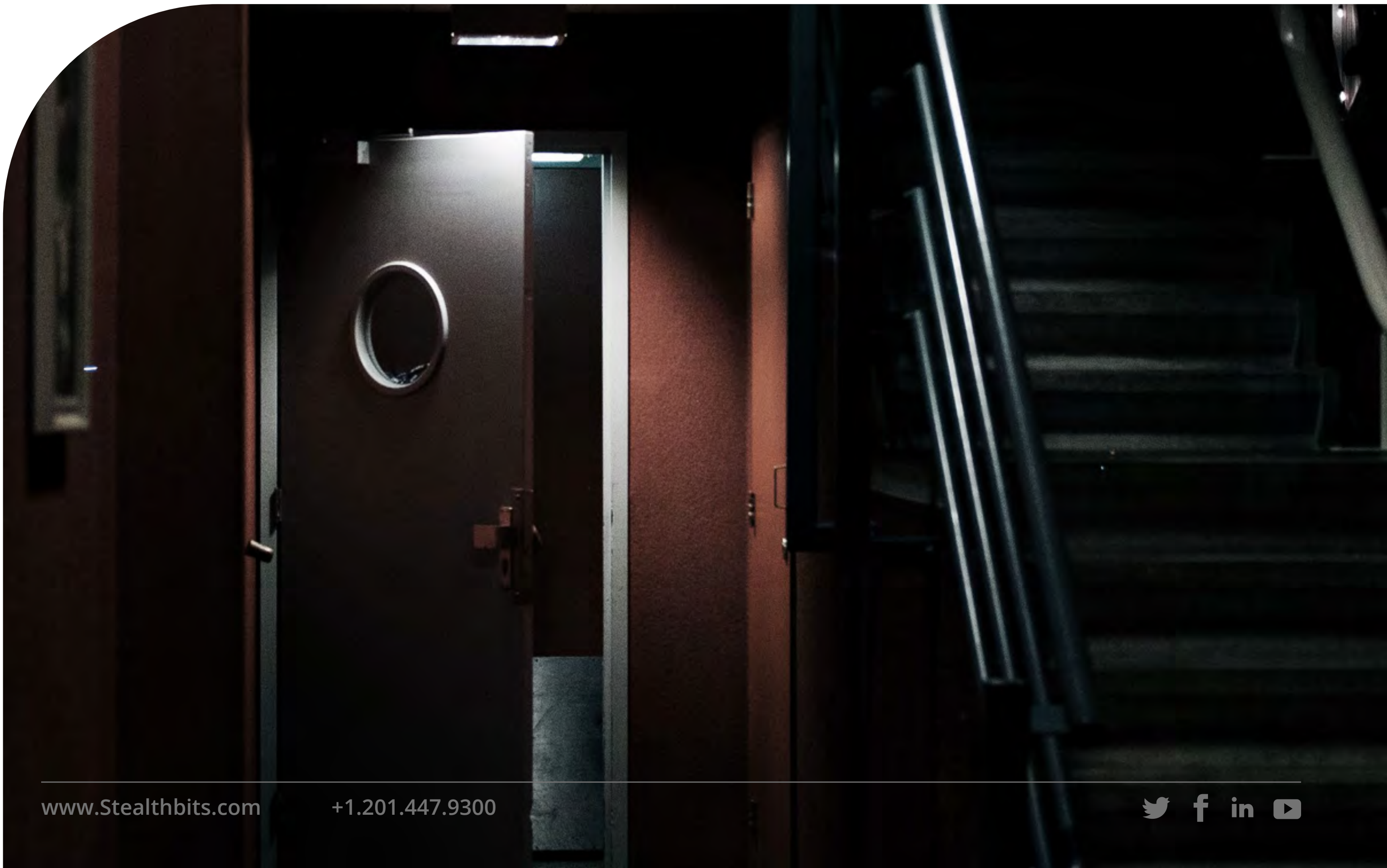
SOLUTION BRIEF

PRIVACY: DATA HAS A BACKDOOR - HAVE YOU LOCKED YOURS?

