Access controls can be applied in various forms, levels of restriction, and at different places within a computing system. A combination of access controls can provide a system with layered defense-in-depth protection.

**Instructions:**

For the scenarios that follow, identify the data that would need to be protected. Recommend how you would implement one or more of the access controls (listed after the scenarios) for the given scenario and justify your recommendation.

**Scenarios:**

1. Shovels and Shingles is a small construction company consisting of 12 computers that have Internet access.
2. Top Ads is a small advertising company consisting of 12 computers that have Internet access. All employees communicate using smartphones.
3. NetSecIT is a multinational IT services company consisting of 120,000 computers that have Internet access and 45,000 servers. All employees communicate using smartphones and e-mail. Many employees work from home and travel extensively.
4. Backordered Parts is a defense contractor that builds communications parts for the military. All employees communicate using smartphones and e-mail.
5. Confidential Services Inc. is a military-support branch consisting of 14,000,000 computers with Internet access and 250,000 servers. All employees must have security clearances, and they communicate mainly using BlackBerry devices and e-mail.

## 

## Access Controls

## Administrative controls: Policies approved by management and passed down to staff, such as policies on password length.

## Logical/technical controls: Control access to a computer system or network, such as a username and password combination

## Hardware controls: Equipment that checks and validates IDs, such as a smart-card for or security token for multifactor authentication.

## Software controls: Controls embedded in operating system and application software, such as NTFS permissions.

## Physical controls: Control entry into buildings, parking lots, and protected areas, such as a lock on an office door.