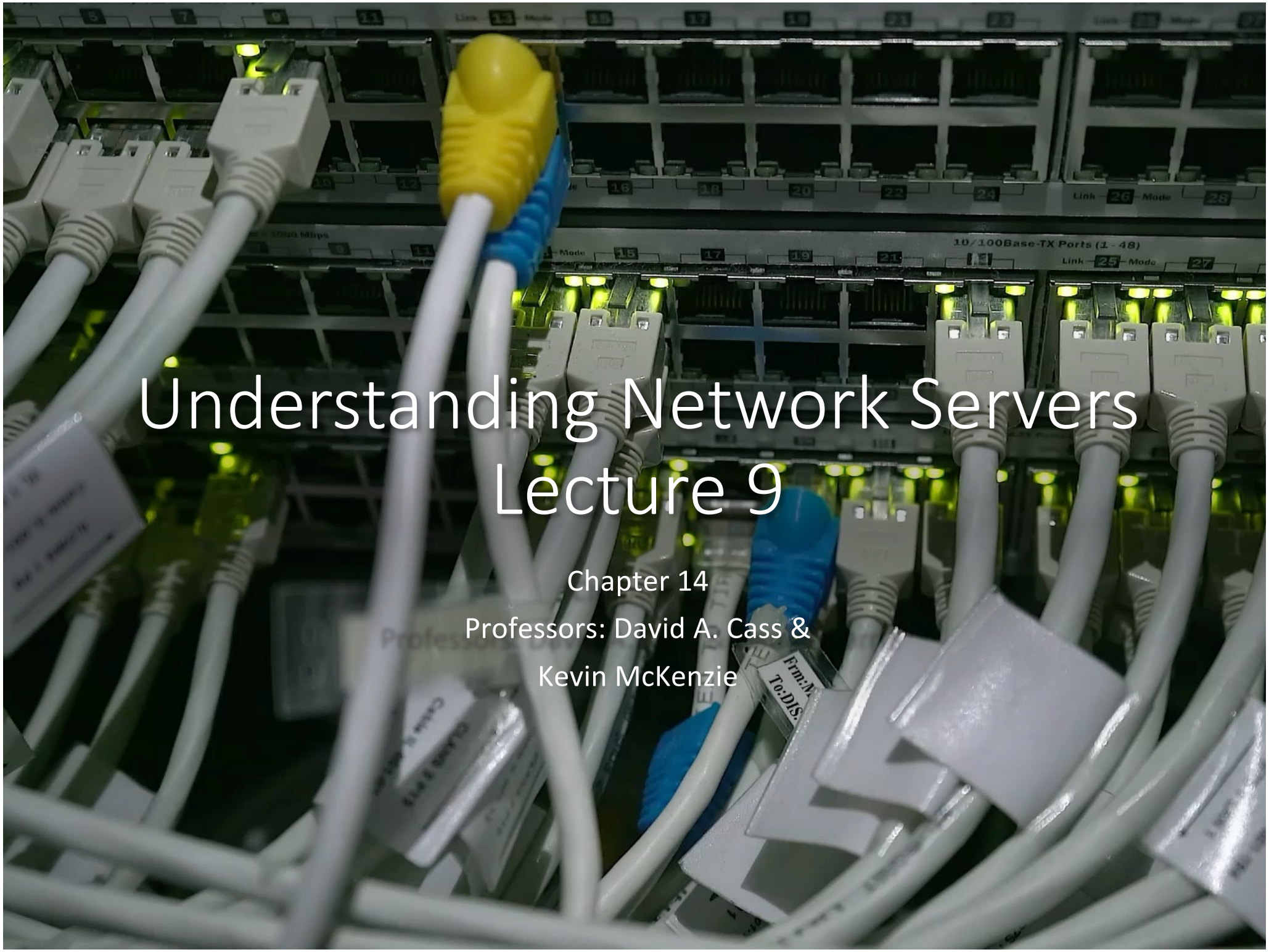


Understanding Network Servers Lecture 9

Chapter 14

Professors: David A. Cass &

Kevin McKenzie

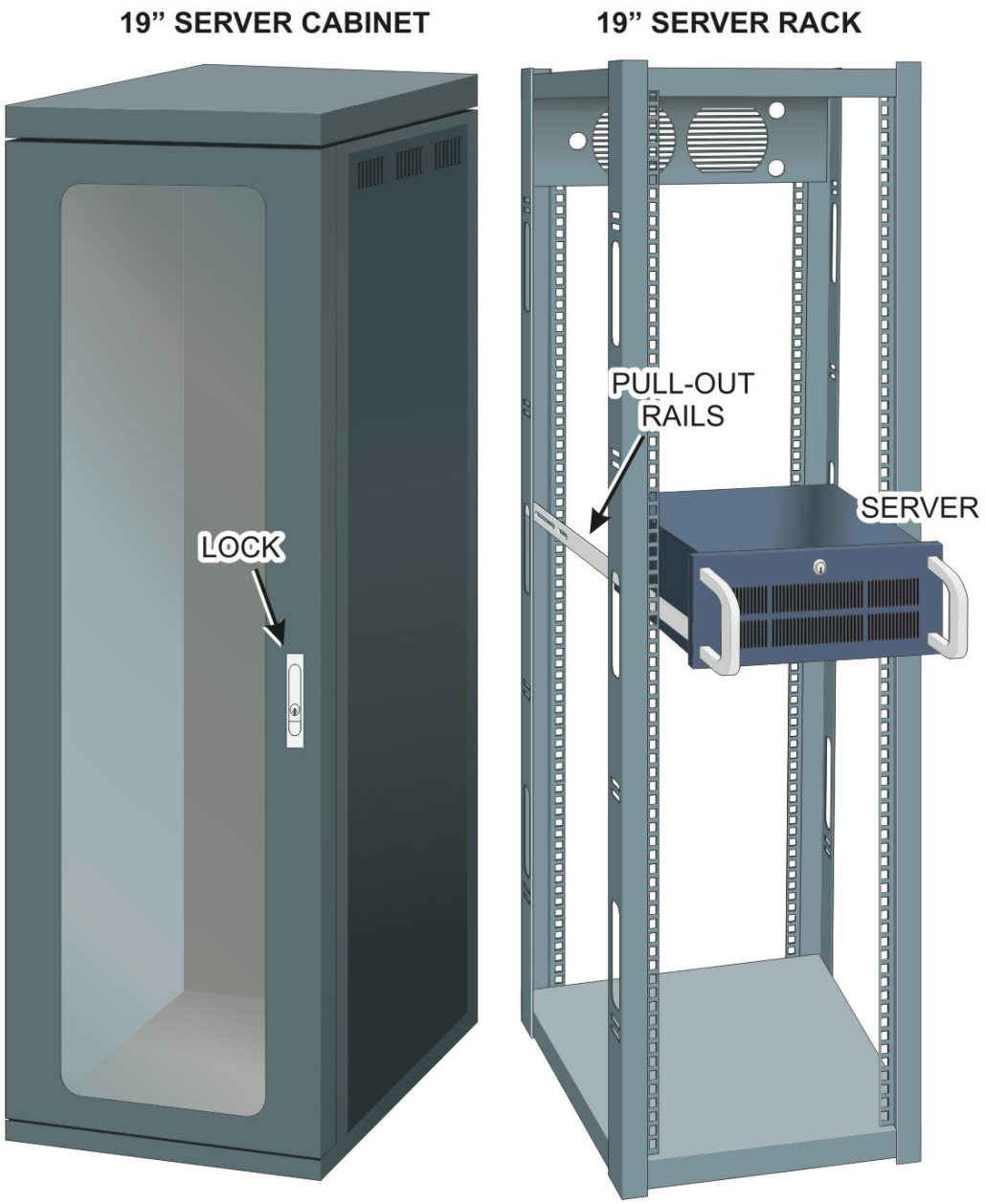
In this chapter, you'll learn to:

- Understand server security
- Understand the role of network administrators
- Understand the importance of server software security
- Understand the two classes of users in a network
- Understand network authentication options

In this chapter, you'll learn to:

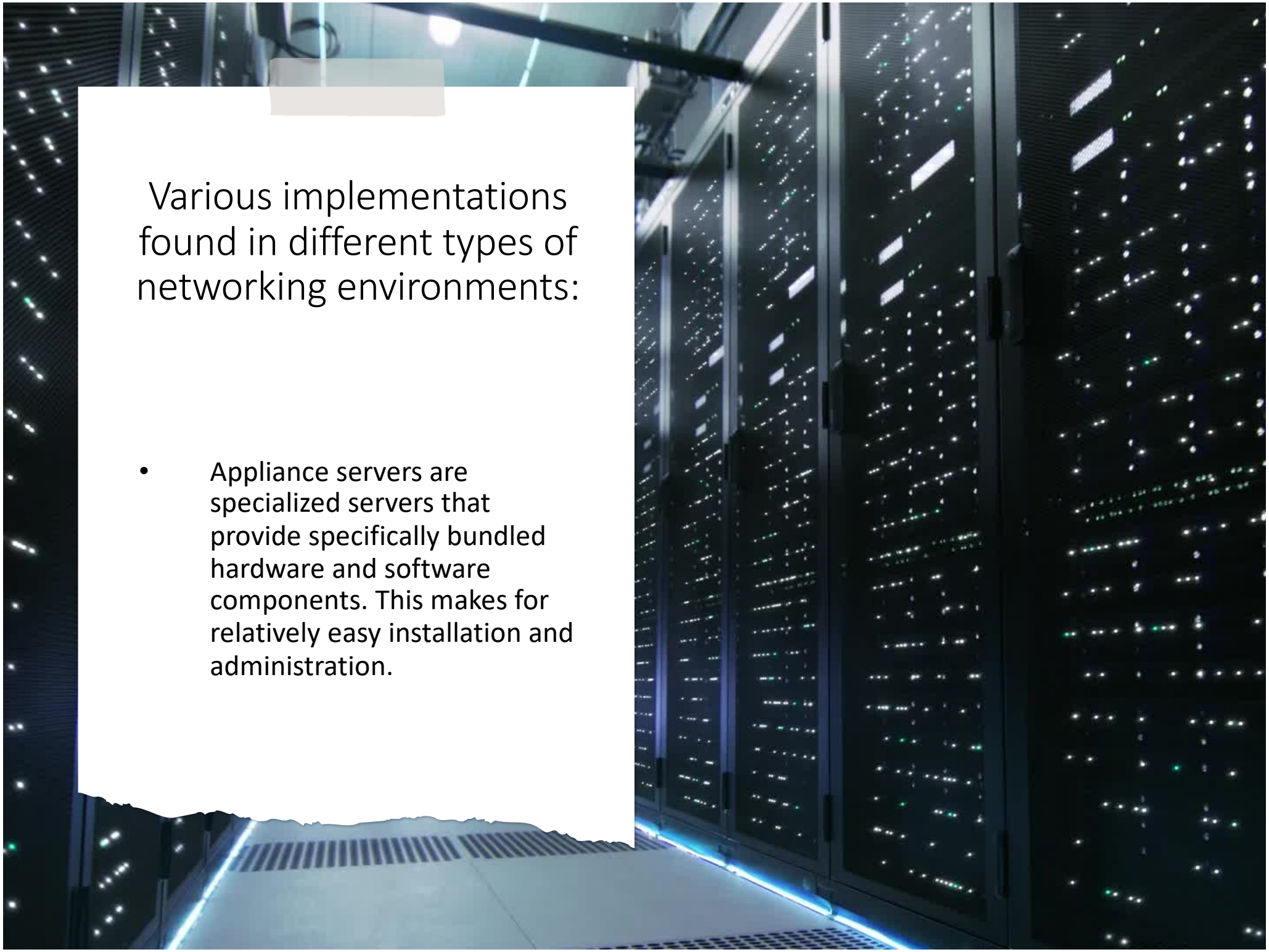
- Understand how to establish resource controls
- Understand how to maintain server security
- Understand how to scan for vulnerabilities

A Typical Rack-Mount Server Cabinet



Various implementations found in different types of networking environments:

- General-purpose servers are employed in most small businesses for multiple purposes such as handling departmental email and providing file, print, and web services running on standard network operating systems.



Various implementations found in different types of networking environments:

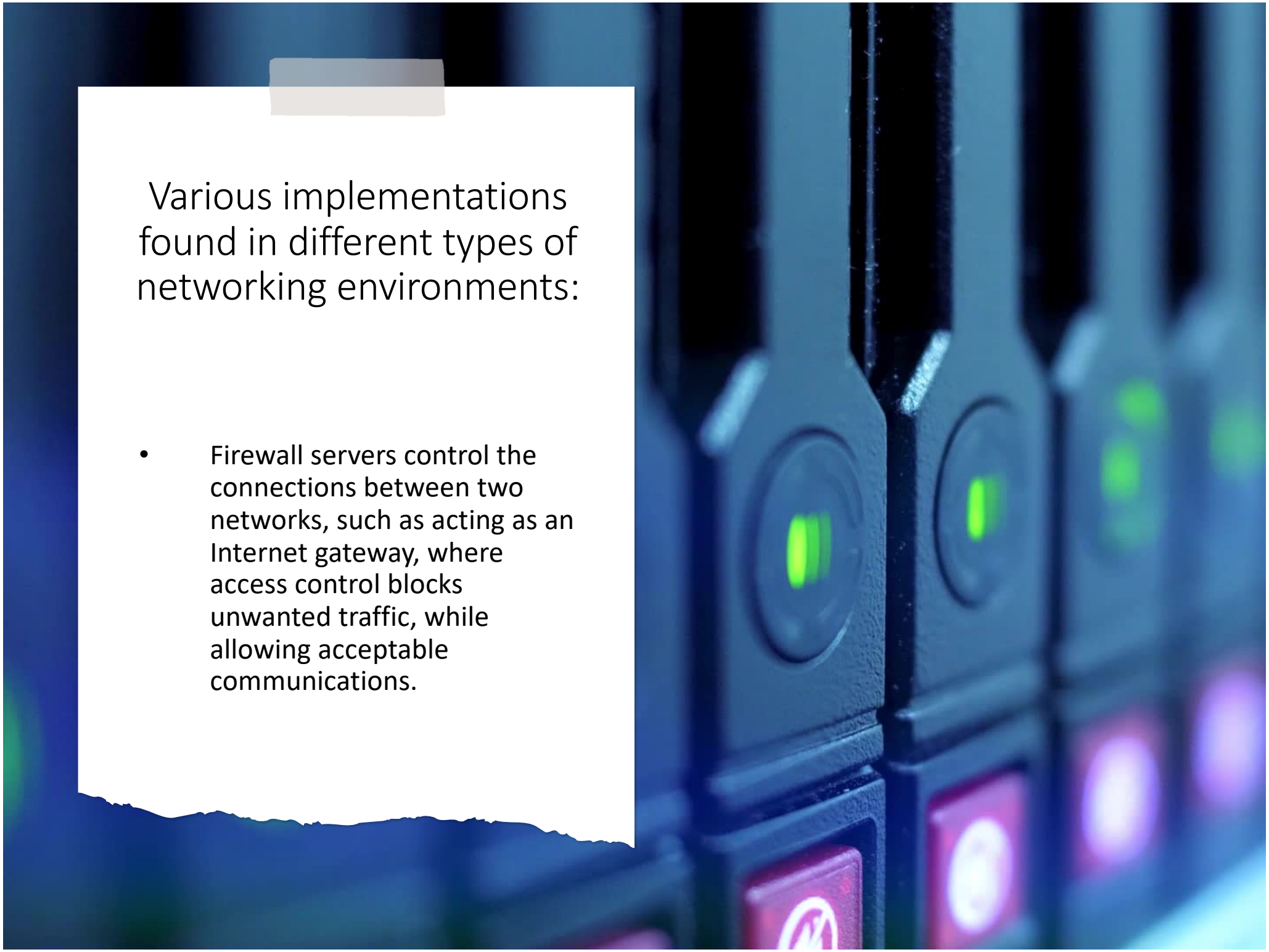
- Appliance servers are specialized servers that provide specifically bundled hardware and software components. This makes for relatively easy installation and administration.

Various implementations found in different types of networking environments:

- Application servers run programs accessed by multiple users, and they often interact with information databases.

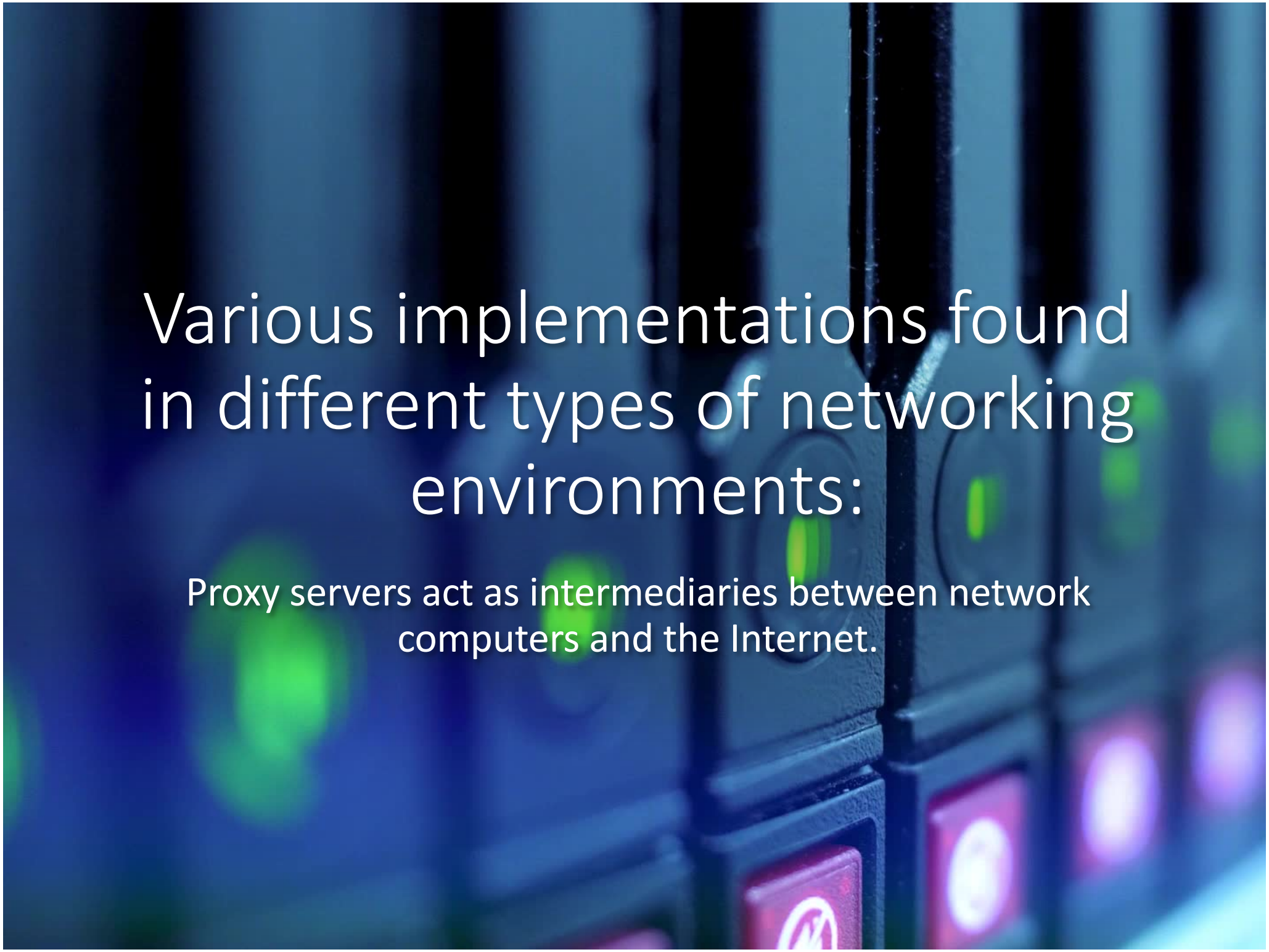
Various implementations found in different types of networking environments:

- Mail servers are client/server types of application servers used to receive and store electronic mail messages in private mailboxes, even when users are not actually logged directly on to the network.



Various implementations found in different types of networking environments:

- Firewall servers control the connections between two networks, such as acting as an Internet gateway, where access control blocks unwanted traffic, while allowing acceptable communications.



