. It is important to note that privileged credentials are also subject to theft.

How do most organizations today attempt to ensure the security of this data at rest? They encrypt it. Encryption uses an algorithm to transform data, obfuscating it, and incorporates a key value that can be used to transform data back to its original form for use. Unfortunately, once someone has the key, they are able to decrypt data. Even the strongest encryption methods – such as the bcrypt algorithm – still use a key to decrypt stored data.

In addition, organizations are increasingly attempting to implement stronger access controls for internal users. Databases offering granular-level access controls are more popular than ever; unfortunately, those credentialed users are a risk to data security. Whether by intentional malicious acts, the theft of privileged credentials, or the elevation of low-access privileges to high-access privileges, theft using privileged database access is an unmitigated threat.

New technologies are overcoming the limitations of these riskier encryption methods. Developing targeted access credential groups gives organizations more control over who can access sensitive data, and when. Format-preserving dynamic masking protects the data while still ensuring the applications and tools your business relies on continue to perform.

To see how ALTR can fragment and scatter data, watch this video:

https://www.altr.com/video-altr-data-security-platform/

Key to this is identifying which groups need access to which information, and which data is the most at-risk for exposure. It is essential to clearly identify, monitor, and manage high-risk data first. Once businesses know who has access to high-risk data – and how much they are accessing it – it is much easier to secure that information. When an organization can do this, using dynamic masking to protect private information, like PHI and PII, can be optimized.

Responding to the threats of privileged database access, cybersecurity experts at ALTR have developed fragmentation technology that uses a secure private blockchain to obfuscate data-at-rest. ALTR Protect, instead of encrypting and storing the data in a “secure” database with keys nearby, replaces sensitive data at the column level with a reference hash, then fragments the data and stores it across an ALTRchain, a high-performance private blockchain. The reference hash points to the first fragment, which contains a reference to the second fragment, and so on. No key or tokenization map exists to make data easy to steal, and data is reassembled rapidly whenever needed.

With ALTR Protect, the ALTR platform creates a keyless vault for data, ensuring that data continues to operate fully for the business but remains impenetrable to attackers, even if they come from privileged administrators within the organization.

[10] https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

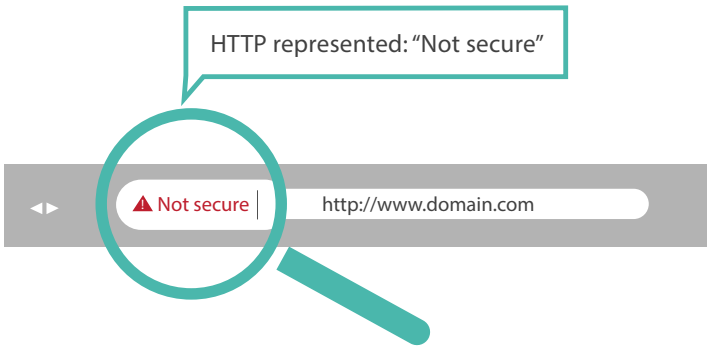
#4 Software or Hardware Misconfigurations

Security misconfigurations remain in the top ten OWASP security threats to business[11]. As organizations install new hardware or transfer to a new software application, simple missteps can wreak havoc on the company's security architecture. Insecure default configurations, incomplete configurations, unsecured cloud storage, misconfigured HTTP headers, and missed patches and upgrades are all examples of misconfigurations. In these cases, a single unchecked box might lead to devastating security holes.

In one OWASP security misconfiguration scenario, an engineer fails to disable directory listing on a server, enabling an attacker to list directories and access compiled Java classes. Using reverse engineering, the attacker can view the code and identify an access control flaw in the application, granting them access to the system. Once in, attackers almost always remain undetected, averaging nearly 200 days globally before being identified[12]. According to a Trustwave Report, 81% of reported intrusions are not detected by internal security controls. Instead, news outlets or law enforcement identify the threat[13].

