Google Cloud

Zero trust policies and complementary controls

Previously, you learned that many organizations are shifting from traditional perimeter security—like Firewalls, IDS, IPS, and physical security controls—to securing individual resources using the zero trust concept of: "never trust, always verify." This means that every user, device, or system must be authenticated and authorized before accessing any resources or data. As a cloud security professional, you can help implement zero trust policies (ZTPs) using both Cloud Access Security Brokers (CASBs) and Secure Access Service Edge (SASE) platforms. These platforms provide granular access controls, continuous monitoring, and adaptive security policies based on context. With zero trust security measures in place, you can help your organization strengthen its security posture and minimize the potential attack surface.

In this reading, you'll first learn more about zero trust. Then, you'll examine zero trust policies (ZTPs) and network Access Control Lists (ACLs) scenarios.

Zero trust in-depth

Recall that ZTP measures can help an organization strengthen its security, and limit or prevent attacks. Using ZTPs, security teams set resources and data to be inaccessible by default, making it less likely for attackers to gain access to your network. The team only grants users permissions to resources with strict, controlled access after authentication and authorization.

Traditional perimeter security measures and zero trust measures

But why should an organization consider ZTPs over traditional perimeter security? Here is a table that summarizes the key differences between traditional perimeter security measures and zero trust measures:

Characteristic	Traditional perimeter security measures	Zero trust measures
Focus	• Creates a strong barrier between the internal network and the outside world	• Verifies access to resources on a case-by-case basis, regardless of location
Key technologies	• Firewalls • IDS • IPS • Physical security controls	• Identity and access management (IAM) • Multi-Factor Authentication (MFA) • Micro-segmentation • Network Access Control (NAC) • Continuous monitoring with Cloud Access Security Brokers (CASBs) and Secure Access Service Edge (SASE) platforms
Benefits	• Can be relatively simple to implement and manage	• Can provide more comprehensive security and visibility for a large number of users than traditional perimeter security measures
Drawbacks	• Can be difficult to protect against sophisticated attacks • Provide limited protection once an attacker is in the internal network	• Can be more complex to implement and manage than traditional perimeter security measures

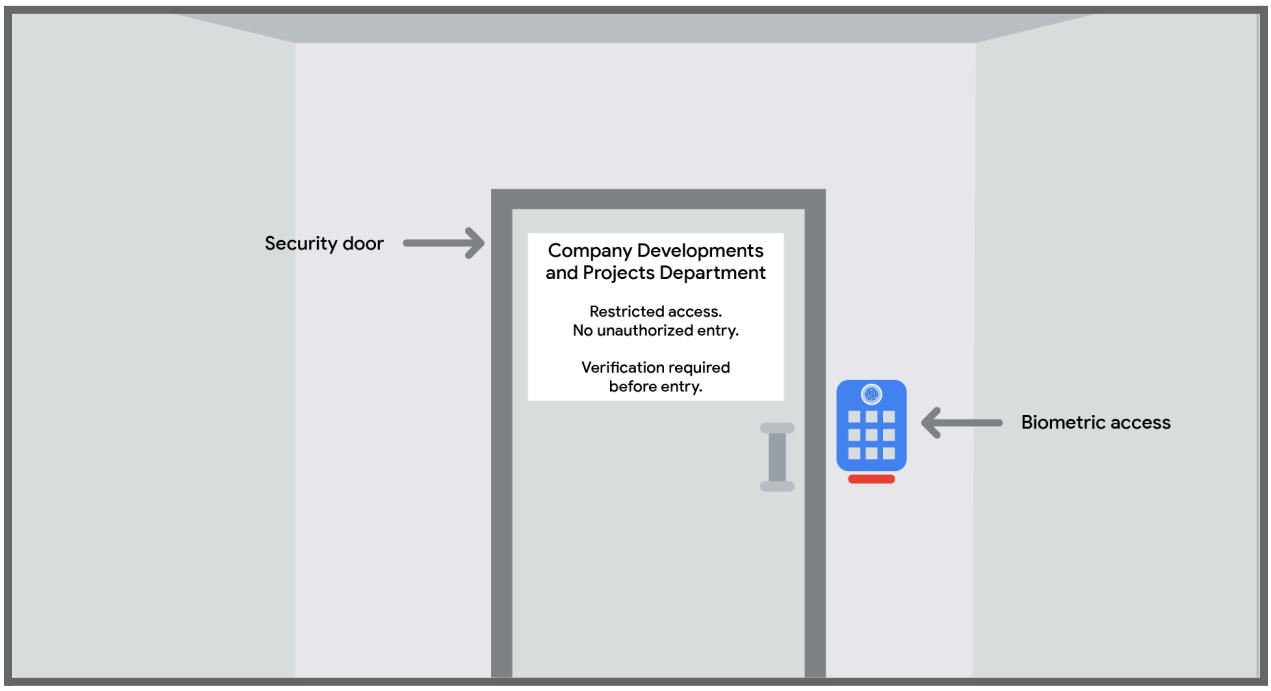
What this table lays out is that zero trust measures are a better fit for larger organizations with complex IT environments and a high volume of remote workers. While zero trust measures can provide more comprehensive security and visibility than traditional perimeter security measures, zero trust measures can also be more complex to implement and manage. Organizations should carefully consider their needs before choosing which approach to take.

