CIRRO.COM

Benefits of an Identity-Based Perimeter

A CIRRO WHITEPAPER

Redefining the Perimeter: Identity

Cloud technology, big data, mobile connectivity—the rush towards digital transformation continues. Enterprises are rapidly integrating innovative technologies into all areas of their business, changing how they operate and how they deliver value to their customers. Modernizing by leveraging digital technology is critical for businesses to stay competitive and relevant in the market, and can bring great rewards—but also amplify risk.

And while securing data is and has been a significant priority for decades, recent massive data breaches have highlighted the enormous financial and reputational costs associated with this risk. As enterprises are being held more accountable for the security of their data, the financial liabilities have also increased.

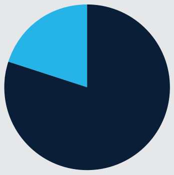
The intersection of disruptive technologies that come with digital transformation and new attack vectors has rendered traditional enterprise security perimeters ineffective—and focusing only on legacy perimeter protection leaves an organization at risk. Modern enterprises have shifted from protecting the perimeter to managing and governing digital identities to meet modern business needs, integrate modern IT infrastructure and eliminate security gaps.

Why Identity?

Gaps in perimeter security and modern business demands are driving businesses to replace or enhance their existing enterprise fixed perimeter security. Businesses now need to protect resources by extending security beyond the traditional walls of the enterprise to individual users, services and devices.   With new technology helping to close security gaps and reduce costs, identity-based solutions take on an even greater significance because they are able to close the two largest and most prominent threats to data: compromised database credentials and excessive rights over data.

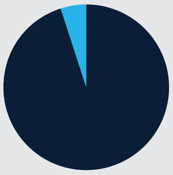
The key benefit in innovating to an identity-based solution is clear: the closer an organization approaches an identity-based perimeter, the less security gaps there are and the cheaper it is to meet modern data needs and manage modern data infrastructure. The move towards zero-trust identity data perimeters has increased as it has become increasingly clear that without a modern identity security solution in place, suffering a data breach becomes almost inevitable.

Eliminate the two major threats to data



80%

of reported data breaches are due to compromised credentials[1]



95%

of compliance issues are due to excessive data rights[2]

1. Australian Cyber Security Centre (ACSC)   2. Security consultants

Zero-Trust Security: Never Trust, Always Verify

1980	**Network Perimeter**
1999	**Virtual Desktop Perimeter**
2007	**Software Defined Perimeter**
2019	**Zero-trust Identity Perimeter**

Arriving at a zero-trust identity-based security solution has been several decades in the making.

Moving from a network perimeter, to the virtual desktop and then the software perimeter has led finally to zero-trust identity perimeter as the increase in mobile computing and cloud infrastructure has allowed people and programs to access data from anywhere at any time.

And although technology has shrunk security gaps, the ones that remain require an identity-based solution to fully secure valuable assets. The zero-trust concept of "never trust, always verify" has created a pervasive force-field of security, utilizing multi-factor authentication and access policy rules as critical components of the verification process.

And although technology has shrunk security gaps, the ones that remain require an identity-based solution to fully secure valuable assets. The zero-trust concept of "never trust, always verify" has created a pervasive force-field of security, utilizing multi-factor authentication and access policy rules as critical components of the verification process.

The many organizations now adopting identity-first approaches to security understand the value of zero-trust security to secure corporate data. This simple identity verification test identifies bad actors with nefarious intent from the get-go—a key component to stopping any infiltration at all, and the underlying concept behind zero-trust security—never trust, always verify.

Today's database security—APIs, VPNs, firewalls, and Privilege Access Management software—while useful, only protects your database perimeter. But what about hackers who pose as valid users? Or hackers that use stolen credentials, an increasingly common tactic? Traditional perimeter security measures do not check and block access, either from humans or programs.

An identity-based perimeter can solve security problems using zero-trust security principles, while facilitating easy, platform-agnostic access to verified users. It also provides a more efficient and secure set of database access and management tools and takes full advantage of all the benefits of cloud technology while also dealing with any and all security challenges that have plagued more traditional security technologies.

Need More Reasons to Choose an Identity-Based Solution?

Individuals, applications and “things” are accessing critical data and resources, and each of these has an identity. Identity-based solutions manage these identities of people, applications and devices—and provide other benefits as well. Here are some of them:

Improve employee productivity.

Hiring a new employee means onboarding and giving them access to specific parts of your system, giving them new devices, and provisioning them into the enterprise. Non-security experts can often implement identity-based solutions, and enabling non-technical staff reduces costs.

Self-service.

Self-service provisioning speeds up process and increases productivity, without having to ask your IT team for their time and/or permission.

Eliminate need for passwords.

Never hand out database credentials again. With a digital identity, your customers and partners can access different areas of your system without ever entering or knowing a direct database credential.

Zero-trust security.

Securing all aspects with multi-factor and strong authentication gives you the assurance of knowing the identities that access your system are fully verified. Eliminate the expense and maintenance of VPNs.

Improve business agility.

Security often translates to less agile, due to extra staff and costs that can slow you down. But technology is shrinking the gaps and reducing costs. The closer organizations get to an identity data perimeter, the less security gaps there are, and the cheaper and easier it is to meet modern data needs and manage modern data infrastructure, therefore improving business agility.