Besides SOPs, rigorous checklists, and "buddy" systems, most organizations today do not have structures or tools in place to solve for these security gaps. Data exfiltration by insiders through applications or APIs, or breaches by outside attackers through these holes, are unnervingly common, and – given the predisposition of humans for imperfection – no one is immune.

Thresholding data is a new way to approach the possibility of an inside threat attempting to "smash and grab" data. Insiders often need access to sensitive data to do their jobs, but the amount of access, and what they do with that access, can vary tremendously. Thresholding data enables the business to slow down and stop data exfiltration as it is happening. This increased visibility and management restores digital trust, allowing operations to continue while validating use.



ALTR Govern delivers this real-time control, giving business the tools to impose thresholds and understand typical – and atypical – user behavior.

Outside attackers know where to look for gaps caused by misconfigurations. Once inside, attackers can decrypt databases and worm their way through the network slowly, unlocking your most valuable assets.

A key defense in this scenario is to protect the data when it is at rest, so that even if an attacker enters your network, they cannot access your data. Improving on less secure encryption keys, businesses today are moving towards a keyless data obfuscation model. Innovative developments in blockchain technology and security frameworks – such as fragmentation – keep the data protected from even the most driven attackers.

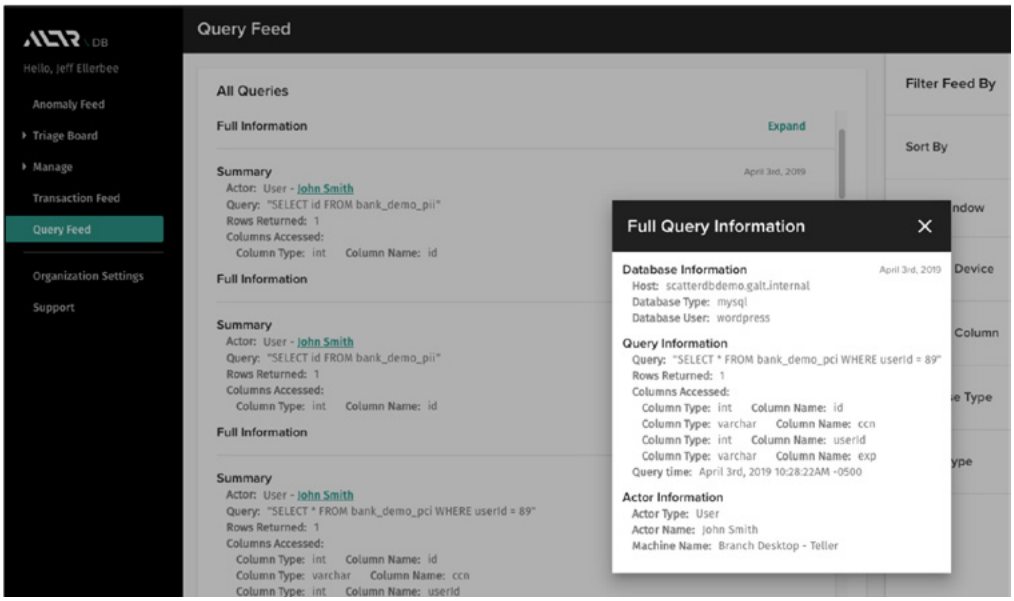
81%
of reported intrusions not detected by internal security processes

ALTR Protect fragments and scatters your data into multiple blockchains, creating keyless protection. Each fragment references the next, so there is no key or token map for bad actors to find and use. This at rest data retains most data operations, and the ALTR driver quickly reassembles the data when requested. The ALTR platform takes the protection of data to the next level by placing security in the critical path of data.