stealthbits
NOW PART OF netwrix

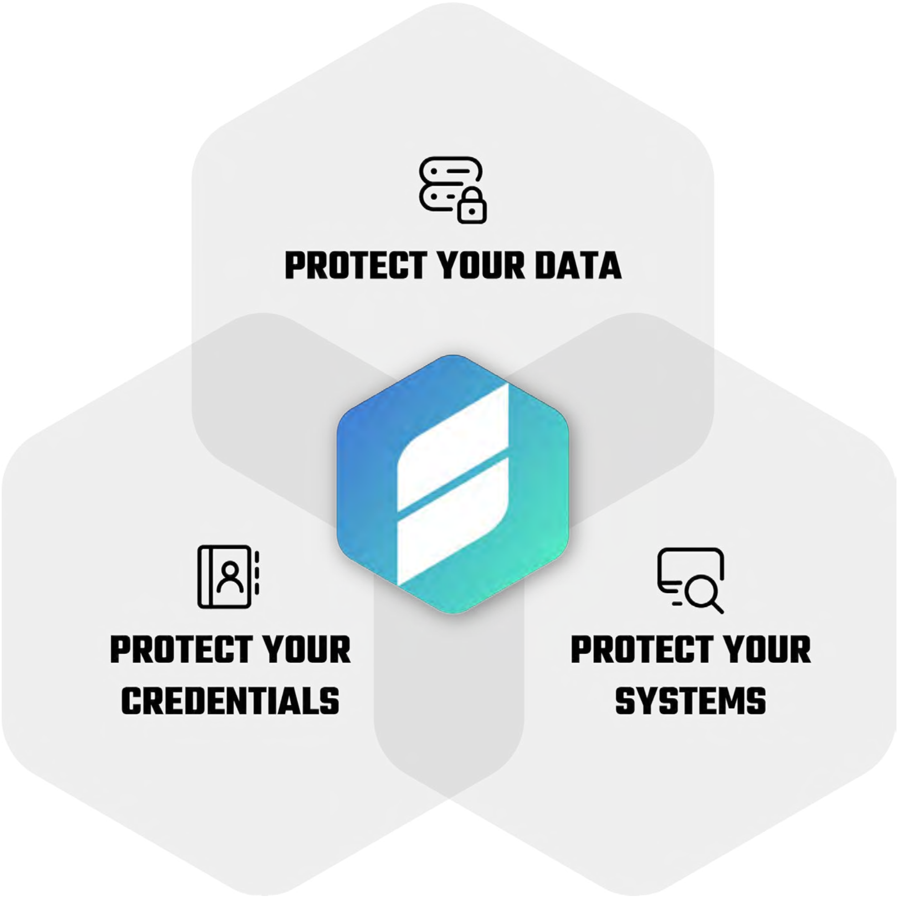
For years, the personal information of consumers has been harvested en masse by many of the organizations they've done business with, shared with and sold to other businesses, and seldomly managed in accordance with sound data protection principles. Stored in virtually every possible data format across virtually every conceivable location, personal data continues to be specifically targeted and often easily exfiltrated by attackers, resulting in the compromised identities of millions of individuals around the world and trillions of dollars in loss. It was inevitable that data privacy regulations like the EU GDPR, CCPA and others would be born and carry with them, stiff penalties for organizations who failed in their ability to locate, secure and manage their customers' data.

In 2021, properly securing data remains among the most challenging of tasks for cybersecurity teams at organizations of any size. While there are literally hundreds of software vendors offering solutions to address this, many organizations have realized most approaches fail to address the real, underlying problems. Put in a simple analogy, imagine that an organization has all their sensitive data placed inside a box, in a room inside a solid brick building. The current approaches dictate that they use reinforced steel doors with deadbolts that require multiple keys to open and even a fence that prevents intruders from getting to the front door in the first place. Standing on the street in front of the building, one would be filled with a sense of security, confident that any sensitive corporate and customer data is kept private. However, in the alley behind the building, there is a backdoor, propped open with a cinder block and anyone who knows it's there, could simply walk right in and access all the data.



How does this happen?

Surely in a world filled with various privacy regulations, awareness and massive media exposure to data breaches, this issue of a backdoor must have been noticed and accounted for by now? The problem usually lies in the fact that the team who is responsible for the back door and the team who is responsible for the front door are not one in the same, and often have different priorities. Putting aside the simple analogy, there are three priorities that are required to achieve privacy and they all start with protection.