Various implementations found in different types of networking environments:

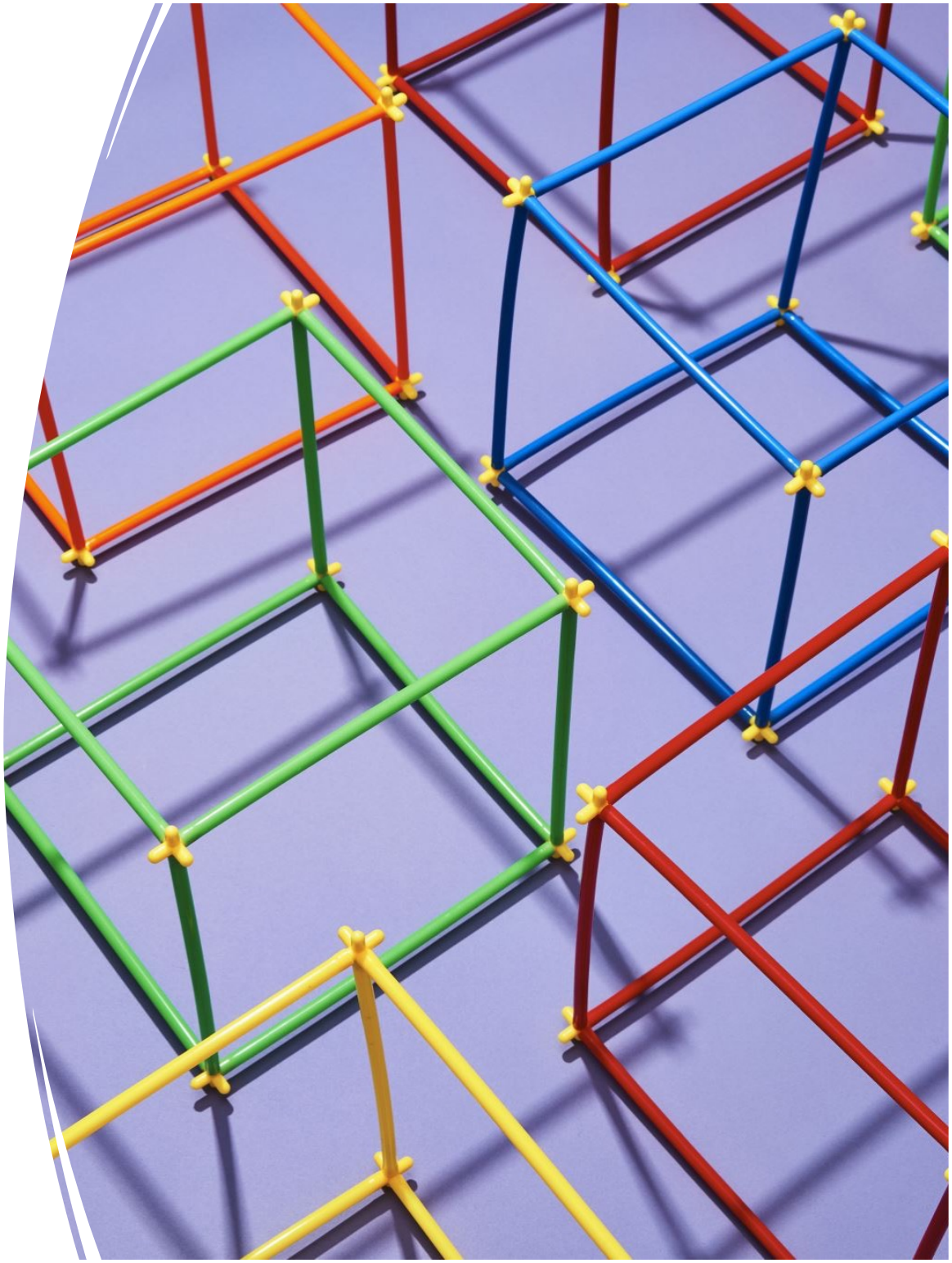
Proxy servers act as intermediaries between network computers and the Internet.

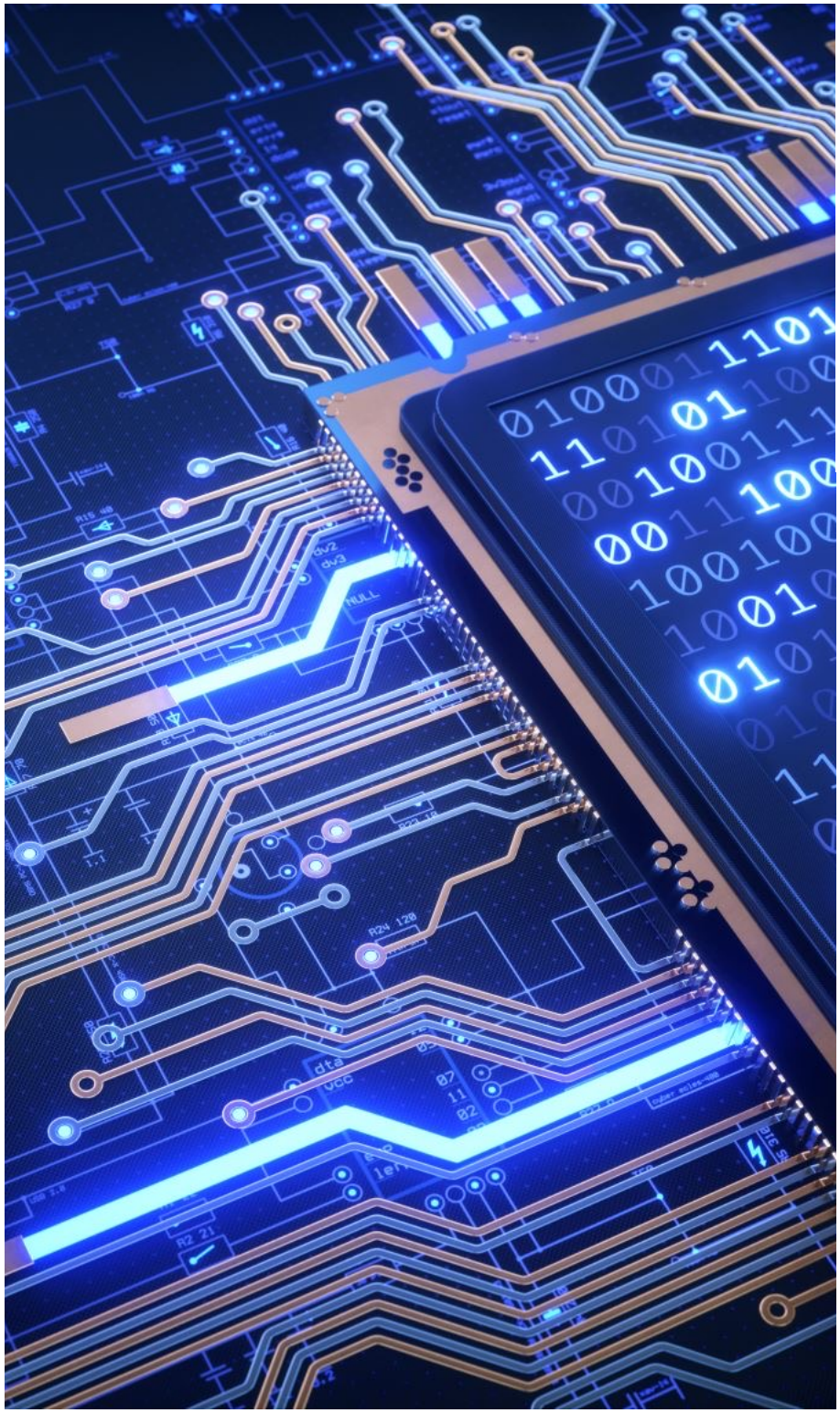
Various implementations found in different types of networking environments:

- Web servers host web pages for intranet and/or Internet access, and can be configured to host more than one site, depending on the server's underlying OS.

Various implementations found in different types of networking environments:

- Database servers are used to store and process data in response to client queries, where organizations must manage large quantities of data.





Various implementations found in different types of networking environments:

- Terminal servers are special-purpose computers fitted with multi-ported asynchronous modem connections, as well as ports designed to interface with hast machines acting as terminals on one side and with a LAN on the other side.

Various implementations found in different types of networking environments:

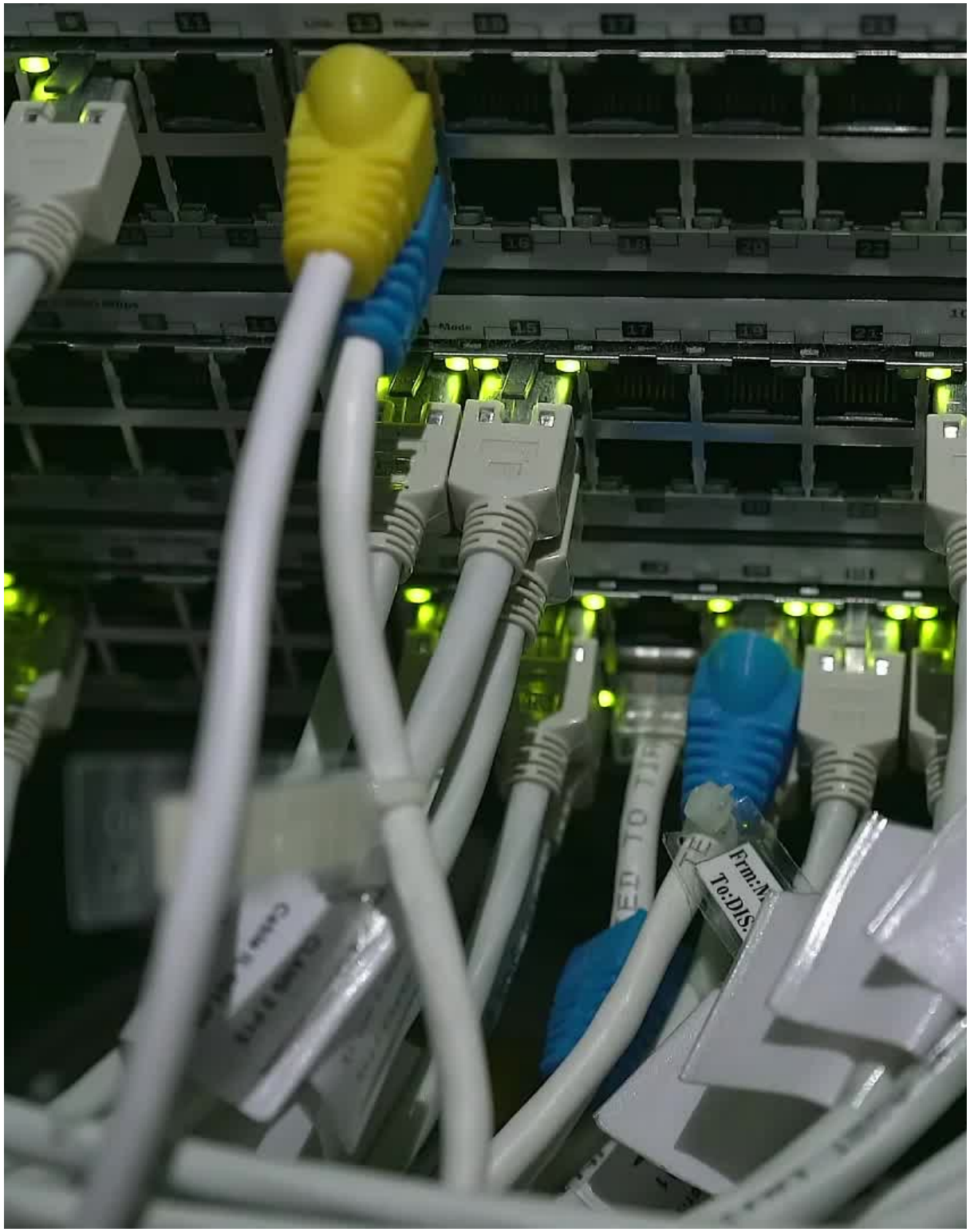
- DNS (Domain Name Service) servers contain database listings used to resolve human-readable computer names to IP addresses.

Various implementations found in different types of networking environments:

- Gateway servers provide interfacing between different types of networks, protocols, or mechanisms to provide access to another system.

Various implementations found in different types of networking environments:

- Router servers manage the shared resources of all other routers in the network, as well as the various transmission speeds and different protocols being used within an organization’s network.

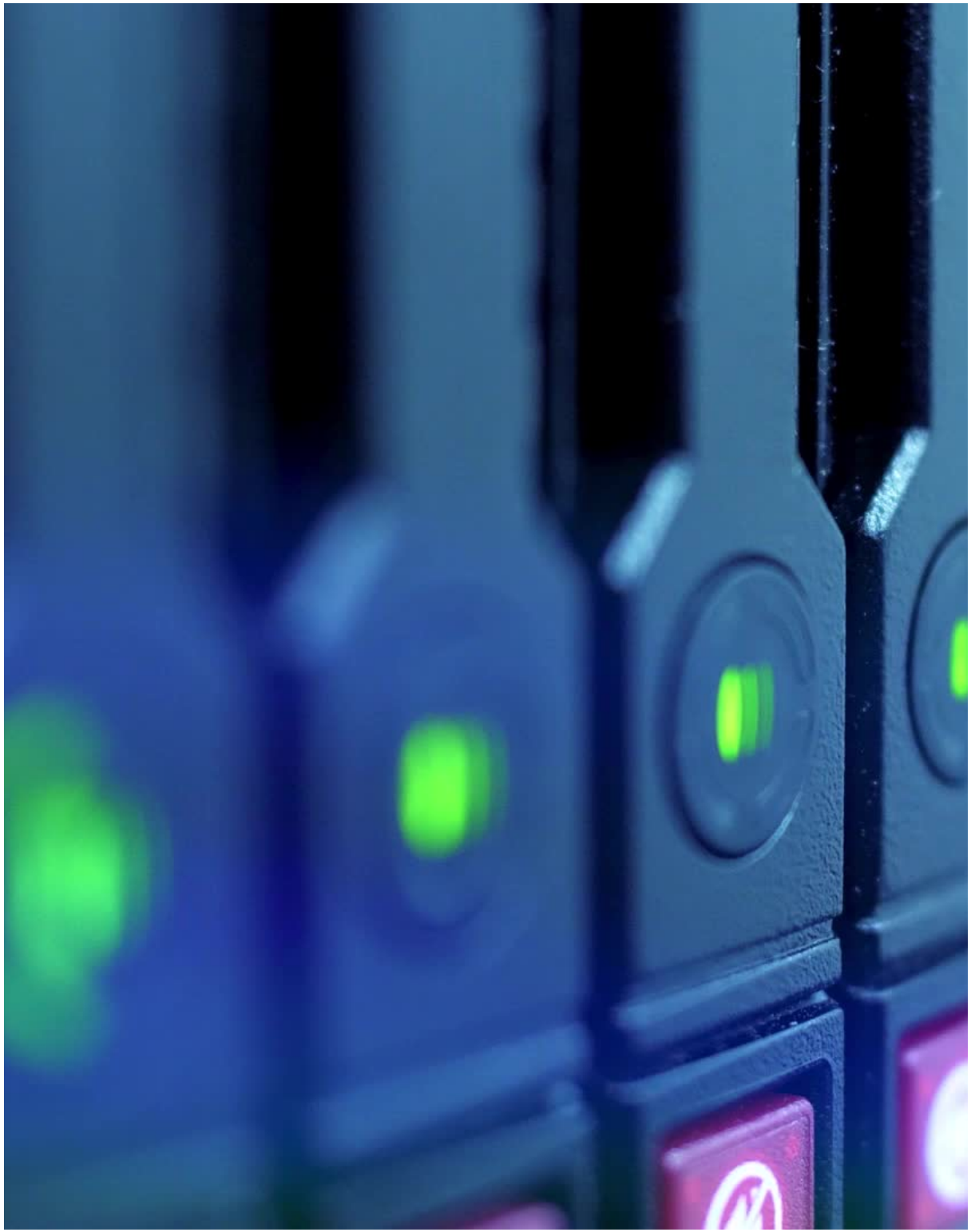


Various implementations found in different types of networking environments:

- Bridge servers use multiple network interfaces to connect groups of computers. They translate between protocols and help to reduce network traffic.

Various implementations found in different types of networking environments:

- FTP (File Transfer Protocol) servers transfer files across the Internet, an extranet, or an intranet through the use of FTP client software.



Various implementations found in different types of networking environments:

- NAS (Network Attached Storage) servers move storage out from behind the file server and put it directly on the transport network, permitting any network user with access rights to directly access stored NAS data.

Various implementations found in different types of networking environments:

- SAN (Storage Area Network) servers operate in enterprise storage environments with disk array controllers and tape libraries attached. They are capable of providing large-scale data protection and retrieval.

Various implementations found in different types of networking environments:

- RAS (Remote Access System) servers allow clients to dial in to a computer from a remote site, even if they are not connected to a LAN.

Various implementations found in different types of networking environments:

- Print servers help to decrease the administrative and management workload by streamlining both local and remote printer control.

Various implementations found in different types of networking environments:

- DHCP (Dynamic Host Configuration Protocol) servers are used to temporarily assign dynamic IP addresses to both network workstations and Internet clients.

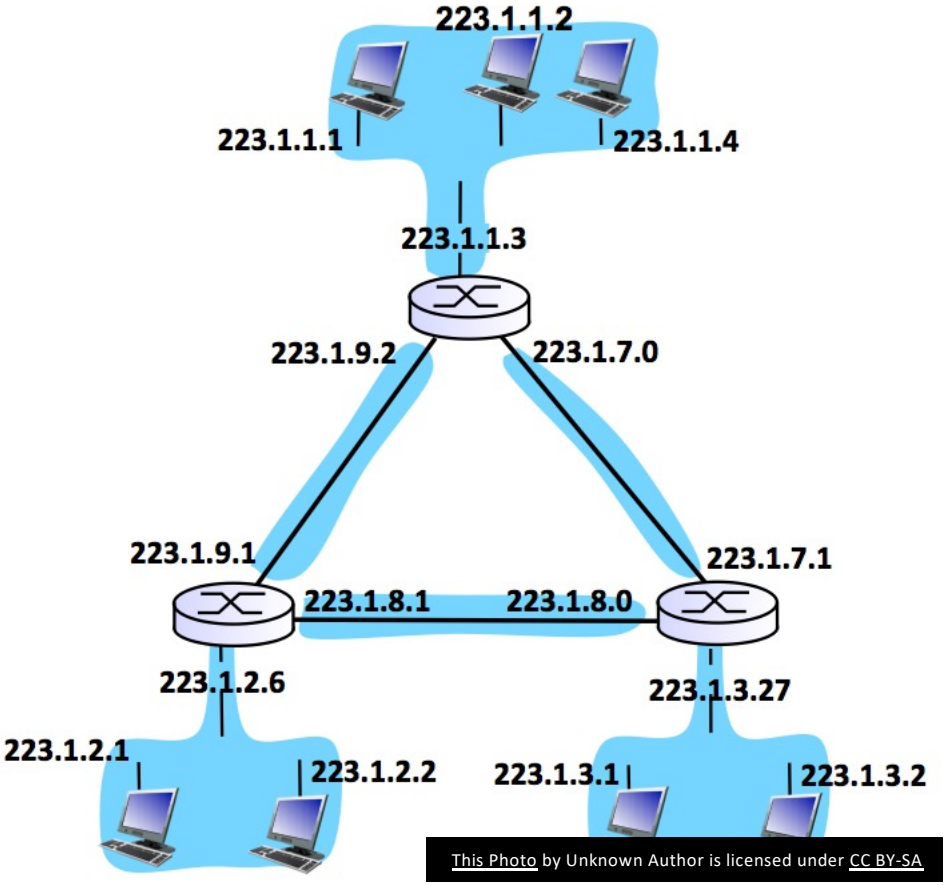
Servers require special consideration and placement

- Access to a server's shared resources should be limited to those users who have both a need and the proper authorization to gain such access. Controls must be in place to make sure that unauthorized employees do not gain access to confidential materials.

Servers require special consideration and placement

- Network access to some types of servers should typically be protected by one or more firewalls that limit traffic to the server.

Servers require special consideration and placement



- Subnets or routers should be used to create secure network segments or zones for different types of servers. For example, a given department, such as the accounting department, may be protected within their own secure subnet and possess their own departmental server resources.

Servers require special consideration and placement

- Because servers are frequently employed for user authentication, the server’s password should be hashed (encrypted) as a preventative measure.

Servers require special consideration and placement

- Critical server resources should be audited periodically to identify potential problems before they escalate into real problems.