[11] https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project
[12] https://www.computerweekly.com/news/252438158/Average-attacker-dwell-time-nearly-six-months-for-EMEA-study-shows
[13] https://www.trustwave.com/en-us/resources/library/documents/2018-trustwave-global-security-report/

#5 Modified Database Access Logs

Every airplane is equipped with a black box, a flight data recorder that records the state of a plane and any cockpit audio that helps forensic teams investigate aviation incidents. A database operates in much the same way with one key difference. The database is continuously monitored, and access logs are kept regardless of an incident. Database access logs identify who accessed the database, when, from what device, and include other pertinent information valuable in a security investigation.



Detailed Query Feed Within the ALTR Platform

Unfortunately, cyber criminals are typically quite technically adept and modifying database access logs is no great feat for those with malicious intent. By modifying the access logs, technical users hide unauthorized acts by editing or deleting log files. Depending on the criminal's intent, they may modify the log files to show another user accessing the database or simply delete any evidence they were ever there.

To identify these changes, organization must continually review the log files. But monitoring access log files is a tedious process, and humans are prone to overlook subtle changes. Even small networks produce copious numbers of log files – far too many to monitor manually – so many businesses use log analyzers, automated auditing and analysis tools. These tools may tell you if something seems suspicious or if there is an obvious breach, but they do not ensure modified or deleted access logs will be identified 100% of the time.

Developments in blockchain technology offer a glimpse at a better solution. The technology prevents users from modifying records by saving every data access event to an immutable blockchain record. By removing the ability of users to modify records, blockchain restores digital trust. Since every act is saved to the blockchain, where it cannot be altered, there is no need for complex predictive analytics and behavior monitoring. Attackers no longer have a place to hide.

The ALTR platform delivers on these complex capabilities. ALTR Monitor logs all activity, including administrative actions, to an immutable log that is stored in an ALTRchain, stopping any attempts at log modifications.

Data is everything to the enterprise. It is the raw material that fuels the business, driving growth and building the future. That is why it is essential that organizations take steps to ensure the data on which they rely is secure. Unfortunately, most organizations today are reactive, operating without visibility into data flow. Despite clear recognition by business leaders regarding the human threats to data security, few believe they have a comprehensive, hardened security architecture capable of deterring, detecting, and remediating the ever-evolving threats of tomorrow.

While humans remain the largest threat to data security, many are working tirelessly to develop new technologies to better manage our faults. Understanding these threats to data is the first step in identifying the right solutions.

End the Threat to Your Data

The ALTR platform offers a comprehensive set of tools that work together to ensure your organization is prepared for these most significant data threats. ALTR augments the database manufacturer's driver, creating a buffer between your data and those requesting it. The ALTR smart driver is optimized for low latency and deploys with zero impact on databases or applications.

Together, ALTR Monitor, ALTR Govern, and ALTR Protect make up the ALTR platform. By reporting on the confluence of data and user risk to inform policy, delivering real-time control and breach investigation, and enabling impenetrable protection of data at rest, these components work together to provide visibility, management, and security tools to the business.

The technology that supports the platform is cutting edge, and the patented ALTRchain uses private blockchain architecture across the ALTR platform, restoring digital trust through an immutable ledger that logs database activity.

The ALTRchain works at application speed and in any environment, whether on-premise, in a private or public cloud, or in a hybrid configuration.

ALTR offers a path forward for enterprise security that moves beyond traditional data security tools. Data threats are everywhere, and the humans inside the network are one the most significant threats to data privacy and exposure. By taking an innovative approach to data security, the ALTR team seeks to create a permanent record of the truth for every client. By monitoring, governing, and protecting your data with ALTR, you can manage these risks to data and restore digital trust to your organization. ■

If you would like to learn more about ALTR or request a demonstration of the ALTRchain, contact us at www.altr.com.

www.linkedin.com/company/altrsoftware/

twitter.com/altrsoftware

www.altr.com/contact-us/

1-888-757-2587

ABOUT ALTR

ALTR's mission is to restore digital trust by transforming the way that data is monitored, accessed, and securely stored.

WWW.ALTR.COM