ZTP implementation scenario

Organizations can implement zero trust measures in a variety of ways. There is no one-size-fits-all approach. The best approach for an organization will depend on its specific needs and requirements.

Here's an example of a physical representation of zero trust. A company has a building where developers work on highly classified, internal corporate projects. It's vital that no outsiders observe developer work, or catch any part of developer conversations that may give away company secrets to the public. So, the company hires a team to secure the building.

The team installs physical security controls to all access points inside the perimeter of the building, including a security screening machine inside the building's main entry and biometric locks on entry ways into each section of the building. As people enter the building, they must successfully clear the security screening, and then proceed only to the building sections where they have biometric access. The security team sets each person's access based on their business needs and the amount of time they need access to a particular building section. For example, if a visitor goes to the lobby, the cafeteria, or the washroom, they'll have to go through the same biometric access to enter that area of the building again.



Access Control Lists (ACLs)

Remember, you can use ACLs to restrict access to resources in the cloud, ensuring that only authorized users have access to specific data or services, like data in storage account buckets. Also, remember that the “trusted” or “untrusted” sections of a network aren't about the “room” itself, but about the level of protection and the sensitivity of the information within.

ACL implementation scenario

Let’s next check out an example of how to apply effective ACLs. A company’s security team wants to customize access to individual objects within a bucket. The team decides to use ACLs to define who has access to buckets and objects and what level of access they have. The team’s ACLs are made of **entries.** Each **entry** has two bits of information:

- A **permission**, which defines what actions can be performed, like reading or writing
- A **scope**, which defines who can perform actions, like a user or group of users

While the security team can use ACLs to customize individual objects and fine-tune access to individual objects, they also need to use the ACLs in tandem with other methods, like identity and access management (IAM). In other words, the team cannot use ACLs exclusively, since they cannot be set on parent resources or the overall project.

Note: Permissions that IAM policies grant do not appear in ACLs, and permissions ACLs grant do not appear in IAM policies.

Next, the security team continues the implementation to use ACLs to control access to the objects in a bucket. To do this, the team sets the ACLs based on users' needs by granting permissions at the user or group level. For example, the team stores the company's images and files in their public-facing website in a bucket. The website is open to the public, so everyone visiting the site is granted read-only access to the images and files in this bucket. The read-only access enables the images to display correctly. The marketing team is responsible for maintaining the site, so only the marketing team is granted access to upload new images and other files, or replace the old images and other files.

Key takeaways

Zero trust is vital in modern cloud computing. The approach uses the concept of "never trust, always verify." As a security professional, you should only grant access to verified users who need access and only to the specific areas of the infrastructure they need, for as long as they need that access.

While methods like IAM can give you the power to authorize who can access your cloud, or even individual buckets, ACL complements IAM to give you the power to customize access to individual objects within a bucket.