System's administrators are generally responsible for

- Installing, configuring and maintaining the servers and network components in compliance with the organizational security policies

System’s administrators are generally responsible for

ESTABLISHING AND MAINTAINING USER AND GROUP ACCOUNTS AS NEEDED

IMPLEMENTING AUTHENTICATION OPTIONS

PERFORMING SYSTEM MAINTENANCE ACTIVITIES IN A SECURE MANNER

CONDUCTING TIMELY SYSTEM BACKUP AND SOFTWARE UPDATING OPERATIONS

System’s administrators are generally responsible for

ENABLING SYSTEM AUDITING AND EVENT LOGGING

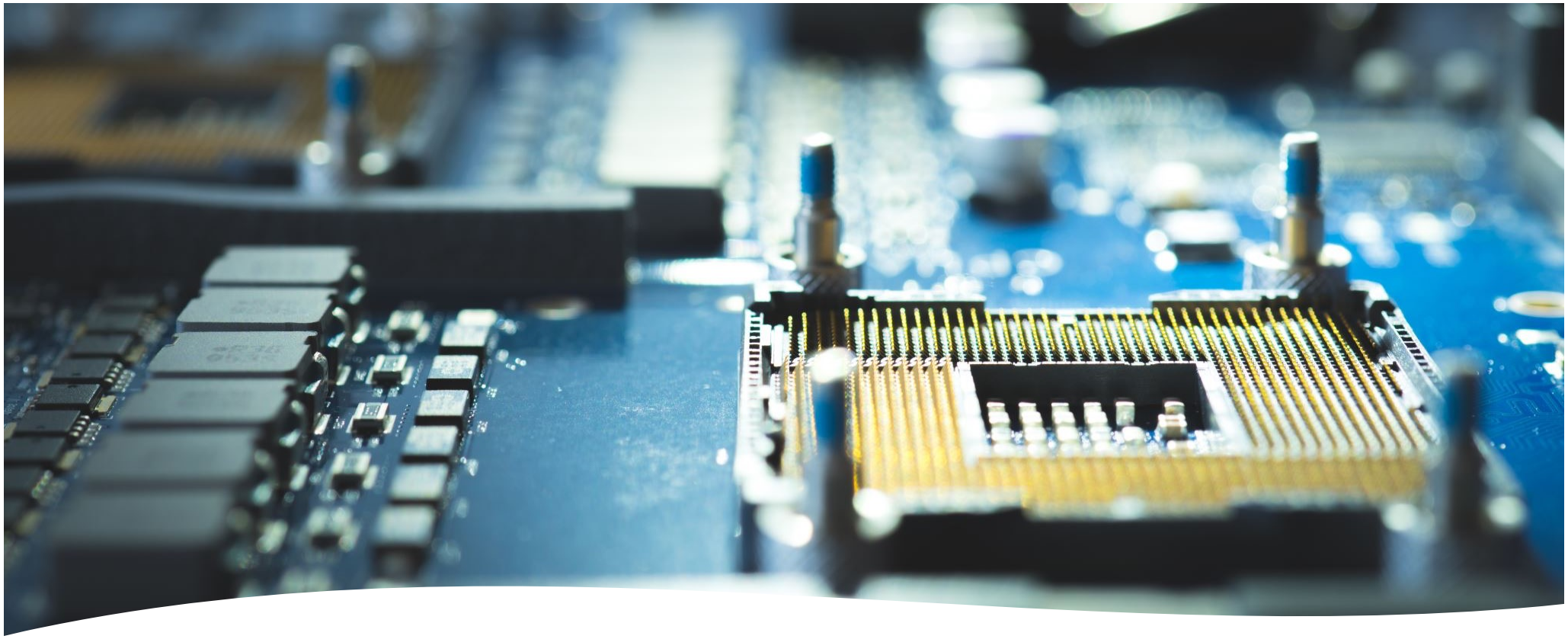
USING INTRUSION DETECTION AND AUDITING TOOLS TO MONITOR NETWORK INTEGRITY, PROTECTION LEVELS, AND SECURITY-RELATED EVENTS

ESTABLISHING FIREWALL SETTINGS

System’s administrators are generally responsible for

Establishing and implementing malicious-software protection policies

Following up on detected security anomalies associated with their information system resources



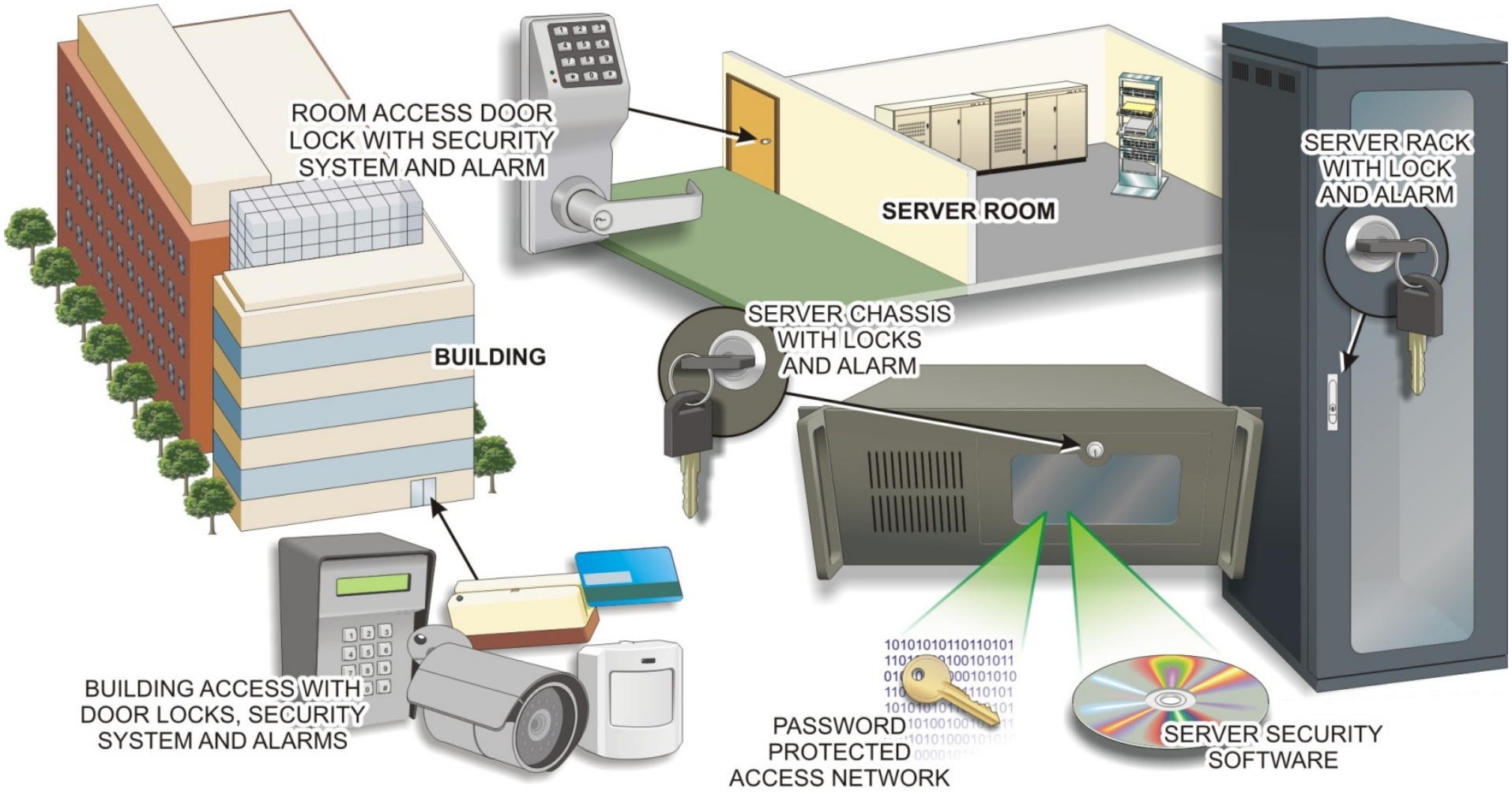
System's administrators are generally responsible for

- Using vulnerability scanning and penetration testing tools to conduct security tests on the network and its components as required

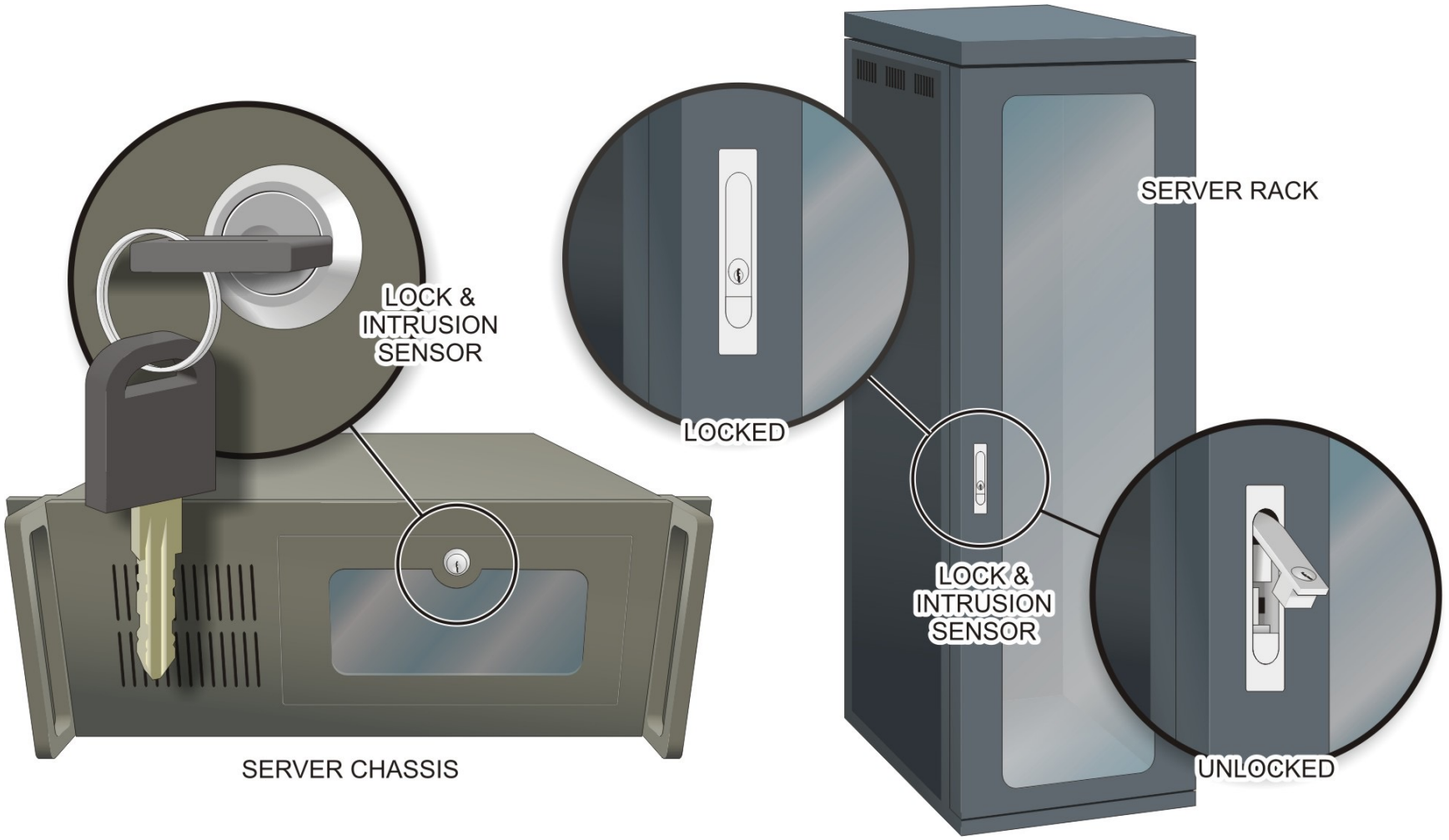
Alternatives to Separate or Centralized Server Rooms

- Reasonable alternatives to a separate or centralized server room include using a locked cabinet or even using a secure rack.

Server Security Points

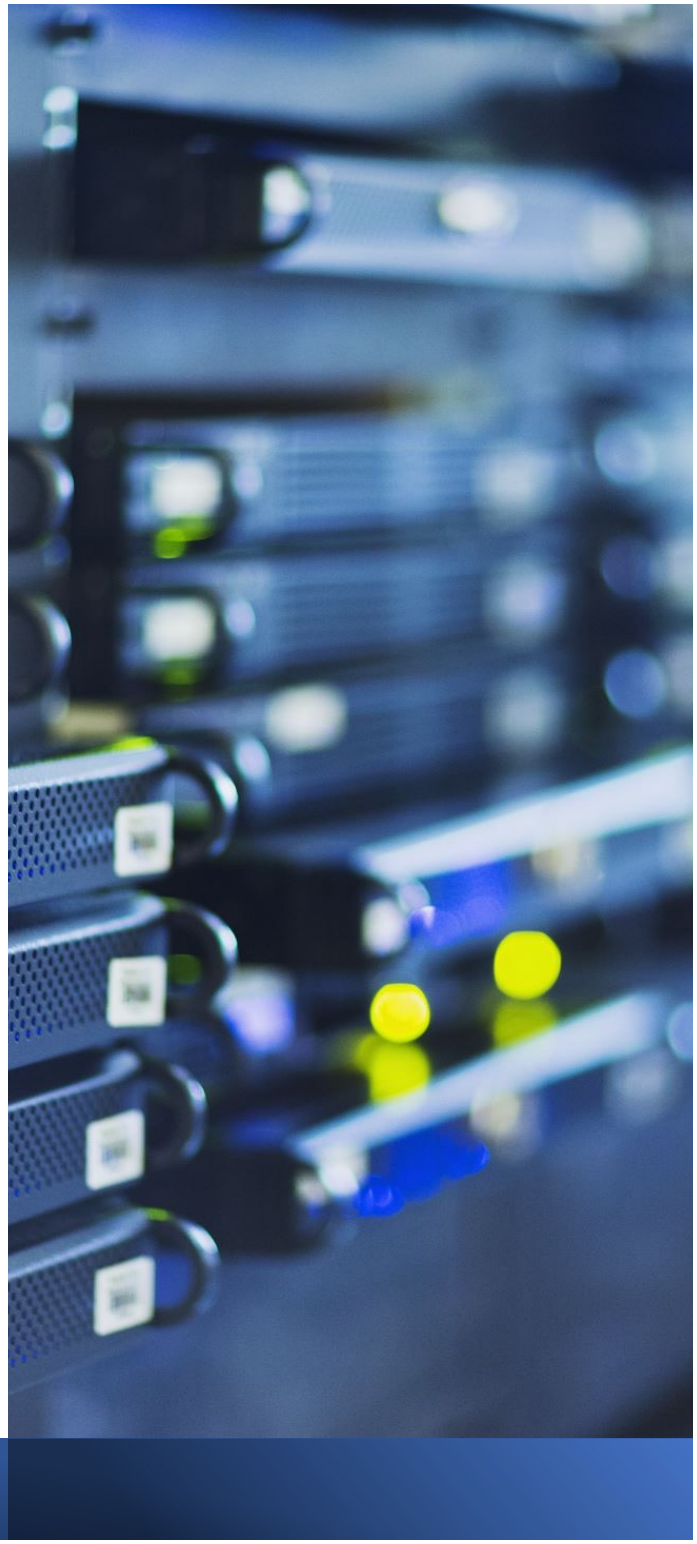


Locking Server Chassis



Securing the operating system

1. Install the server operating system using the manufacturer's installation guidelines.

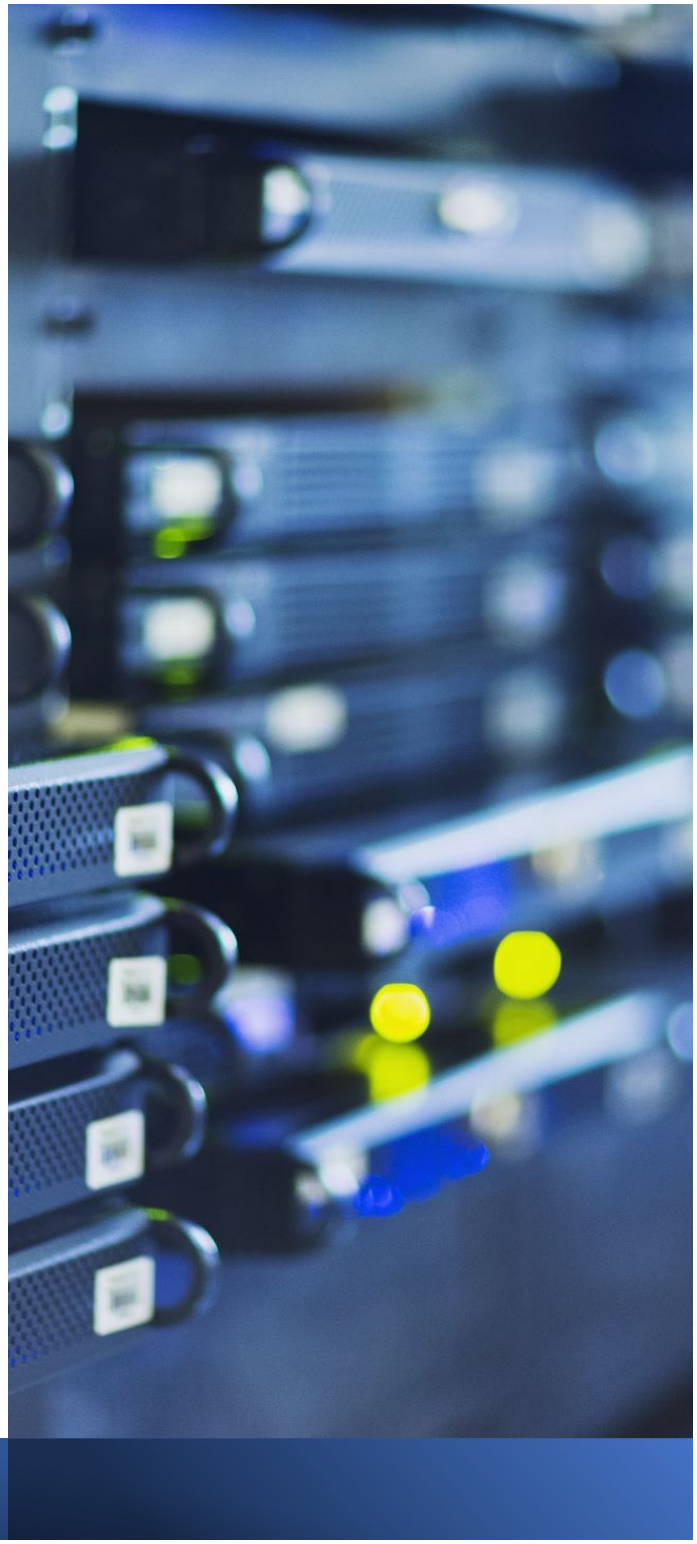


Securing the operating system

2. Patch and update the new installation. The operating system creator cannot know the full security requirements for a given organization's servers. In addition, new security threats are created every day, so there are security gaps that exist between when the software was created and when it is installed. Applying patches and updates to the new install before it is put into operation should correct any known current vulnerabilities.

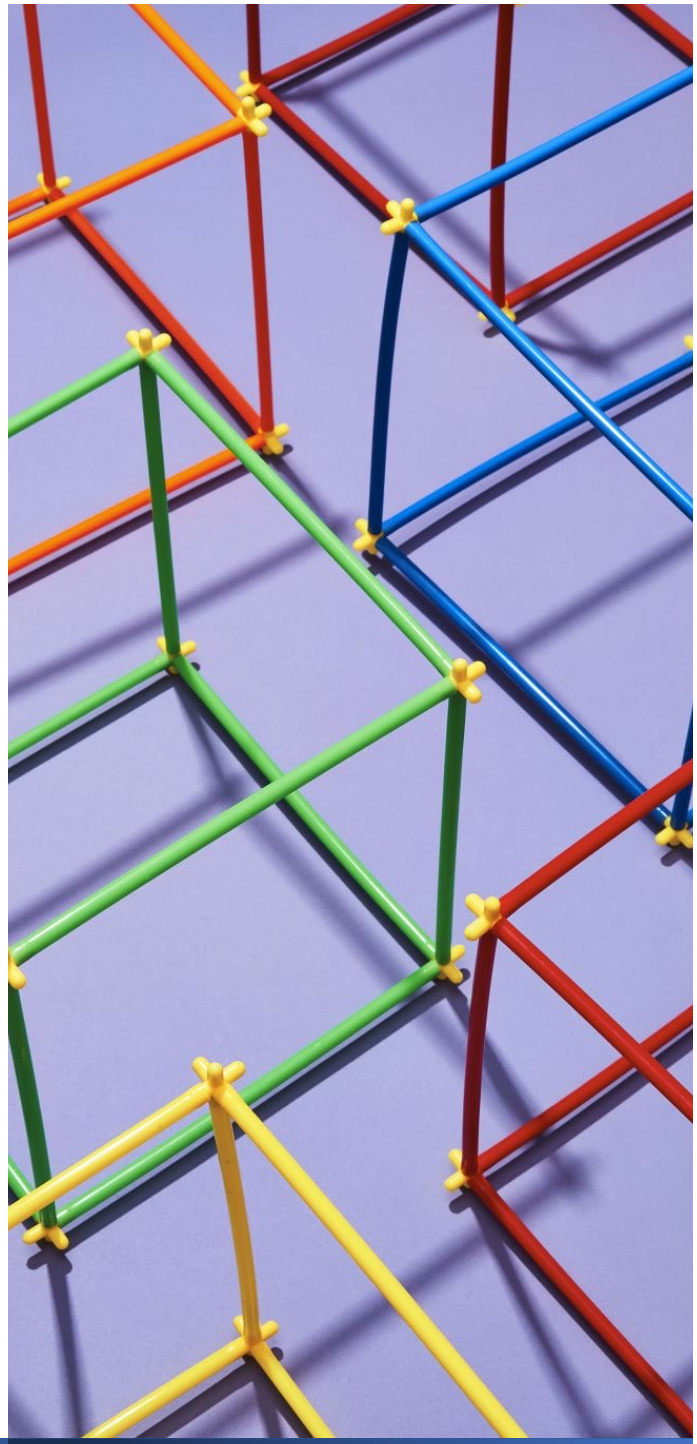
Securing the operating system

3. Configure and harden the new operating system to implement the organization's security policies.



Securing the operating system

4. Install and configure any additional third-party security controls required to address the organization's security policies.