Protect your data?

Data Access Governance is about making access to data exclusive. It's about limiting the number of people who have access to data – and their permissions to data – to the lowest levels possible. At a high level, this involves the discovery of where your data lives followed by classifying, monitoring, and remediation of the conditions that make managing data access so difficult in the first place. The result is effective governance that promotes security, compliance, and operational efficiency. This is the focus of the "front door" in the analogy mentioned earlier.

Protect Your Credentials

Ensuring the security of your data is more than just understanding where it is and who has access to it. Data security relies heavily on the security of Active Directory. It's crucial to pinpoint vulnerabilities in Active Directory permissions, account passwords, privileged access rights, configurations, objects, and more. Ensuring that Active Directory is clean, understood, configured properly, monitored closely, and controlled tightly, directly impacts data security, virtually wherever your data lives. Think of it this way, if you have taken the important steps of ensuring that only members of a certain group can access sensitive data, but someone can still go into Active Directory and simply create a new user and add it to that group, they've just walked in via your back door and your data is no longer safe.

Protect Your Systems

Breaches typically begin at the desktop and server layers of an organization's IT infrastructure and spread through the overabundance of privileged access rights. Reducing "standing privileges" and remediating misconfigurations and vulnerabilities across desktop and server infrastructure mitigates risks like lateral movement and privilege escalation, keeping AD safe from advanced attacks. Imagine if you could provision only temporary access to perform a specific task, then remove it when the task is completed. If approached in that manner, you'd eliminate standing privileges all together, drastically reducing your attack surface. Referring to our analogy, someone can't walk in through a backdoor if it doesn't even exist.

Benefits of a Multi-Layered Approach

Once you understand that achieving data privacy is done through data security, protecting your data, credentials and systems, it's then important to look at the capabilities you will gain from this approach.

Data Discovery

The capability to perform "identity-centric" discovery of subject data is extremely beneficial as it will enable you to maintain an understanding of which records pertain to which data subjects. This is a very important step that will help you down the road in this area because it empowers you to make appropriate decisions about access, recovery and other actions. You can't protect what you don't know about.

Subject Access Requests

Considering that several of the regulations involving data privacy provide the use case for people to request clarity around what information an organization has about them, being able to respond to these requests with a detailed report is a crucial capability. It doesn't stop there though. Having the ability to build workflows that automate the response and any actions that need to be taken as a result of the report is just as important.

Privacy By Design

This refers to implementing a least privilege model. When you have taken steps to truly protect your data, credentials and systems, it only makes sense to establish a baseline of policies that keep things protected. This can be built in going forward and you can then maintain records of who has been granted access and why.

Breach And Detection Response

At a high level, once your house is in order and everything is where it should be, you're going to easily notice when something is askew. This goes even deeper than simply noticing something off and refers to the multi-layered approach that mitigates, prevents, detects, and responds to advanced threats in real-time through orchestrated and automated responses.

NEXT STEPS

Organizations cannot afford to waste time, money, and focus deploying and maintaining two or more technology stacks to achieve data privacy. It is inefficient and nonsensical. Stealthbits provides the technology and the know-how to address data privacy and data security simultaneously, helping to facilitate critical data privacy workflows and processes, while also implementing effective controls that mitigate the risk of credential and data compromise. Remember, if you aren't addressing all three aspects of protecting your data, credentials and systems, your data is vulnerable to exposure.

Why not find out what sort of back doors your organization may have open by doing a deep-dive into the security of your structured and unstructured data, Active Directory, and Windows infrastructure? Stealthbits offers a Credential and Data Security Assessment (CDSA) which will look at each of the three layers:

- **Data** — Discover sensitive data, open access rights, high-risk permissions, and stale data that is putting your organization at risk.
- **Credentials** — Pinpoint vulnerabilities in Active Directory permissions, account passwords, privileged access rights, configurations, objects, and more.
- **Systems** — Identify privileged access rights, service accounts, critical misconfigurations and conditions attackers exploit to steal credentials.

To learn more about how Stealthbits' privacy-embedded approach ensures appropriate access governance and removes hidden vulnerabilities for heightened security, while facilitating critical data privacy processes, please visit: www.stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix