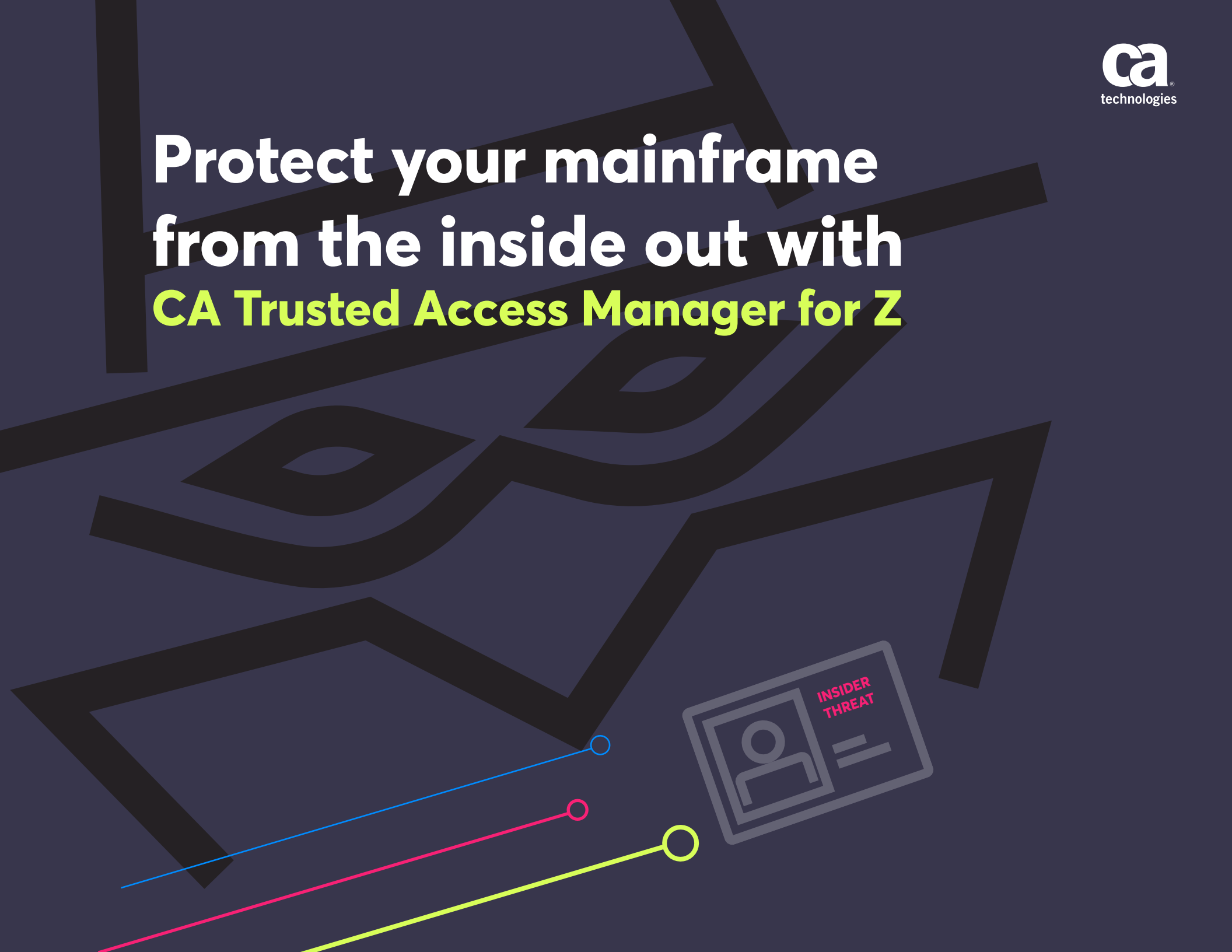
Protect your mainframe from the inside out with

CA Trusted Access Manager for Z



If you think the biggest security risk to your business is from outside your office, think again.

We like to think that our businesses are made of the most trustworthy and dedicated employees and, more often than not, we are correct. But sometimes, trust is breached, either through careless actions or intentional ones. And when that breach involves your mainframe—which transacts over 80 percent of corporate data—the results can be catastrophic.

When privileged identities aren't managed securely, your business is exposed to significant risk of insider threat, putting extensive access to the most sensitive resources in the entire data center into the wrong hands.

And it happens **more often** than you think.

The security landscape on the mainframe is changing drastically, and you need a strategy to secure the most sensitive data in your business, and those that have the highest levels of access to it.