Securing the operating system

4. This step includes installing and configuring network protection systems:
    - Installing Rootkit detectors
    - Installing host (server)-based IDPS software
    - Installing and configuring host (server)-based firewalls
    - Installing or configuring disk encryption software to protect the stored data from attackers that gain physical access to the server.

Securing the operating system

5. Test the security of the new installation to ensure that it addresses all of the organization's security issues. This step involves using vulnerability scanning and penetration detection tools to test the server's security capabilities. This particular step should be performed periodically throughout the life cycle of the server to ensure that its security capabilities remain acceptable.

Configuring/Hardening Server Operating Systems

1. Map the network topology the server will serve and determine what devices are attached to it. Include a detailed record for each local device on its network along with a list of its operating system version, who should have authorized access to it, expected times of operation, and expected network connections.

Configuring/Hardening Server Operating Systems

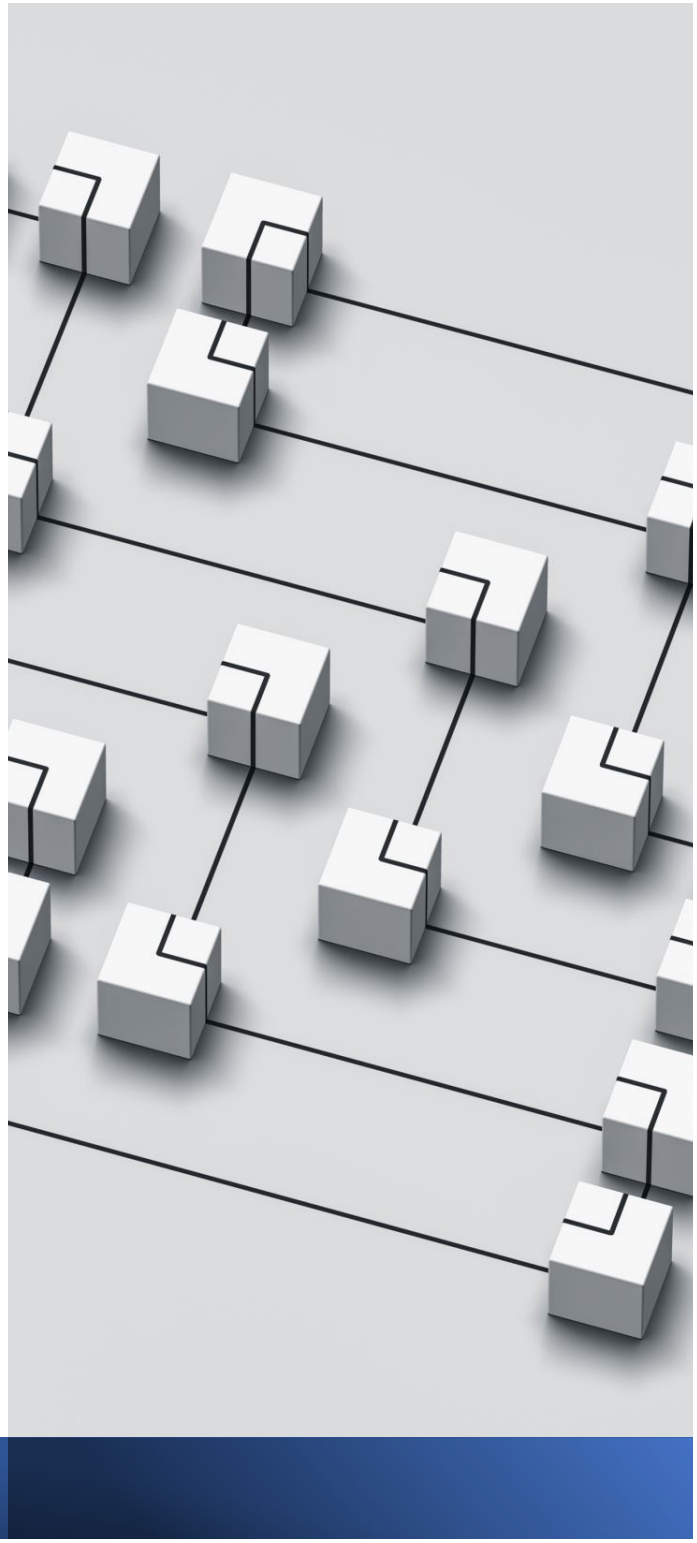
2. Compare the level of security provided by the operating system with the needs of the organization. Particularly look for open services running on the different servers to determine whether those services are needed. Turn off services that are not needed or not being used on the network.

Configuring/Hardening Server Operating Systems

3. Compare the security needs of the organization's users with the capabilities of the operating systems in use.
    - Ensure that the network's operating system is running the most current updates and support available.
        - Antivirus software
        - Anti-malware products
        - Anti-spyware software

Configuring/Hardening Server Operating Systems

3. Compare the security needs of the organization's users with the capabilities of the operating systems in use.
    - Configure Admin and User authentication systems.
        - Rename the default administrator account.
        - Remove or disable any unused default or user accounts, along with their existing authentication settings (usernames and passwords).

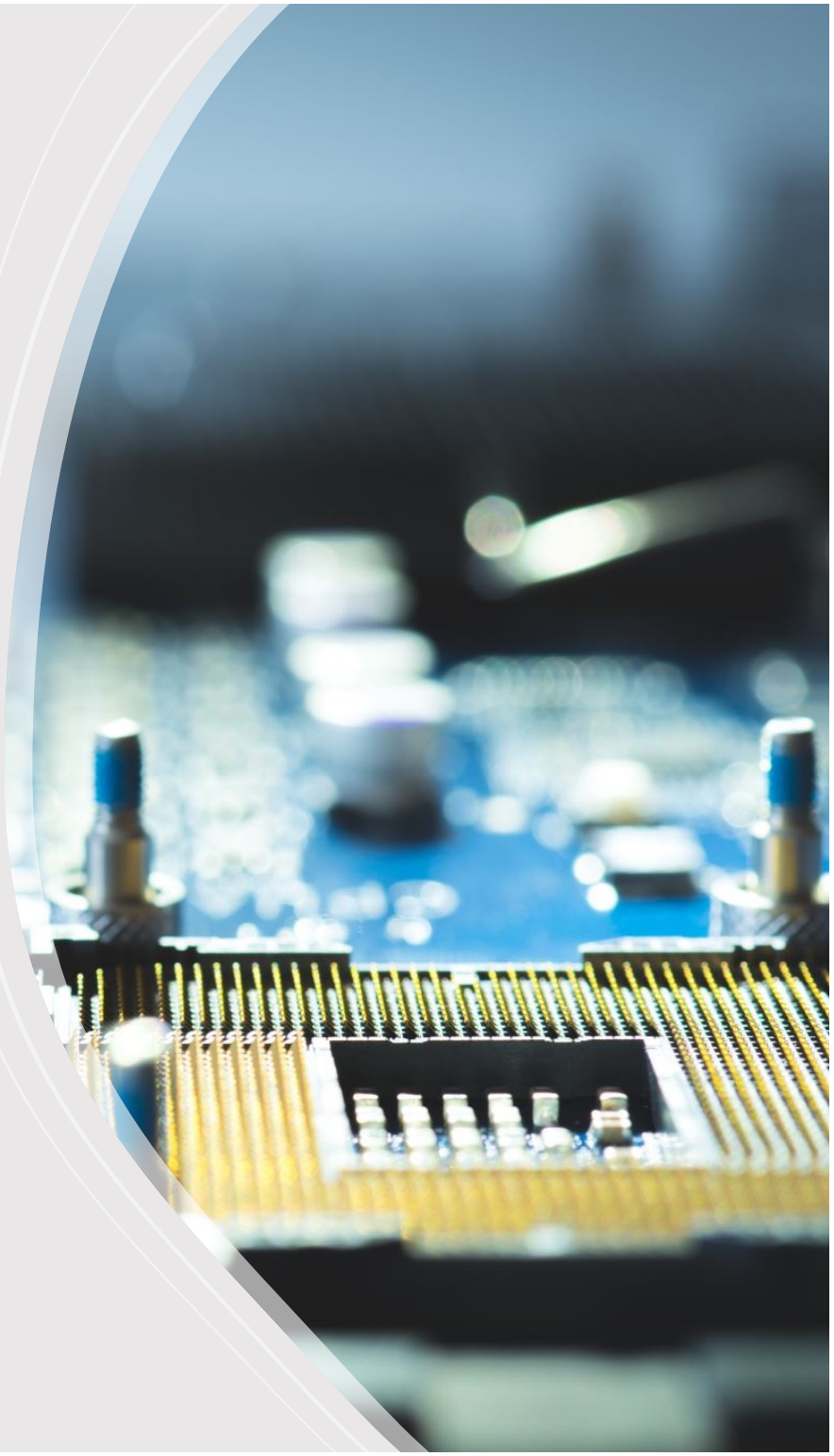


Configuring/Hardening Server Operating Systems

3. Compare the security needs of the organization's users with the capabilities of the operating systems in use.
   - Configure resource controls as required.

A Word of Caution Before Disabling Any Default Services

- Before disabling any default services on a server, verify that the service and any dependencies related to it are not required by different network users.



Configuring/Hardening Server Operating Systems

4. Employ the principle of least privilege to provide services and access permissions to network users. Typical steps involved in this process include:
    - Removing any unnecessary software packages or utilities from the server including remote access programs, language compilers and development tools, along with any system and network development tools.

Configuring/Hardening Server Operating Systems

4. Employ the principle of least privilege to provide services and access permissions to network users. Typical steps involved in this process include:
   - Removing or stopping unnecessary services, applications, and protocols.
     - File and print-sharing services functions
     - Wireless networking services
     - Directory services
     - Email services

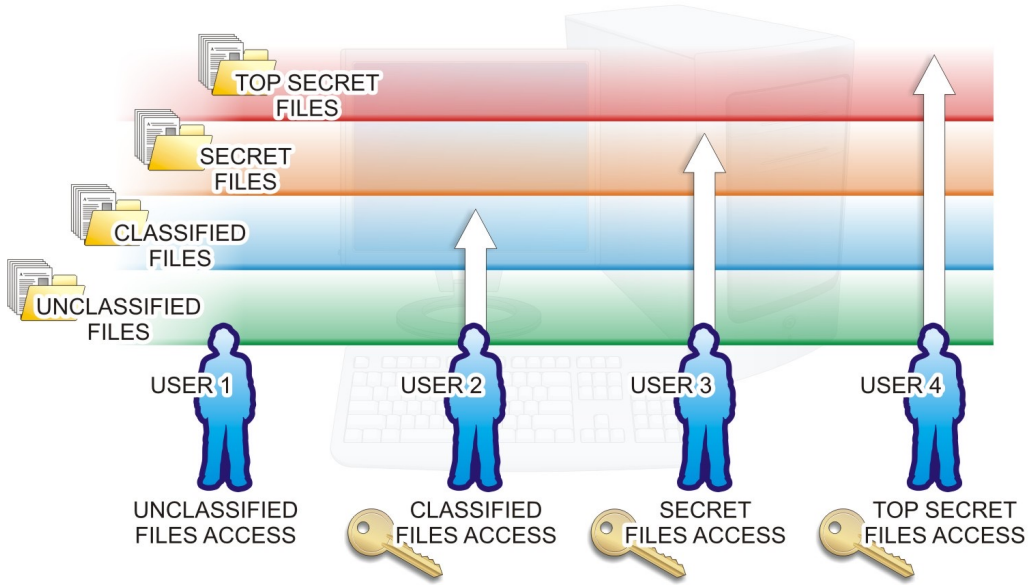
Configuring/Hardening Server Operating Systems

4. Employ the principle of least privilege to provide services and access permissions to network users. Typical steps involved in this process include:
   - Closing any open TCP/UDP network ports.

Three Standard Network Access Control Strategies

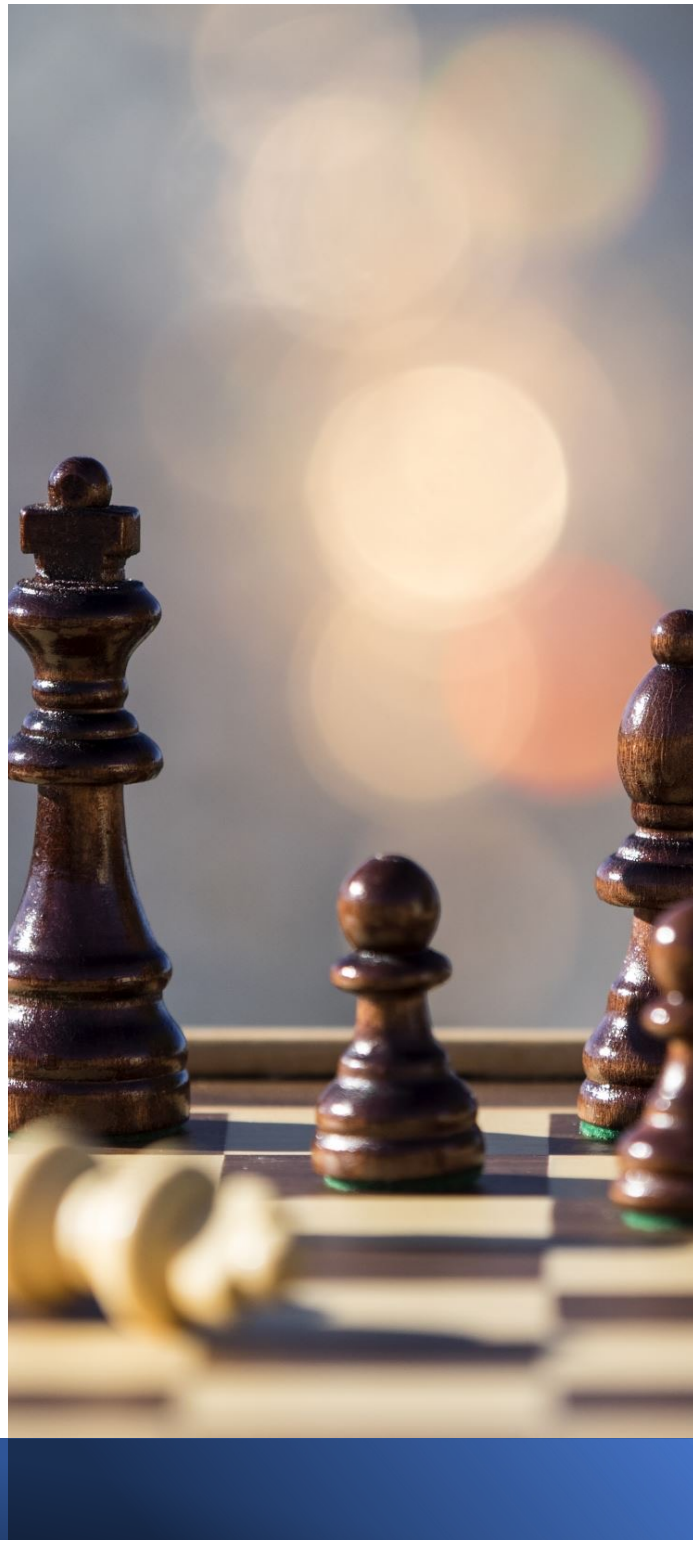
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Non-Discretionary, Role-Based Access Control (RBAC)

Mandatory Access Control

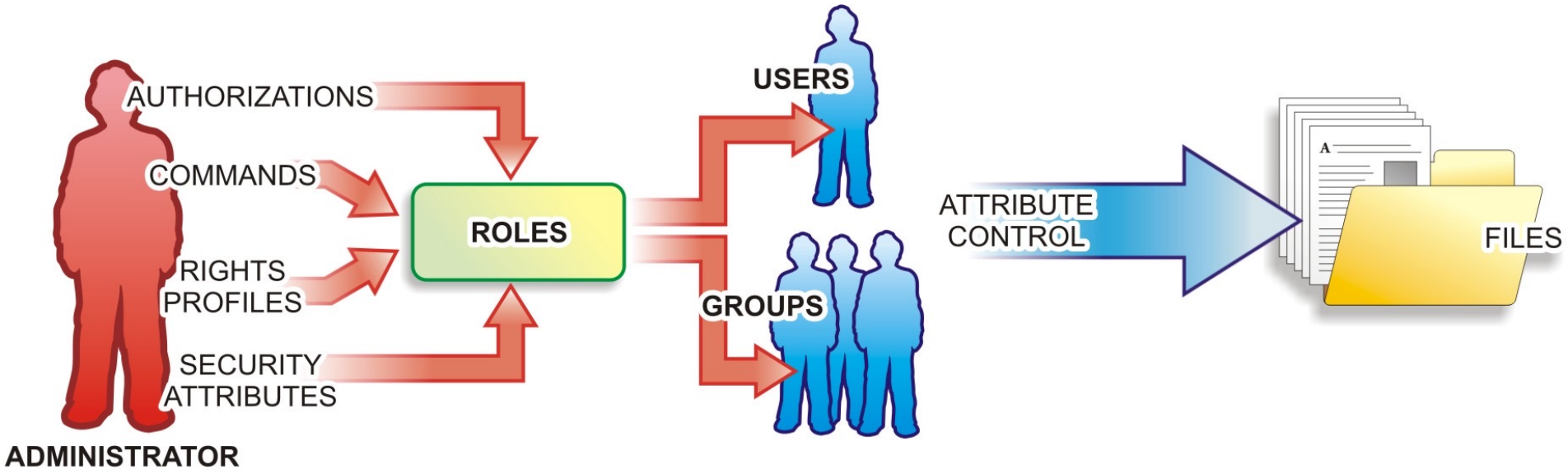


The Fourth Access Control Method Rule-Based Access Control

- There is a fourth access control method called *Rule*-Based Access Control, also known as *automated provisioning*. In this method, a rule is the basic element of a role. The rule defines what operations the role can perform.



Role Based Access Control

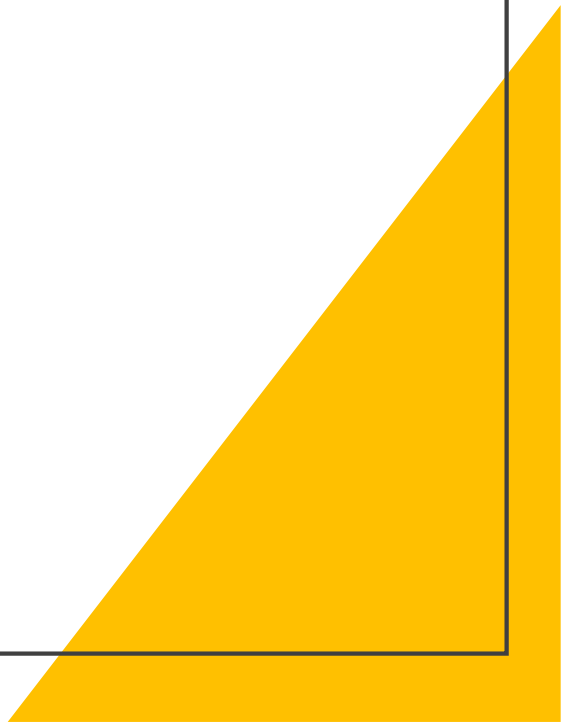


RBAC Rights and Permissions

Individual Rights			Group Membership			Other/Nonmember		
Read	Write	Execute	Read	Write	Execute	Read	Write	Execute
0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	0	0	1
0	1	0	0	1	0	0	1	0
0	1	1	0	1	1	0	1	1

In the following sample (File A)

- Individual owner can read, write, and execute the file.
- Group members can read and write the file.
- All others can only read the file.



File A

Individual Rights			Group Membership			Other/Nonmember		
Read	Write	Execute	Read	Write	Execute	Read	Write	Execute
1	1	1	1	1	0	1	0	0

In the following sample (File B)

- Individual owner can read and write to the folder.
- Group members can only read the folder contents.
- All others are denied access to the folder.