Why Choose an Identity-Based Perimeter Security Solution?

Most organizations have to prioritize their security solutions. There are many security products on the market—and obviously, not all security products are the same. Some cybersecurity products monitor and alert if there is suspicious movement. Some try to lock out intrusions, like firewalls, VPNs, password management systems and virtual desktop security solutions. And then there are identity-based data access and controls solutions—a force field for your data.

What if you had to choose just one? What would you choose? An organization that chooses an identity-based perimeter solution is choosing the most pervasive solution that will close the most significant data security gaps.

Choose Cirro as Your Identity-Based Perimeter Security Solution. Become More Secure and More Productive for Less Cost.

Cirro is the unhackable database solution that easily transforms existing data infrastructure into a modern identity-based perimeter, immediately providing all the security, auditing and access benefits that you want.

These new technologies improve the agility of security, DevOps and data teams to better respond to business needs. Until now, providing universal data access with speed, control, compliance, and ease had come at the expense of security. That contradiction is solved with the market's first self-service database access and data controls solution.

Zero-Trust employs multi-factor verification for users instead of relying on traditional database credentials. Service accounts are verified through access control policies. Combined, these make Cirro virtually hack-proof. It also features alerts, blocking and SQL auditing capabilities, as well as management tools that allow full control to easily migrate, replicate, subset, and compare and sync data.

Cirro also features data controls with row and column security, obfuscation, and key-based encryption. These controls integrate with your directory and multi-factor providers, allowing users to access databases with their multi-factored identities instead of shared database credentials. With this you can:

- **Eliminate VPNs**
- **Never hand out database credentials again**
- **On- and off-board data access to staff in seconds**
- **Allow users to use their standard database tools**
- **Connect across network and directory domains**
- **Monitor, log, block and alert on connection and SQL activity**
- **Easily implement large-scale database credential rolling**
- **Easily secure and access embedded IoT databases**

Your organization doesn't have to sacrifice security at the expense of business productivity. Contact Cirro today to find out how Cirro's data solution combines access controls, data controls and data management features that can:

- **Help any size business operate under any security compliance regime**
- **Reduce the cost of security infrastructure and administration**
- **Improve the agility of your security team to better meet business demands**

CyberSecurity for dummies - check list.

Don’t be a dummy, make sure your organization passes the test.

Identity-based access and data controls

- ☐ Are you using 2-factor for all application access?
- ☐ Are you using 2-factor for all OS server access?
- ☐ Are you using 2-factor for all direct access to databases from all data clients?
- ☐ Do you have access policy rules that lock down service accounts and block/alert on invalid use?
- ☐ Have you removed databases from networks?
- ☐ Are you using identity-based data controls across all data systems?
- ☐ Are you using identity-defined workstations?

Encrypting Sensitive Data

- ☐ Is there transparent database file encryption?
- ☐ Is there transparent data encryption?
- ☐ Are you storing all sensitive data encrypted?
- ☐ Do you use tokenization? Separation of data?
- ☐ Are you enforcing encrypted data connections?

AI Monitoring & Alerts

- ☐ Are you unifying identity-based SQL activity logs?
- ☐ Are there rule-based alerts?
- ☐ Is there an unsupervised AI risk-scoring solution?
- ☐ Do the access policy rules lock down service accounts and block/alert on invalid use?

An Historical Example of Verification Through Language

THE CONCEPT OF ZERO-TRUST or verification been around for a long time, and can be easily explained by way of a quick history lesson of how the Allies turned back Germany in World War II.

Allied soldiers used a very simple and effective test involving the word ‘squirrel’ to identify German spies during World War II. After occupying France, the Germans turned their attention to England, and to the many obstacles in the way of a successful invasion and occupation.

England had all the traditional military defenses in place, including the Royal Air Force, the Royal Navy and sea passages lined with mines. And while Germany developed and revised invasion plans many times, they never invaded England—and it wasn’t just because of England’s formidable perimeter defenses, although that was certainly a deterrent. It was because Germany needed reliable intel in order to successfully carry out their invasion and subsequent occupation, and the Allies were able to stop them from gathering this intelligence.

And here’s where the word ‘*squirrel*’ comes in.

When teams of German spies came ashore to try to infiltrate England and learn what they needed for their invasion plans, they tried to blend into local towns by dressing in Allied uniforms and carrying false papers. The Allies asked all suspected infiltrators to say “squirrel,” a word native German speakers simply cannot pronounce—and spies were immediately identified.

It was this additional layer of security that stopped German spies from accomplishing their mission. This simple identity verification test identified bad actors with nefarious intent from the get-go—a key component to stopping any infiltration at all. And that’s the underlying concept behind zero trust security—never trust, always verify.

Like England’s traditional military defenses, today’s database security—APIs, VPNs, firewalls, and Privilege Access Management software—only protects your database perimeter. But what about hackers who pose as valid users, like German spies did? Or hackers that use stolen credentials, an increasingly common tactic? Traditional perimeter security measures do not check and block access, either from humans or programs. And most, if not all, organizations that are hacked thought they could trust legacy solutions to protect their data.

There are many more real-life examples of how zero-trust security ensures that the right people are accessing the right information, at the right time.

ADDITIONAL INFORMATION

Learn more about how Zero-Trust security truly authenticates who is accessing your data.

Related products, white papers, documentation and blog posts are available at cirro.com