77% of data breaches were from **internal sources** in the past year.[1]

70% of inside data breaches take **months** or **years** to discover.[1]

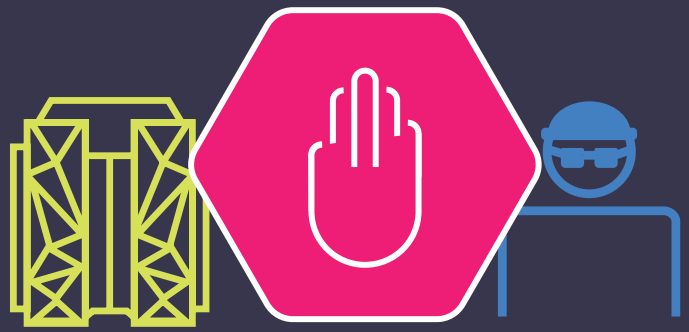
$11M Direct **cost** of a single data breach for U.S. financial organizations.[2]

31% of consumers **discontinued their relationship** with the company that had the breach.[3]

Sources:
[1]Verizon Data Breach Report, 2016; [2] Ponemon Institute, "Data Breach Study", 2016;
[3]Ponemon Institute, "Reputation Risk Study", May 2017

Protect against insider threats and improve your risk posture.

CA Trusted Access Manager for Z gives you tighter control and tracking of privileged access to mainframe resources, reducing the risk of insider threats and data breaches.



CA Trusted Access Manager for Z provides streamlined and secure management of privileged user identities, providing that only the **right users** have the **right access** to critical mainframe resources at the **right time**.

CA Trusted Access Manager for Z runs 100 percent on the mainframe, easily integrating into mainframe security teams' existing processes and best practices. Leveraging enterprise security manager (ESM) solutions, **CA ACF2** and **CA Top Secret**, CA Trusted Access Manager for Z can both promote and demote existing users to greatly reduce the threat surface of sharing privileged credentials.

CA Trusted Access Manager for Z:

- **Provides privileged user management on-platform**
  Runs on-platform and in line with mainframe security teams' processes and workflows
- **Promotes and demotes existing user IDs**
  Leverages CA ACF2™ and CA Top Secret® user ID to eliminate the need for privileged credential sharing
- **Protects against recovery costs, customer loss and fines**
  Enables security teams to stay in complete control, deliver trust, streamline audits and mitigate fines

Life without CA Trusted Access Manager for Z

Often, privileged identities with shared credentials are created – sometimes through negligence and sometimes with malicious intent. When privileged identities aren't managed securely, it exposes businesses to a significant risk of insider threats.

For a company that does not use CA Trusted Access Manager for Z, such data breaches can happen in a blink of an eye.

For example, let's say that the manager of mainframe security is approached by a team member who needs elevated access to perform a specific job function. The timebox is only about 10 minutes, so the manager gives him his password.

Then, let's say that another team member gets hold of this same password, but has other (deceitful) plans for what he can do in this privileged state. This employee now has access to sensitive personally identifiable information (PII) that he can sell on the black market.

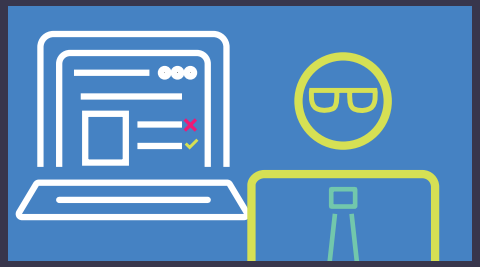
The discovery of insider privilege misuse can take months and even years. And once credentials are shared, pinning the data breach to any one employee can be next to impossible.

The result: one malevolent employee gets away with a crime while the company loses millions in direct costs … not to mention severe reputational damage.

Life with CA Trusted Access Manager for Z

Using this same example, a company that uses CA Trusted Access Manager for Z would benefit by eliminating the need for shared privileged credentials and giving its managers complete control over mission-essential mainframe data.

Here, the manager of mainframe security uses CA Trusted Access Manager for Z to streamline the elevation of his team member's user ID to a privileged ID.



For as long as this team member works on his job function, the security manager is in the driver's seat. He can restrict and monitor all privileged activity and he can demote permissions and rules on-demand to greatly reduce the threat surface of sharing privileged credentials.

And when the job function is complete, CA Trusted Access Manager for Z generates auditing and forensics on all actions performed by the team member in his privileged state—from the activity in the datasets to the demotion of the user identity—providing a holistic, full-picture view for the security manager.

The result: a business that operates far more efficiently and securely than ever before, building trust while protecting the company against recovery costs, customer loss and fines.

It's all about trust.

Digital trust is the cornerstone of the application economy. The secure management of privileged users across the mainframe is vital to both business success and developing trust—inside and outside the organization.

CA Trusted Access Manager for Z helps organizations build trust by streamlining the management of privileged identities on the mainframe. It allows you to:

- Control who has access to which critical mainframe resources—and when
- Leverage existing identities to reduce the risk of creating new users
- Work with CA ACF2 and CA Top Secret for reliable mainframe security

Learn more about how you can protect against insider threats and improve your risk posture. Visit CA.com/TAM

ca technologies