File B

Individual Rights			Group Membership			Other/Nonmember		
Read	Write	Execute	Read	Write	Execute	Read	Write	Execute
1	1	0	1	0	0	0	0	0

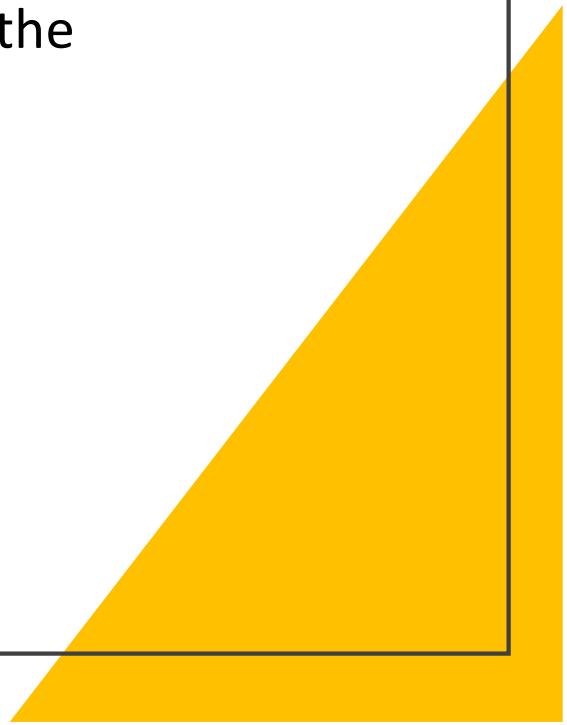
Classes of users in a network

IN LOCAL ACCOUNTS, DATABASES LOCATED ON THE INDIVIDUAL CLIENT DEVICES

IN NETWORK ACCOUNTS, DATABASES LOCATED ON NETWORK SERVERS

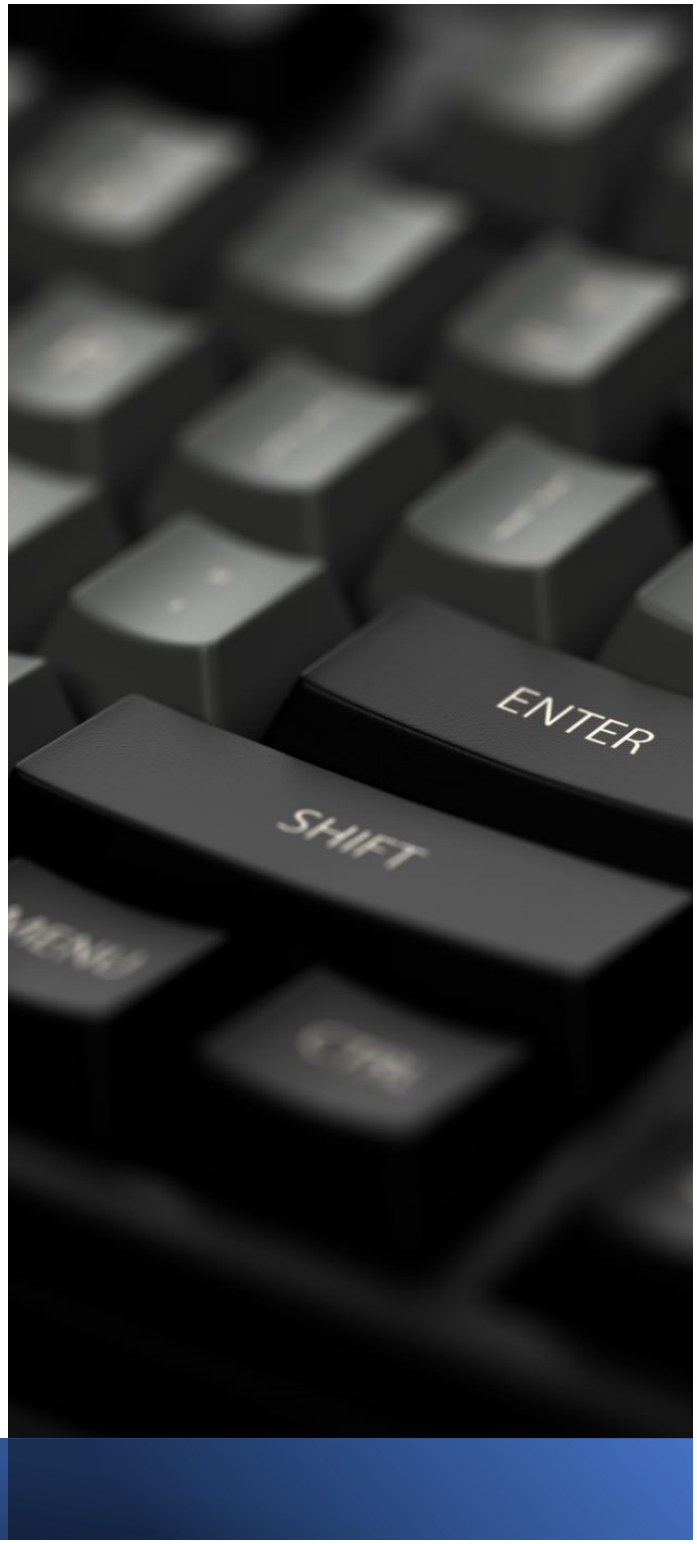
Default User Accounts After Installation

- **Administrator** This is the main administrative management account that has full access to the system and all its management tools.



Default User Accounts After Installation

- **Guest Account** This is a catchall account used to provide access to users who do not have a user account on the computer. This account should be disabled after user accounts have been established.



Default User Accounts After Installation

- **HelpAssistant** This is a special Windows account used with its Remote Assistance utility to authenticate users connecting through it. This account is enabled whenever a remote assistance invitation is created, and it is automatically disabled when all invitations have expired.

Default User Accounts After Installation

- **SUPPORT_XXXXX** This is a special Microsoft account used to provide remote support through their Help and Support Service utility.

A Word About Root Accounts

- The root account has unlimited access to the Linux operating system and its configuration parameters, and it is provided for administrative purposes. For security purposes , you may want to lock the root user account after creating users and groups to prevent others from using the default user without a username and password.

Default Group Accounts in Windows Server Systems

- **Administrators** Members of this group have full access to the computer and its tools and can perform all management functions. This group automatically includes the Administrator user account as a member.

Default Group Accounts in Windows Server Systems

- **Guests** This default group has minimized access to the system, and all members share the same user profile. The Guest user account is automatically a member of this group.

Default Group Accounts in Windows Server Systems

- **Power Users** Power Users is a special group that has permissions to perform many management tasks on the system but does not have the full administrative privileges of the administrator account. Power Users can create and manage users and groups that they create. Also, they do not have access to files and folders on NTFS volumes unless they are granted permissions to them through other sources. There are no members in this group when it is created.

Default Group Accounts in Windows Server Systems

- **Backup Operators** As the name implies, members of this group can back up and restore all files on the computer. Through the backup utility, members of this group have access to the system's entire file system. There are no members in this group when it is created.

Default Group Accounts in Windows Server Systems

- **Network Configuration Operators** Members of this group can manage different aspects of the system's network configuration. In particular, they can modify TCP/IP properties, enable, disable, and rename connections, and perform IPCONFIG operations. This group is empty when it is created.

Default Group Accounts in Windows Server Systems

- **Users** This is a catchall group with limited default permissions. Except for the guest account, all user accounts created on the system, including the administrator account, are made members of this group by default.

Default Group Accounts in Windows Server Systems

- **Remote Desktop Users** Members of this Windows group have user rights to log on to the system remotely to perform remote desktop activities. The group has no members by default.

Group memberships are automatically changed

- The Domain Admins group is added to the local Administrators group so that domain administrators will have administrative control over all the computers in their domain.

Group memberships are automatically changed

A DOMAIN USERS GROUP IS ADDED TO THE LOCAL USERS GROUP.

A DOMAIN GUESTS GROUP IS ADDED TO THE LOCAL GUESTS GROUP.

Adding Users or Groups in a Linux Distribution

Linux groups that appear in most distributions

GAMES THIS GROUP PROVIDES ACCESS TO GAME SOFTWARE

USERS THIS IS THE STANDARD, DEFAULT LINUX USERS GROUP

WHEEL THIS IS AN ADMINISTRATIVE GROUP THAT TYPICALLY PROVIDES ACCESS TO USER CREATION AND CONFIGURATION UTILITIES (SU AND SUDO COMMANDS).

Linux groups that appear in most distributions

- **Daemon** This is a standard, default user/group that has privilege to execute *daemon programs* (background processes) that run without direction from the user. In the Microsoft realm, this type of program is referred to as a terminate-and-stay resident program and most resemble services running in the Windows environment.

Linux groups that appear in most distributions

- **Bin** This is a standard, default Linux group that historically provided running executable files. The bin reference is based on the binary (executable) file types stored there. The folder contains scripts and commands that can be executed to perform a task. The commands in this directory can be run by every user.

Linux groups that appear in most distributions

- **Mail** This group has special mail privileges.
- **Root** The Root admin group is a standard, default Linux group that has complete administrative control of the system.
- **Nobody** This is the unprivileged group.

Linux groups that appear in most distributions

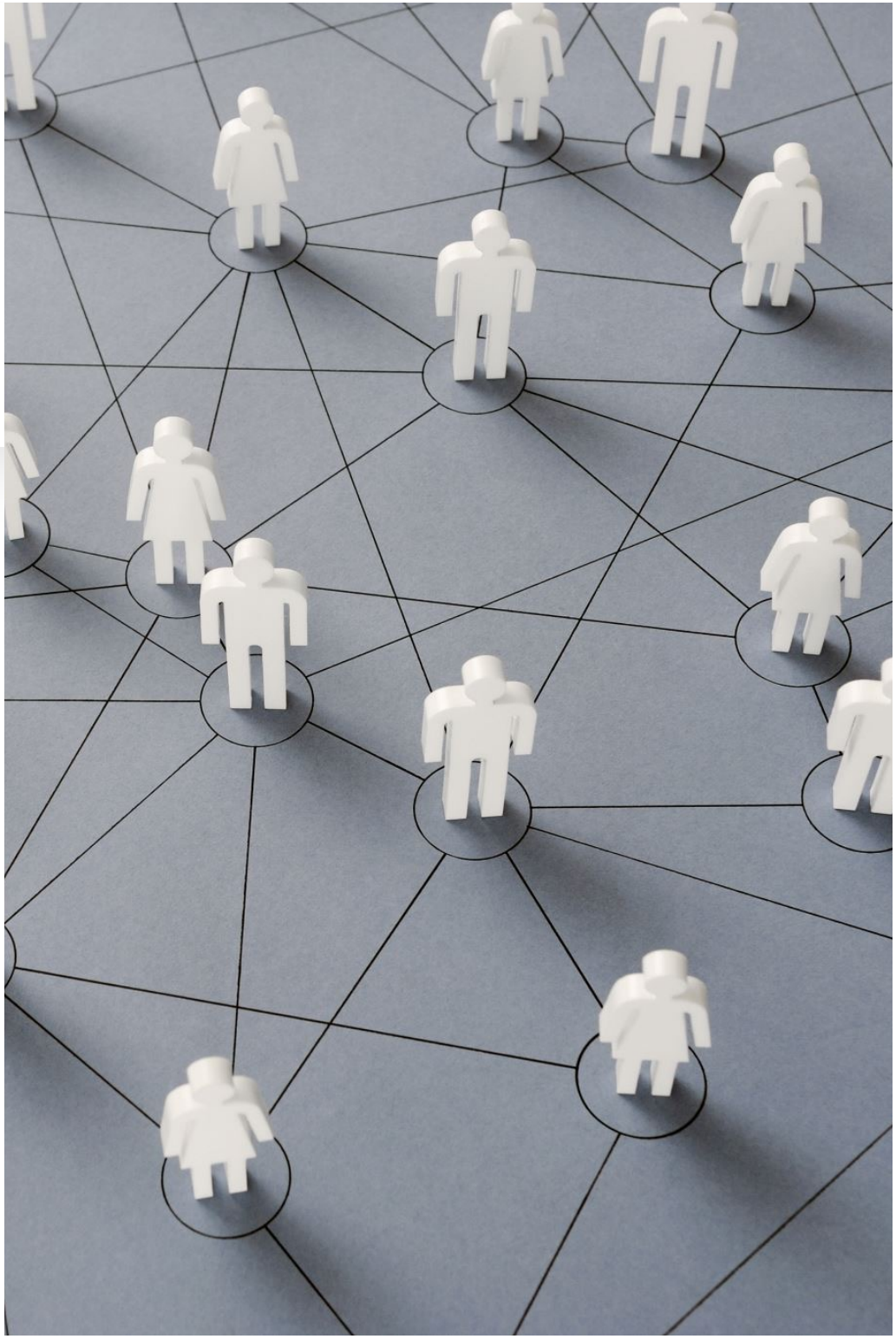
- **Disk** This provides access to “block devices” such as disk drives and optical drives.

Group Account Security

- Remove or disable unused default accounts, such as the guest account. Left unattended, these accounts can be used by hackers to exploit them. If default accounts must be retained, change their names as their standard authentication credentials are well known to potential attackers. Also, severely restrict access, along with rights and permissions available, to these accounts.

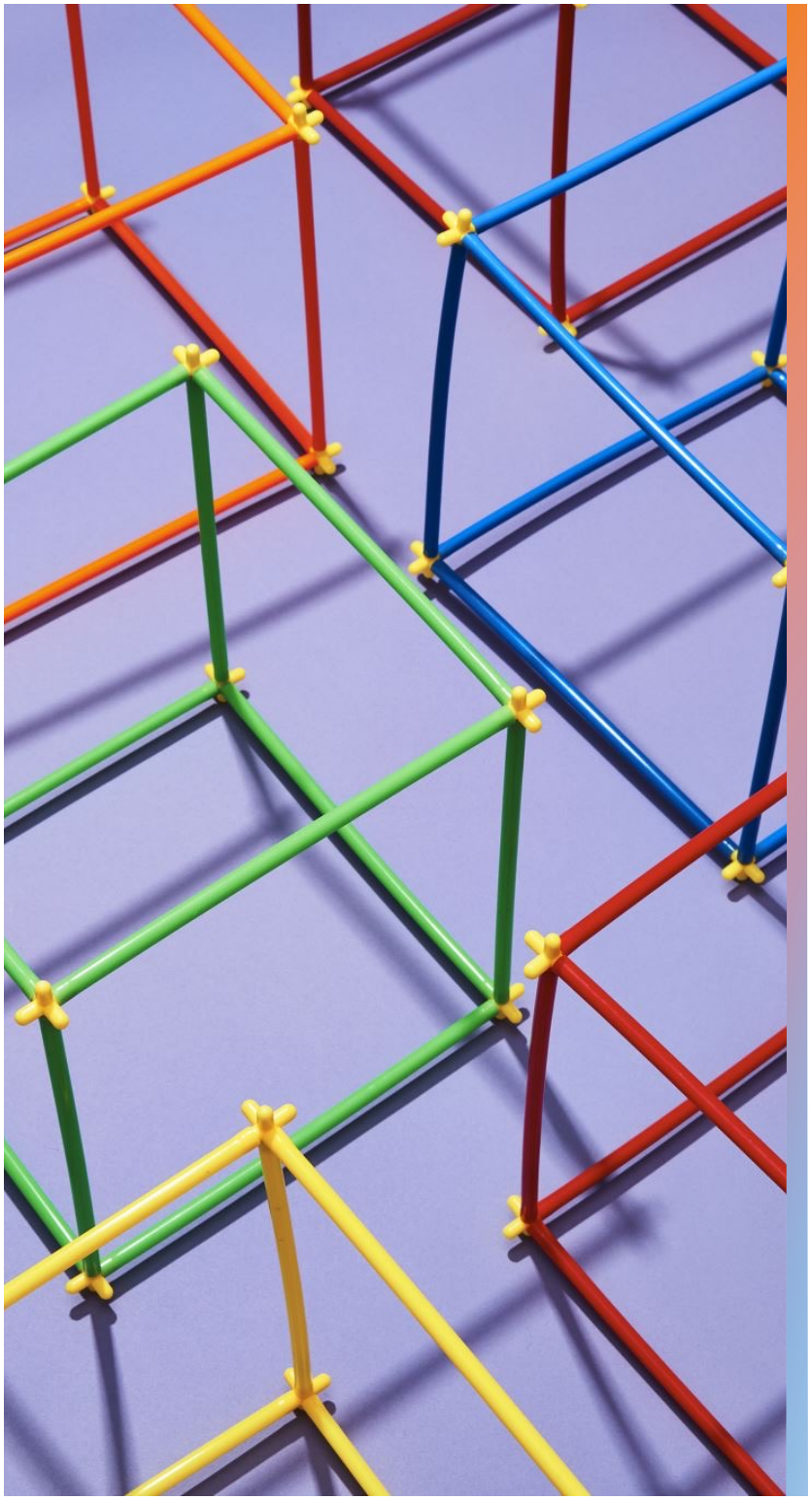
Group Account Security

- Create user groups that encompass the functions associated with different types of users who have common needs and then assign rights and permissions to each group according to the functional needs of the group.



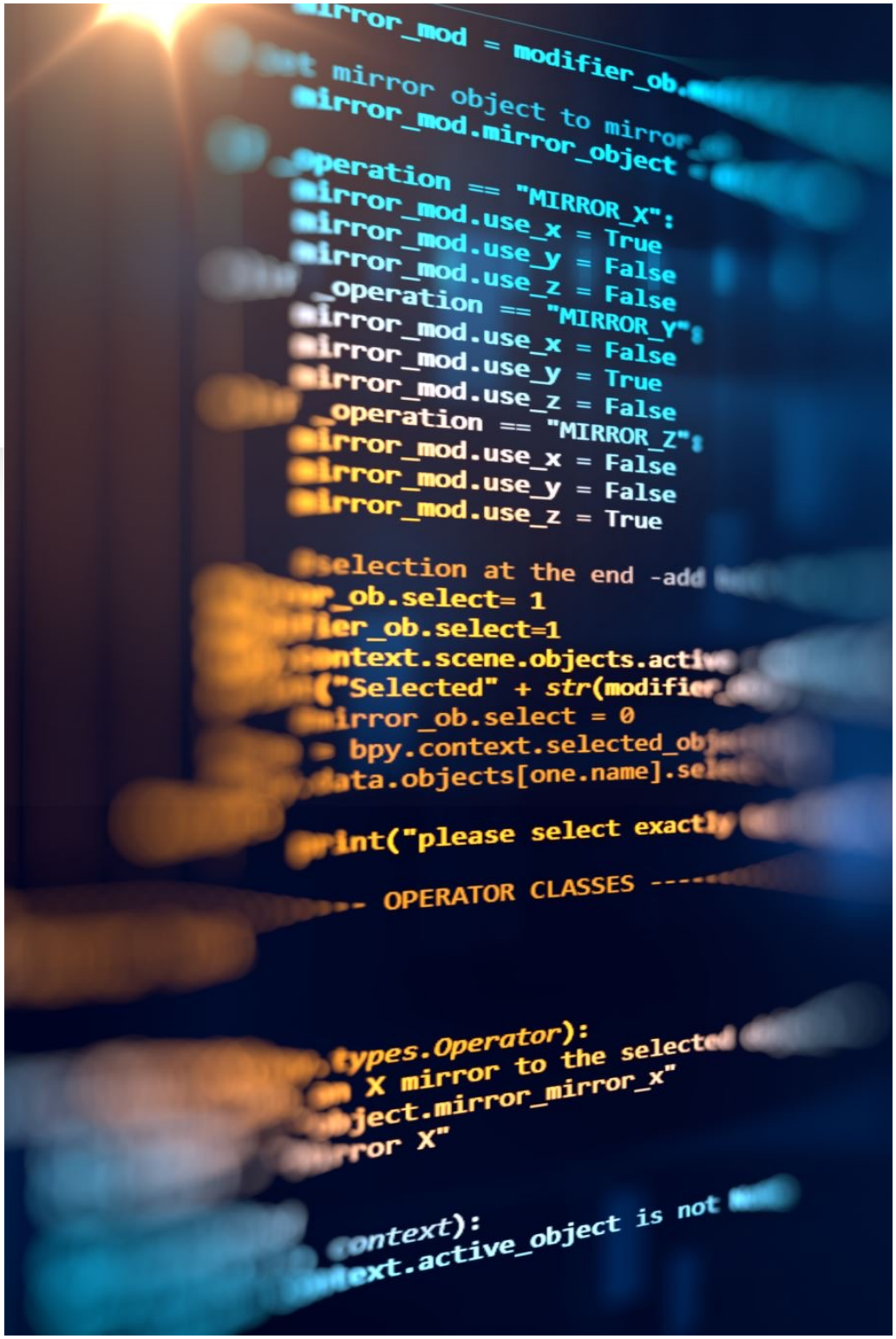
Group Account Security

- Create user accounts and assign them to groups according to their job functions in the organization. Using this approach prevents administrators from having to individually configure each user's account settings. Only create the accounts actually needed as unused accounts can provide security vulnerabilities if discovered.

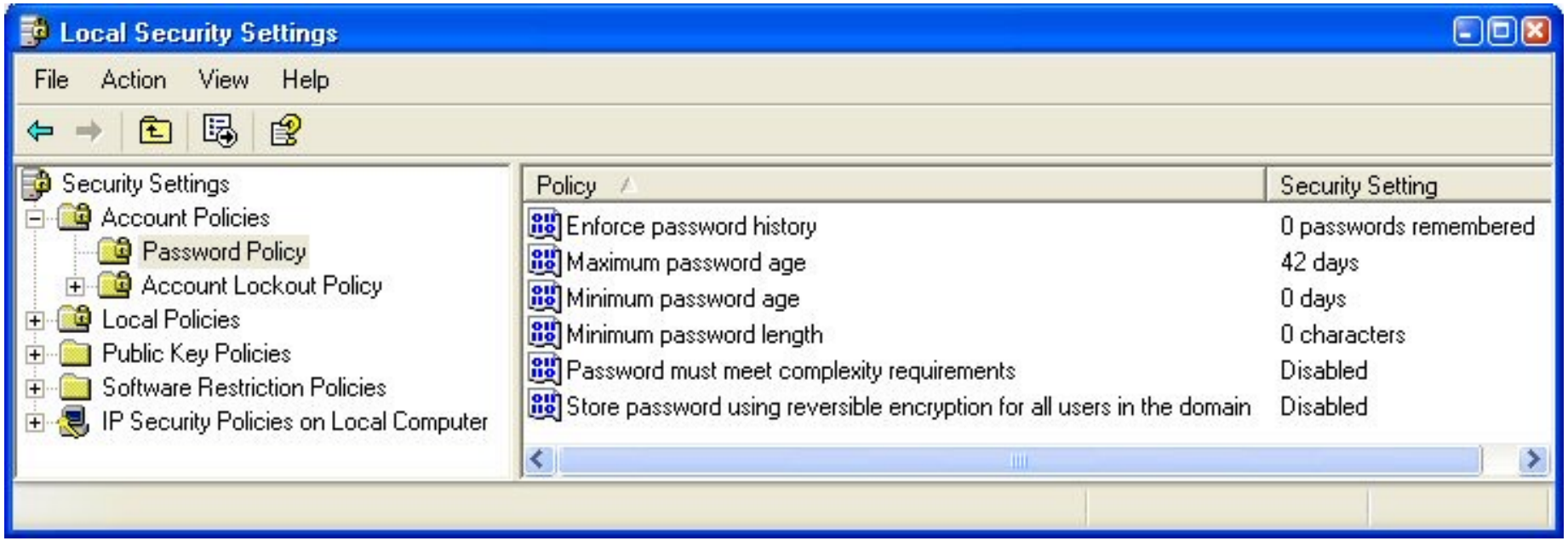


Group Account Security

- Set account passwords to work under the organization's password policy.
- Install and configure any additional authentication systems, such as biometric scanning devices, selected for use with the network.



Password Policies

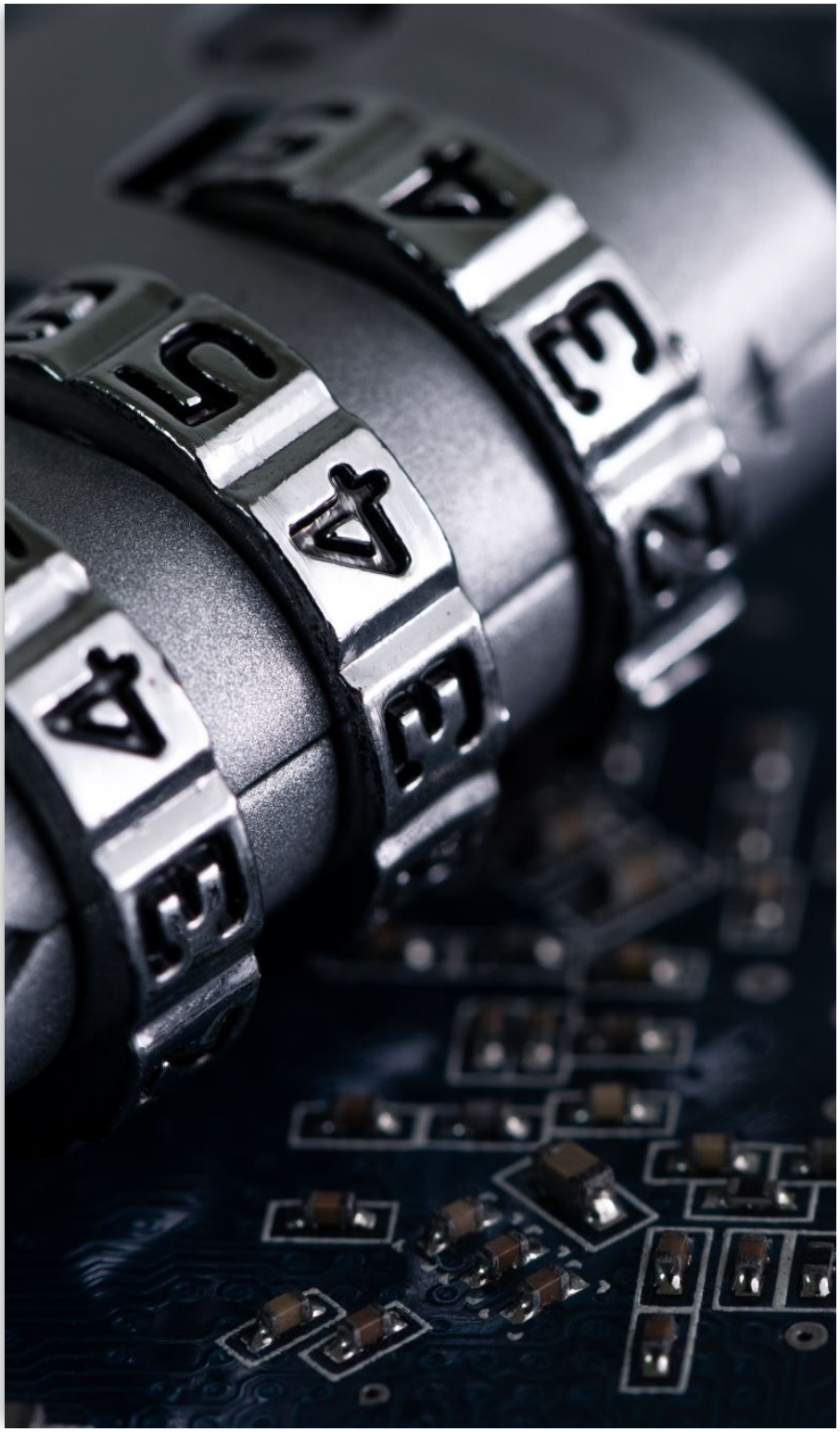


Enforce Password History

- This option is used to specify the number of passwords that will be tracked for each user. When users attempt to change their password, they will not be permitted to reuse any of the passwords being tracked.

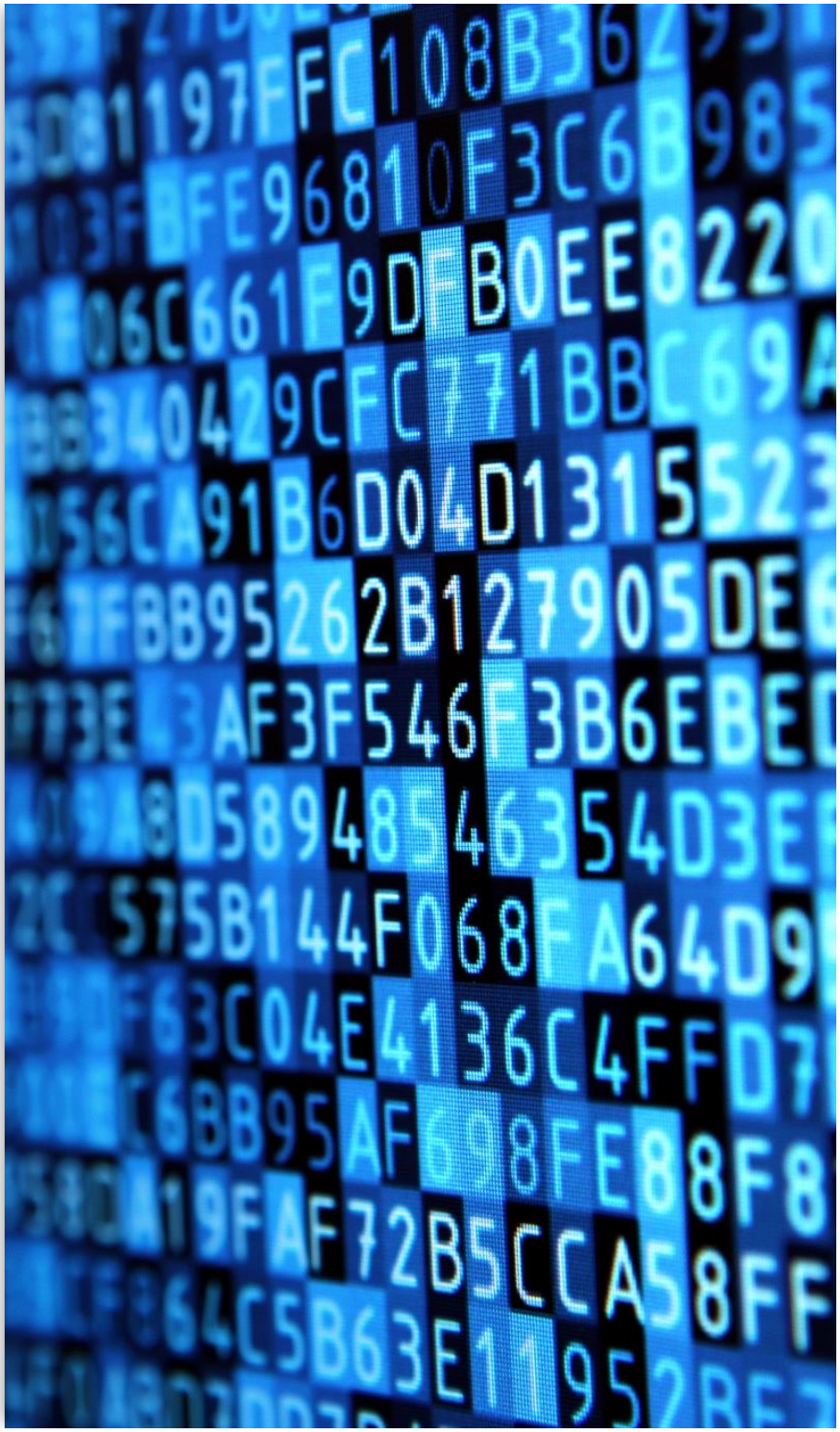
Maximum Password Age/ Minimum Password Age

- These two settings enable administrators to set passwords so that they expire after the specified number of days; they can prevent users from changing their passwords for some specific number of days. When the password expires, the user is prompted to change it, ensuring that even if a password becomes public, it will be changed within a short period of time to close the security breach.



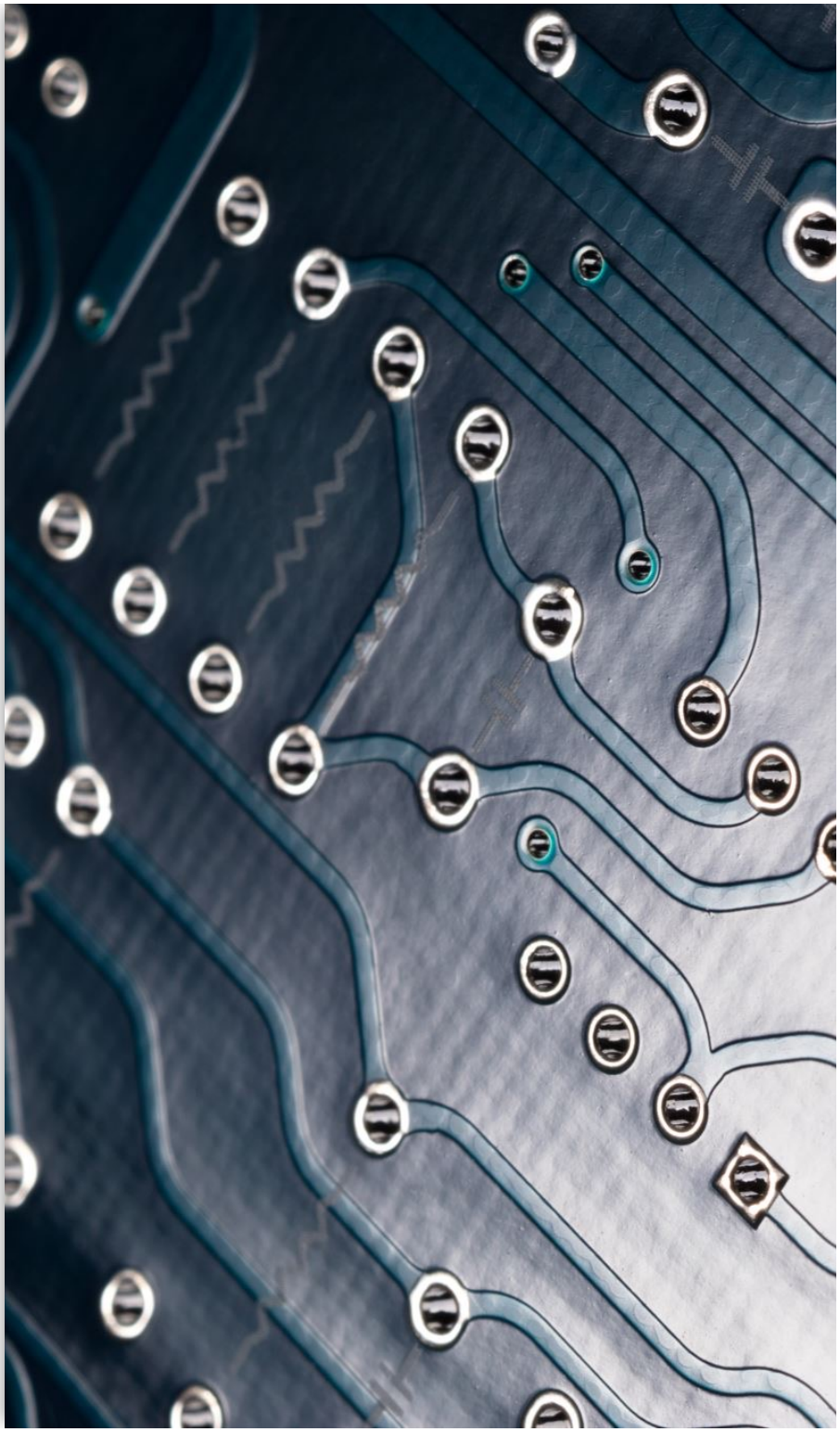
Minimum Password Length

- This option is used to specify the minimum number of characters that a password may contain. This allows the administrator to force users to employ passwords that are longer and harder to guess. A password of at least eight characters is recommended for secure systems.



Passwords Must Meet Complexity Requirements

- Administrators can use this option to force users to use more secure, complex passwords that include some combination of lowercase letters, numbers, symbols and capitalized characters. The administrator sets the level of complexity by establishing password filters at the domain controller level.



Standard NTFS Folder Permissions

- **Read** This permission enables the user or group to view the file, folder, or subfolder of a parent folder along with its attributes and permissions.

Standard NTFS Folder Permissions

- **Write** This permission enables the user or group to add new files or subfolders, change file and folder attributes, add data to an existing file, and change display attributes within a parent folder.

Standard NTFS Folder Permissions

- **Read & Execute** The Read & Execute permission enables users or groups to make changes to subfolders, display attributes and permissions, and run executable file types.

Standard NTFS Folder Permissions

- **Modify** The Modify permission enables users to delete the folder and makes it possible for users to perform all the activities associated with the Write and Read & Execute permissions.

Standard NTFS Folder Permissions

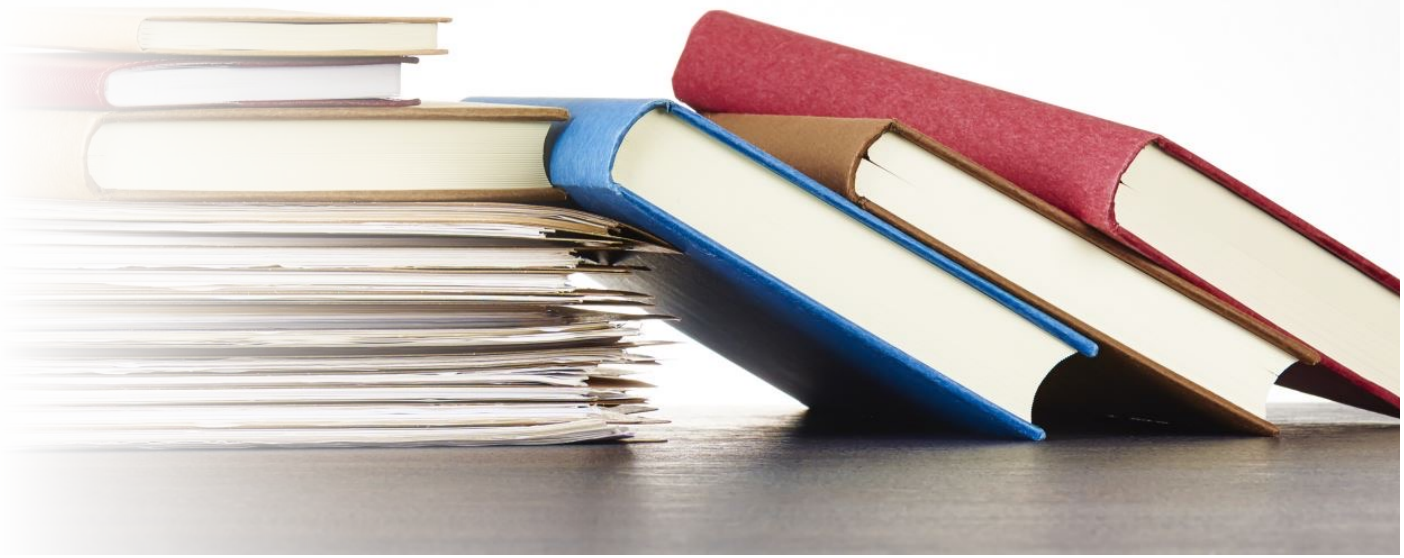
- **List Folder Contents** This permission enables users or groups to view files and subfolders within the folder.

Standard NTFS Folder Permissions

- **Full Control** The Full Control permission enables the user or group to take ownership of the folder and to change its permissions, as well as perform all of the other activities possible with all the other permissions.

Standard NTFS File Permissions

- **Read** This permission enables the user or group to view the file along with its attributes and permissions.



Standard NTFS File Permissions

- **Write** This permission enables the user or group to overwrite the file, change its attributes, and view its ownership and attributes.

Standard NTFS File Permissions

- **Read & Execute** The Read & Execute permission enables users or groups to run and execute an application, along with all the options available through the Read permission.

Standard NTFS File Permissions

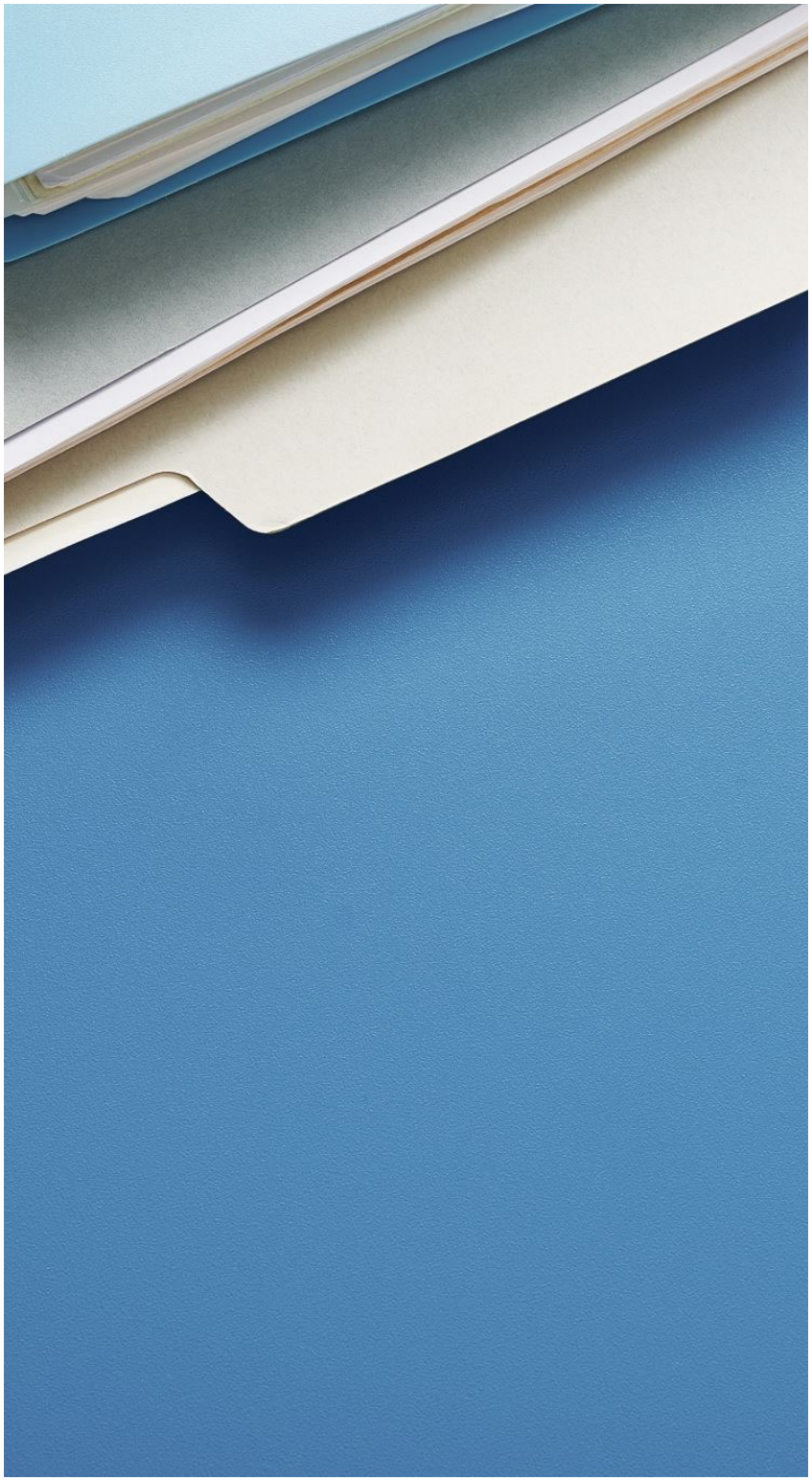
- **Modify** The Modify permission enables users to modify and delete the file and to perform all the activities associated with the Read, Write, and Read & Execute permissions.

Standard NTFS File Permissions

- **Full Control** The Full Control permission enables the user or group to take ownership of the file and to change its permissions, as well as perform all of the other activities possible with all the other permissions.

Linux Access Permissions

- **Read (r)** When specified, this permission enables the user to read the contents of the file or directory.



Linux Access Permissions

- **Write (w)** When specified for a file, this permission enables the user to modify the file by writing to it. When assigned to a directory, the Write permission allows the user to create or delete files in the directory.

Linux Access Permissions

- A typical file permission display (such as that obtained from a list (ls) command) will appear in the following format:

  drwxrwxrwx user group filesize Jan 01 08:00 filename

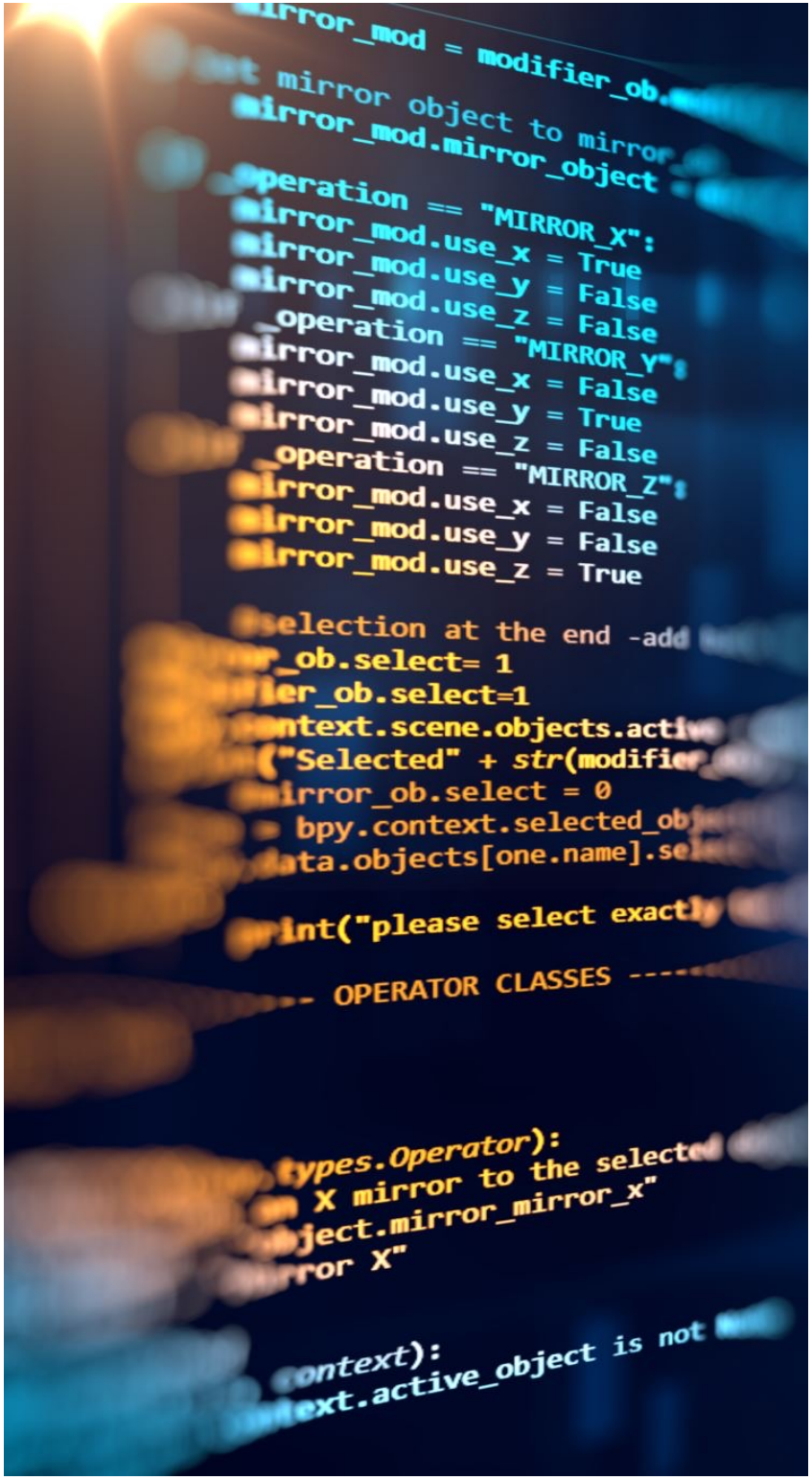
Linux Access Permissions

- When a permission is disabled for a particular user, its space contains a simple dash character:

  drwxrw-r-- user group filesize Jan 01 08:00 filename

A Word About Linux Permissions

- Linux permission assignments for a file are overshadowed by the permissions assigned to its parent directory. Even though a file may be assigned the permissions - rwxrwxrwx, the user will not be able to access the file unless they have read, write and execute permissions to the directory above the file.



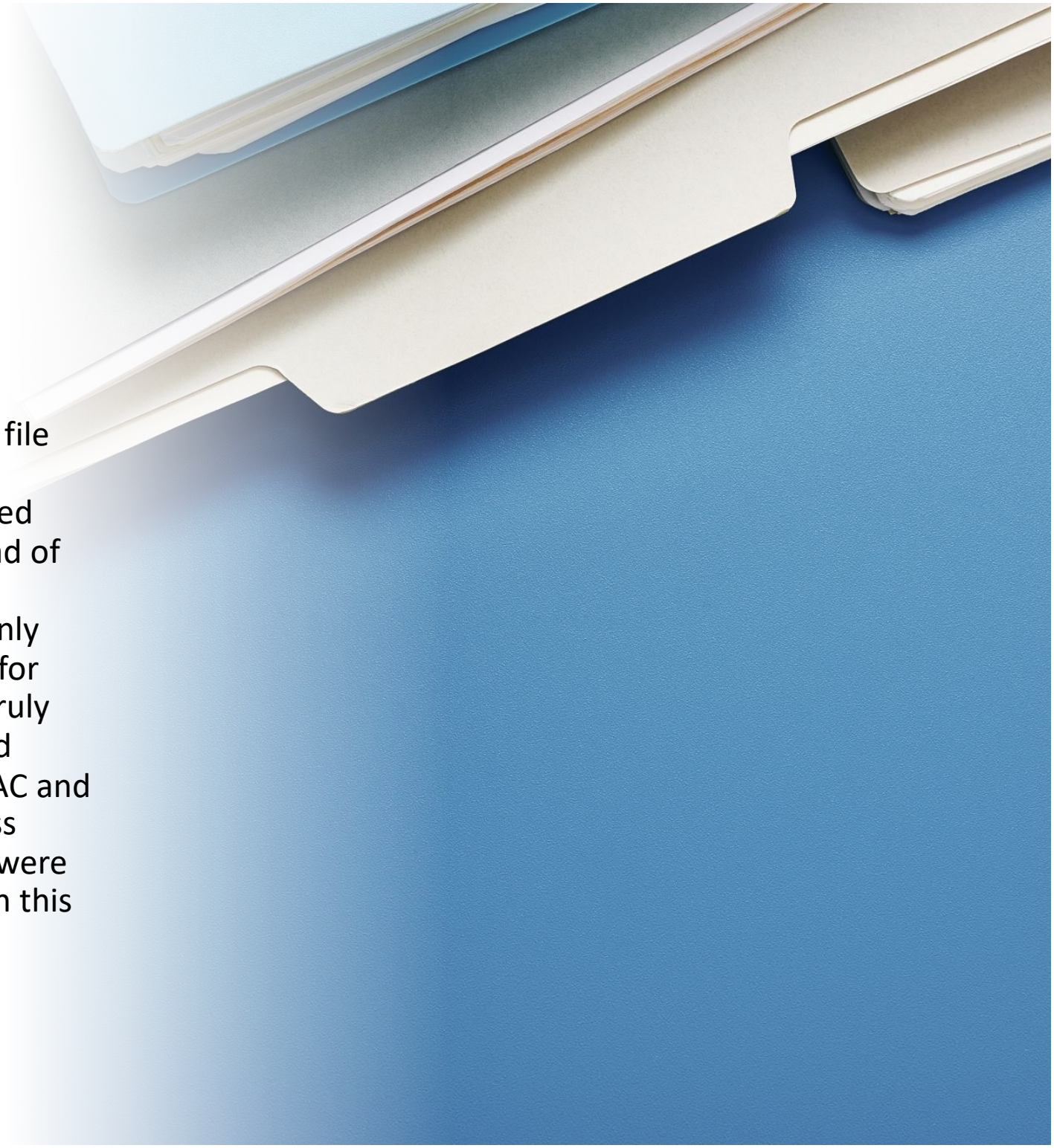
File System Hardening

- The first step is to employ standardized file systems across the organization if possible.
- Consider separating boot/system files from shared directories and data by placing them in different partitions on each server and user computing device.

File System Hardening

- Remove any hidden sharing features from the boot/system partition as well as in any other partition that has information that should not be shared.

File System Hardening



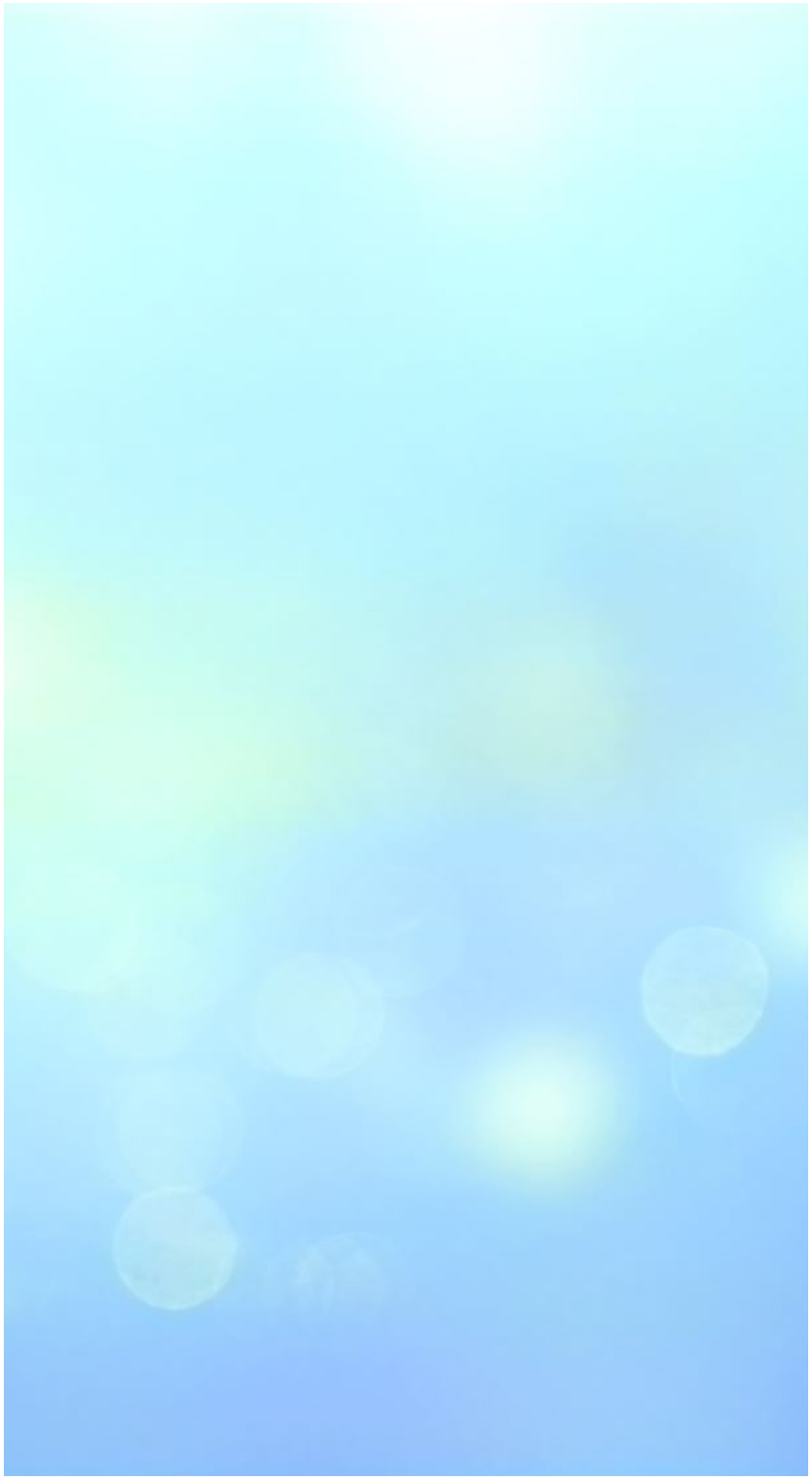
- For key folder and file permissions, use individually assigned permissions instead of role-based access control options. Only use RBAC options for information that truly needs to be shared across groups. RBAC and other logical access control strategies were discussed earlier in this chapter.

File System Hardening

- Employ file and folder encryption options where available.
- Establish periodic auditing and reporting for folders and files that are most critical to the organization’s operations.

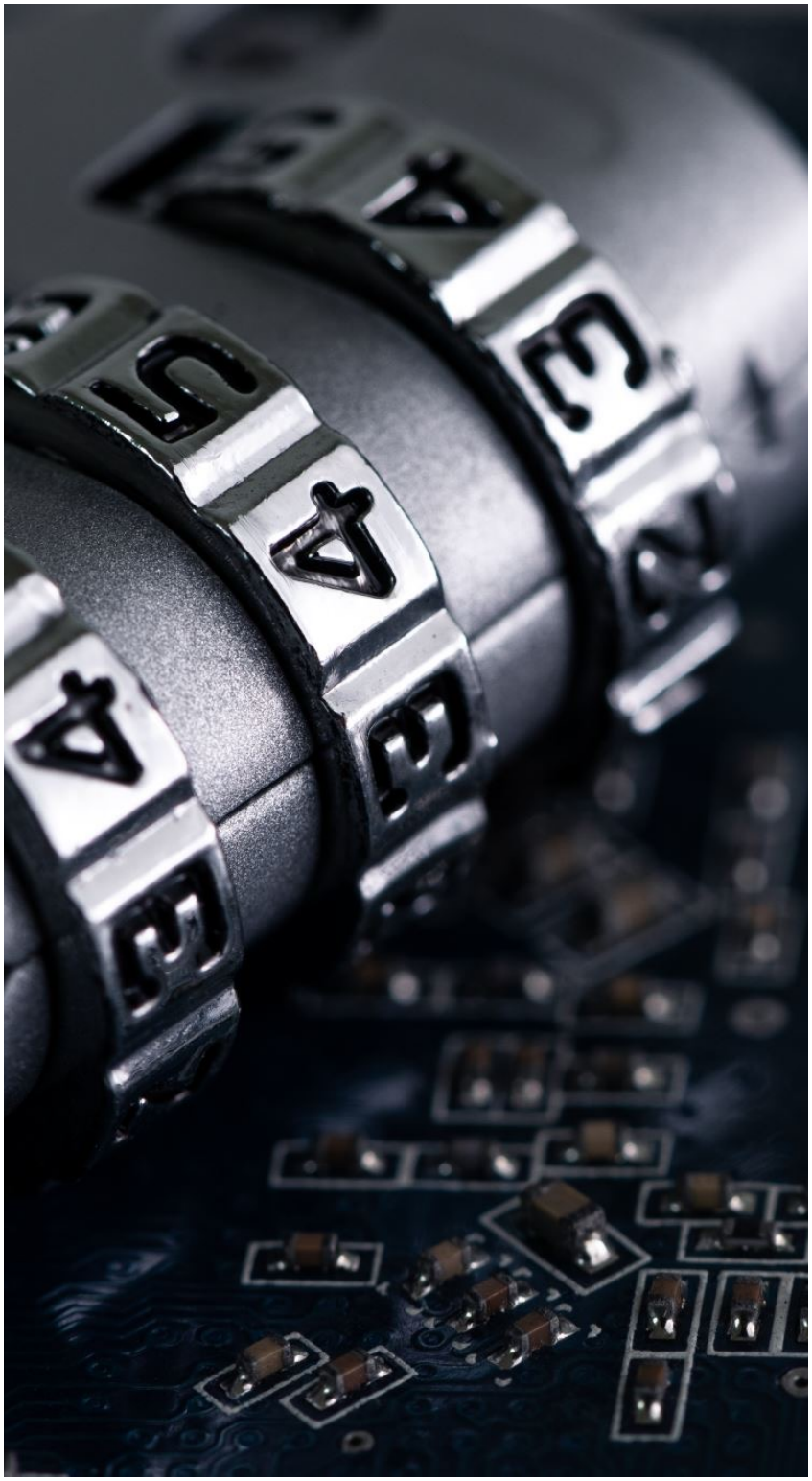
Primary duties associated with ongoing server operations

- Logging and auditing server activity
- Conducting regular server data backup operations

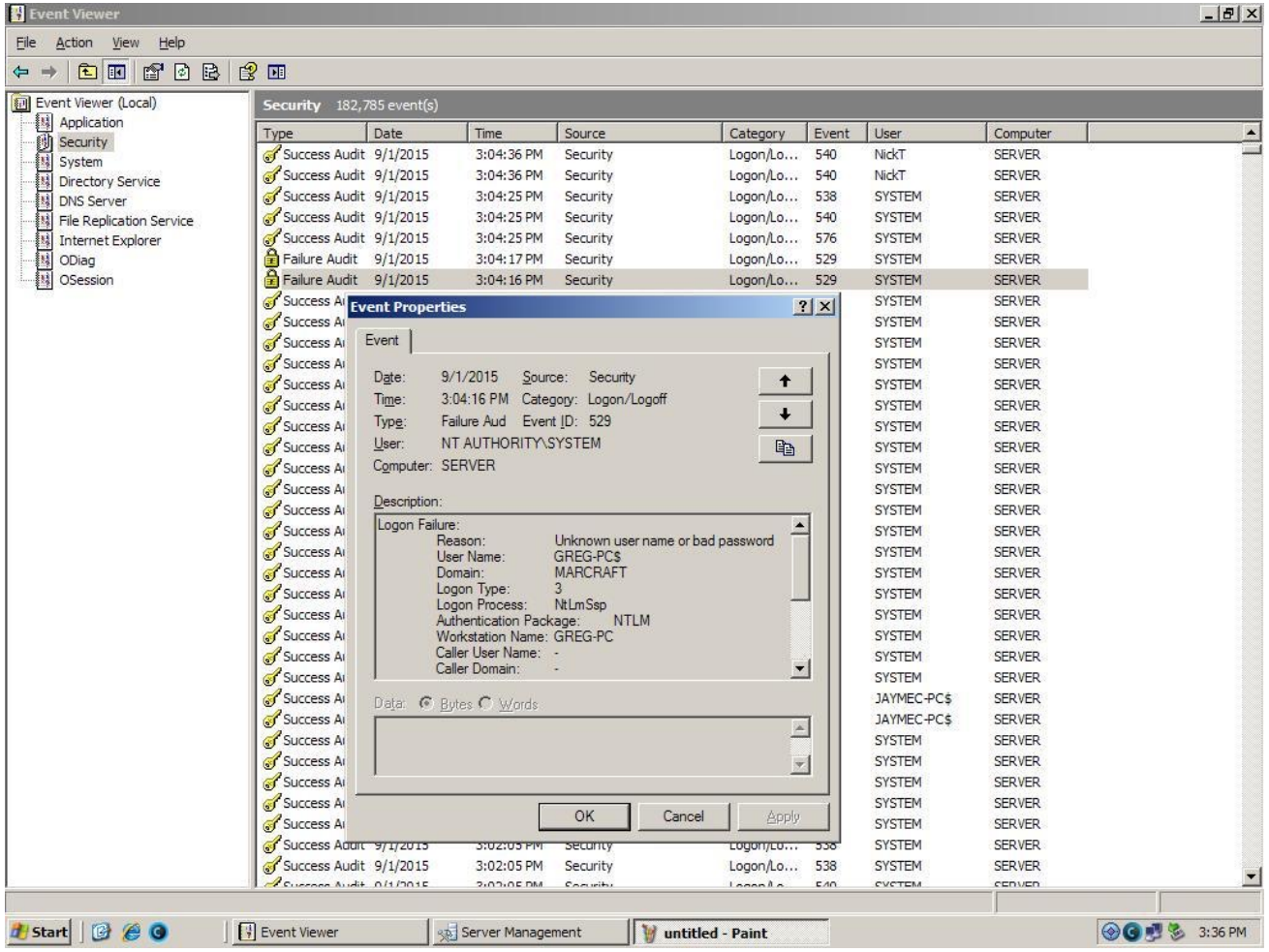


Primary duties associated with ongoing server operations

- Performing server-security testing procedures to verify the server's security remains uncompromised. These procedures include:
  - Maintaining the Intrusion Detection Systems
  - Performing routine vulnerability Testing
  - Performing penetration Testing

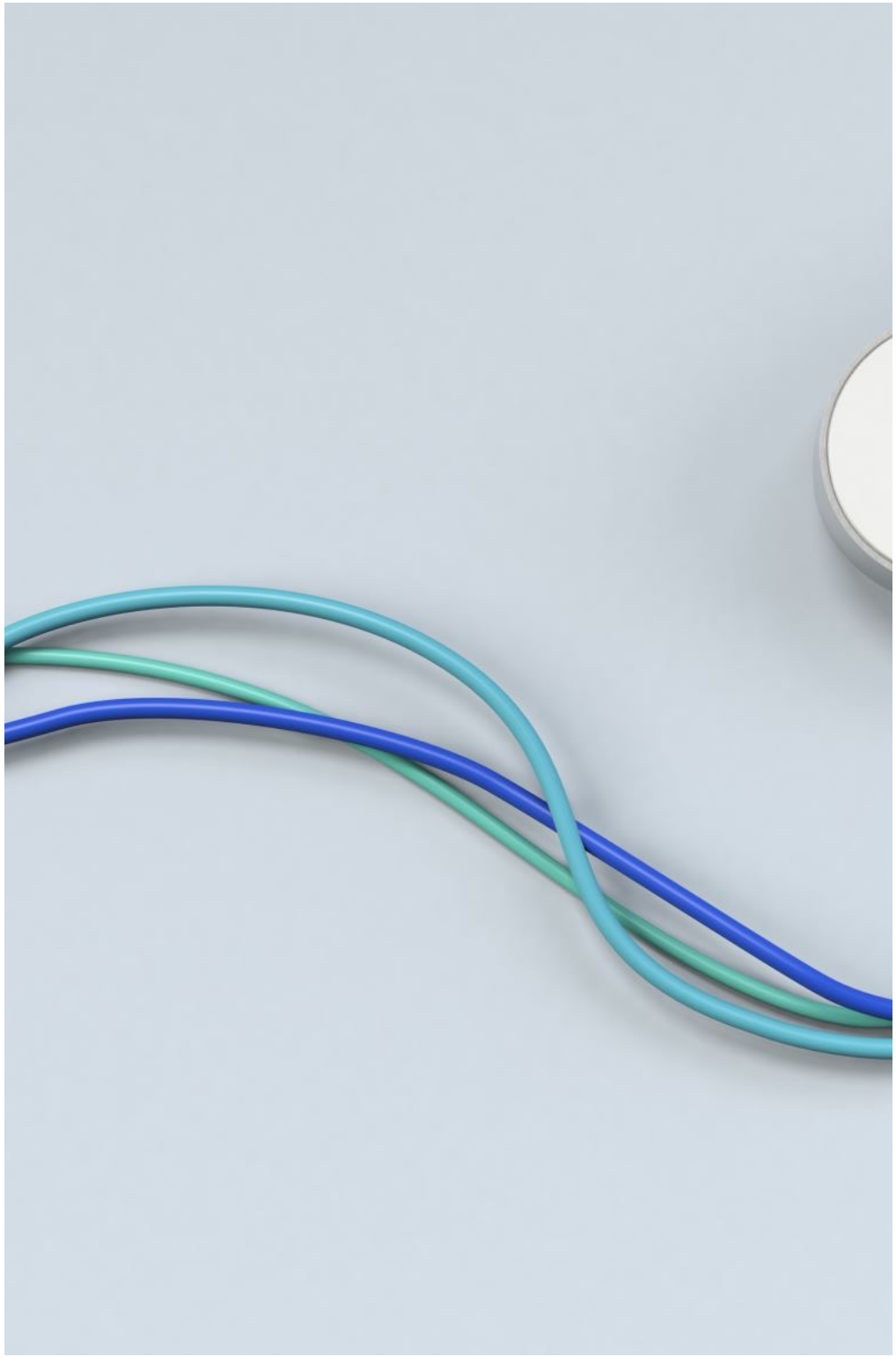


Viewing Security Audit Logs



Administrative Responsibilities

- Establishing types of backups to be performed. This includes configuring the backup utilities to conduct full, differential, incremental, copy, or daily backup options.



Administrative Responsibilities

- Defining how to back up. This includes configuring options for verifying the backup and enabling compression (if it's supported by the backup device). Verifying the backup involves comparing the stored data version with the data that was designated to be backed up (to make certain that all information was copied properly during the backup).

Administrative Responsibilities

- Specifying whether to replace the existing data on the backup media or append the new data to the end of the media.

Administrative Responsibilities

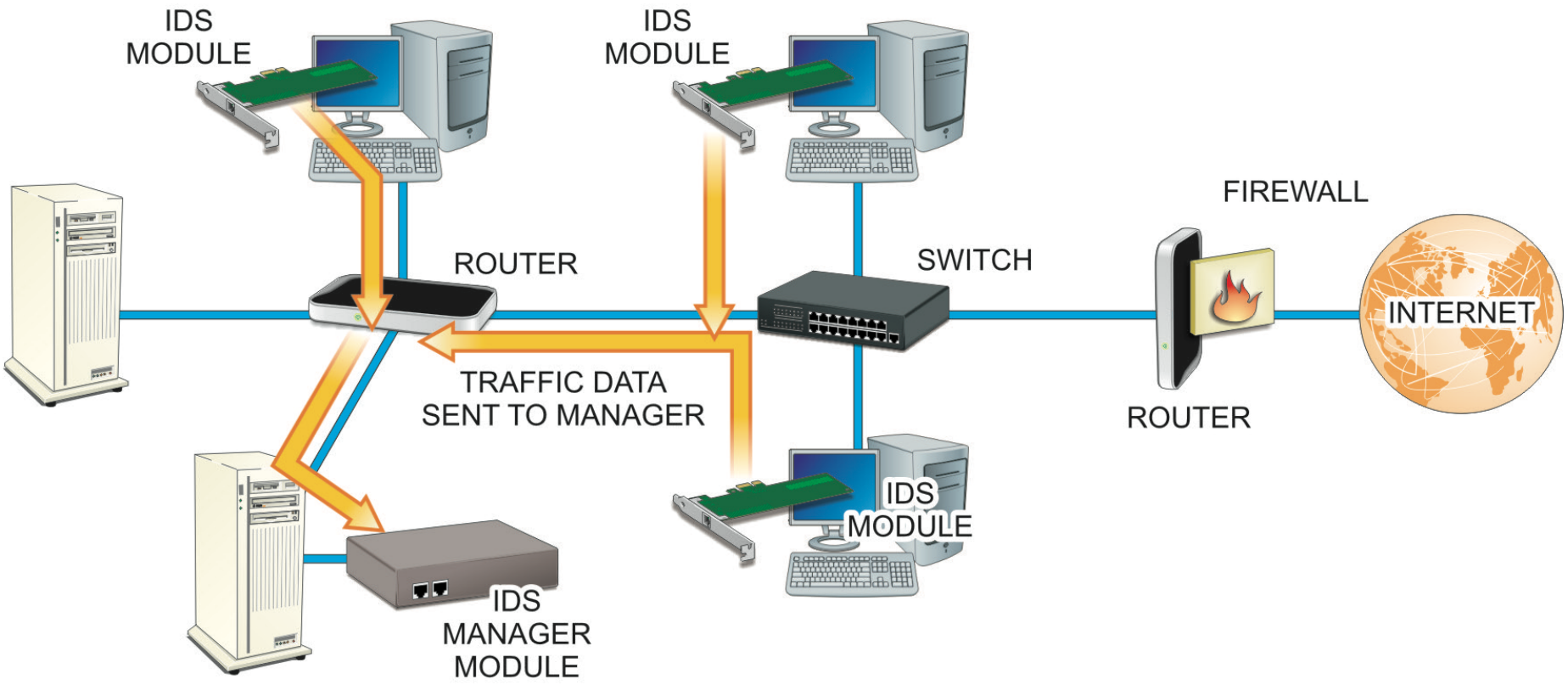
- Establishing backup labeling so that different backup copies that exist on the backup media can easily be identified and differentiated from each other. Normally, this involves labeling backups with the date and time they were performed.

Administrative Responsibilities

- Determining when to back up. This selection involves scheduling when different types of backups occur so that they have the least negative impact on the network's operation - such as late at night or on weekends when fewer users are likely to be using the network's resources.

Be Sure to Store Backups Securely

- Remember that it is possible for others to access the data from a stolen backup and restore it on another system where they have administrator privileges. Make sure backup copies are stored securely.



Distributed IDS

A Word About IDS Performance Factors

- When a distributed IDS system is being implemented, there are two major performance factors to consider: security versus efficiency. Likewise, the major management issues associated with implementing IDS/IPS systems involve the creation of false positive and false negative alerts – particularly when the system is first installed.

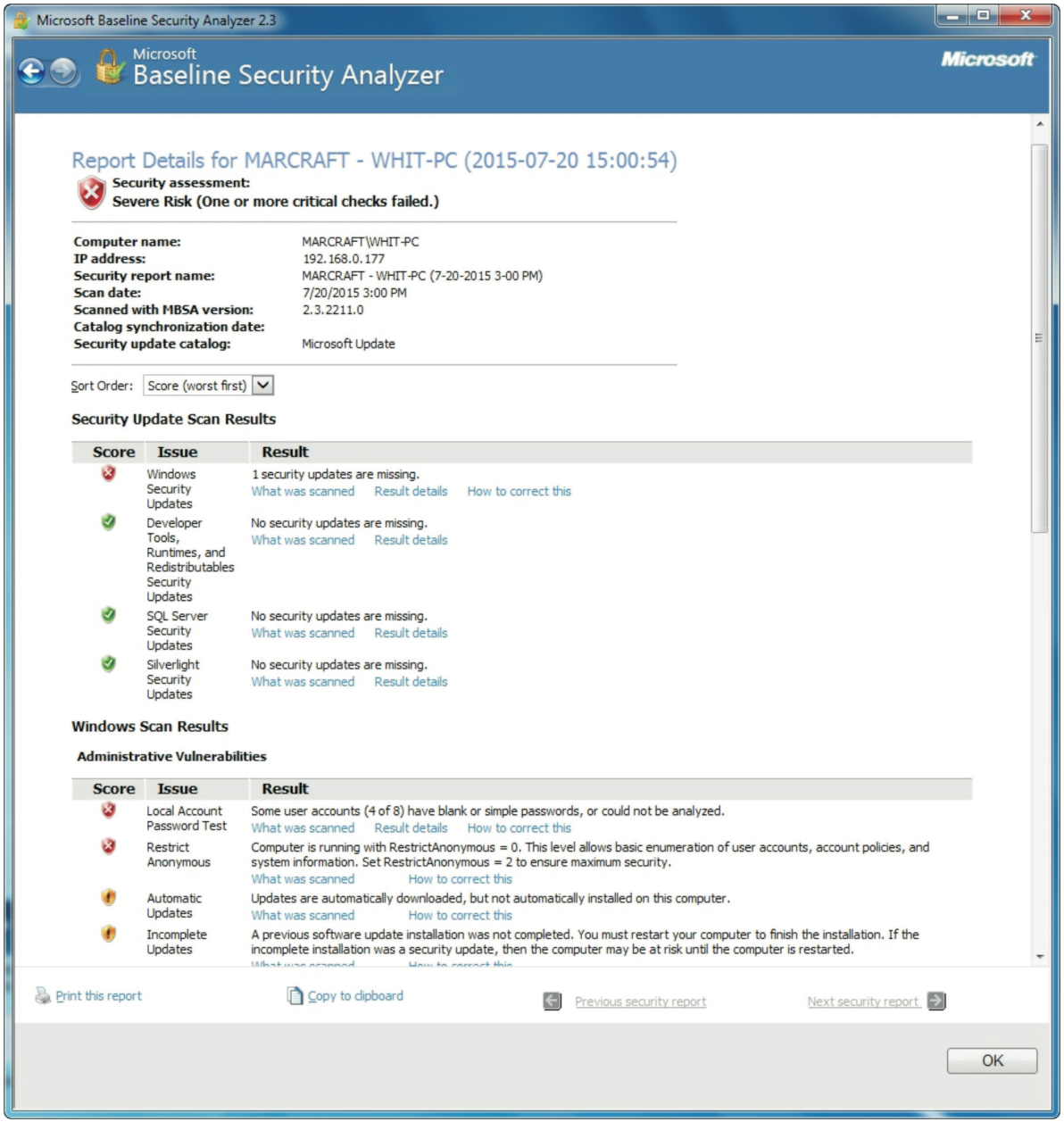
Types of Vulnerabilities

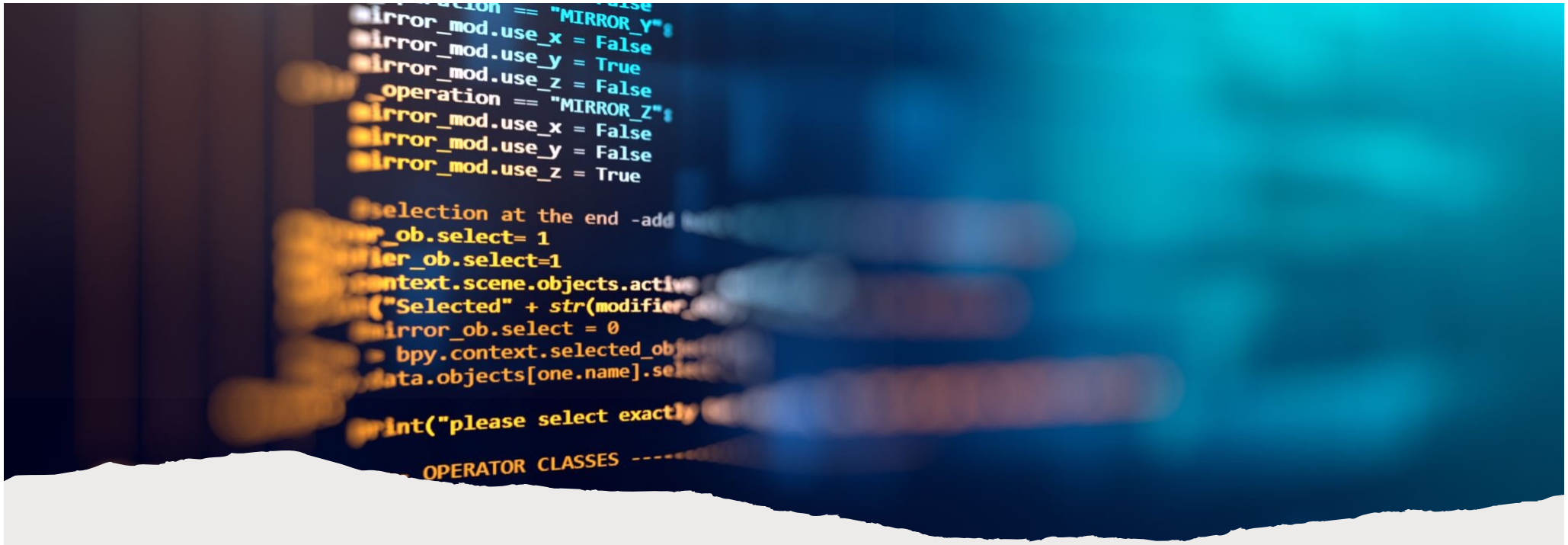
ACTIVE HOSTS ON A NETWORK (INCLUDING THOSE THAT MAY BE HIDING ON THE NETWORK)

ACTIVE PORTS AND SERVICES THAT ARE VULNERABLE

VULNERABILITIES ASSOCIATED WITH OPERATING SYSTEMS SERVER APPLICATIONS

A Typical Vulnerability Scanner





Monitoring Software

- Various server hardware and software operations are selected for tracking during the configuration of the monitoring software. The resulting event information can be stored in a log file.

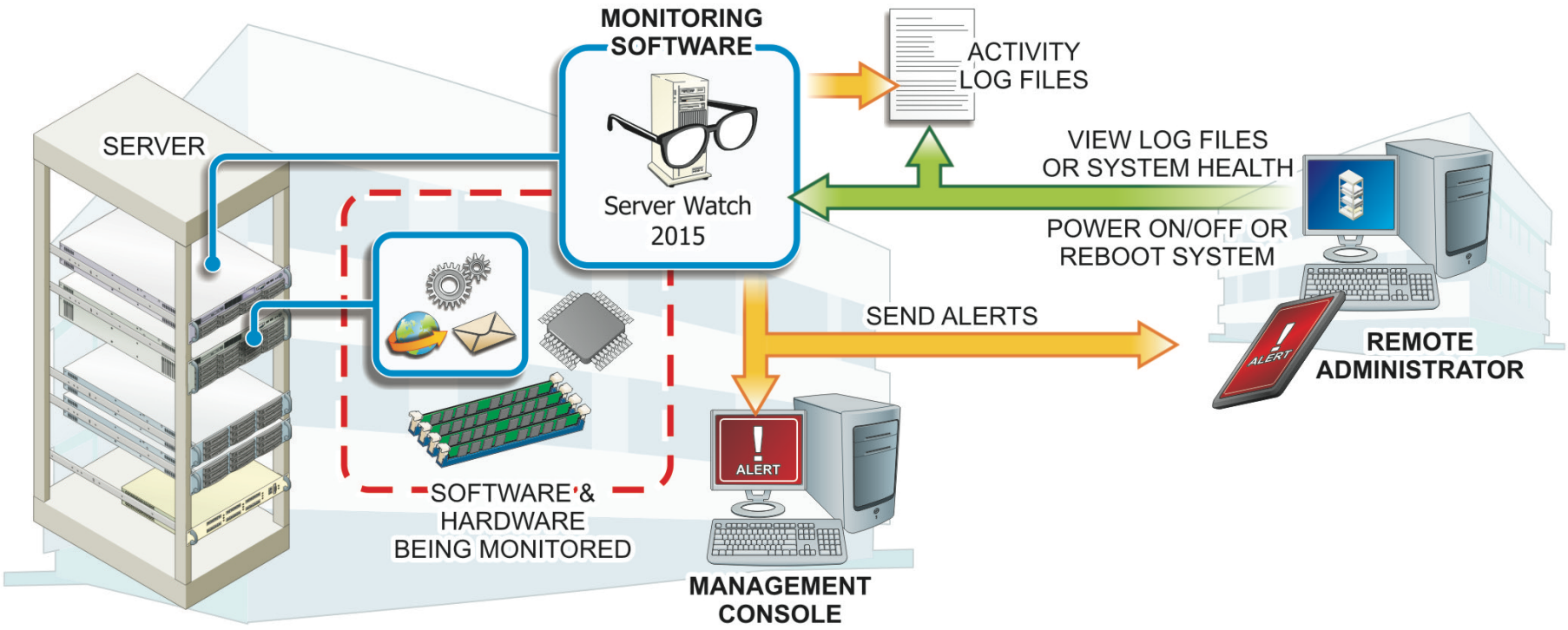
Alarm/Warning Systems

- Immediate warnings either in the form of an alert to the management console, or a page to the administrator, can be issued if and when the server system shows signs of an intrusion or a failure.

Remote Management Features

- Administrators can dial into the server and check on its health from a remote location. Diagnostic logs can be reviewed remotely, and a failed server system can be powered on, powered off, or even rebooted to get it back up and running without waiting for a technician to arrive.

Remote Monitoring Components



All IDS Devices are Based on One of Two Strategies

- Signature analysis: Incoming and outgoing traffic is compared with a database of stored, specific code patterns that have been identified as malicious threats.
- Anomaly analysis: Incoming and outgoing traffic is compared to an established baseline of normal traffic for the system.

Questions