

**Short answer: no—not as one of its eight named mitigation strategies.** The Essential Eight does not prescribe network segmentation as a standalone requirement. But that does not make segmentation irrelevant. A well-designed network can support the Essential Eight's objectives, limit the impact of a compromise and make it easier to detect suspicious activity. Poor network foundations can undermine those same outcomes.

That distinction matters when organisations assess compliance. The Essential Eight is not a complete security architecture, and meeting its maturity requirements does not automatically mean an organisation has adequate network security. Network segmentation, firewalls, capable switching and clear infrastructure records are among the controls that may be needed to manage risks beyond the Essential Eight's specific scope.

In practice, I've seen security incidents and outages traced back to the same sorts of issues: undocumented links, misconfigured switches, patch panels nobody can identify, or a production device connected to the wrong network. Physical infrastructure is part of cybersecurity, not a separate facilities concern. If the network cannot reliably enforce or show where traffic can go, the security design on top of it is only as strong as that weak foundation.

## What the Essential Eight actually covers

The Australian Cyber Security Centre (ACSC) describes the Essential Eight as a set of mitigation strategies designed to help organisations protect against a range of cyber threats. The strategies are:

- Application control
- Patch applications
- Configure Microsoft Office macro settings
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Regular backups

Organisations assess their implementation against maturity levels. The Essential Eight is not a list of network architecture requirements, and network segmentation is not one of the eight strategies. It would therefore be inaccurate to say that every organisation must deploy a particular segmentation design to meet the Essential Eight.

However, that answer needs a qualification: a control can be outside the named strategies and still be important to achieving an organisation's broader security objectives. Segmentation may help contain compromise, protect critical systems and support monitoring. It can also be relevant to other security obligations, risk assessments, contracts or regulatory frameworks that apply to an organisation.

## Why network segmentation still matters

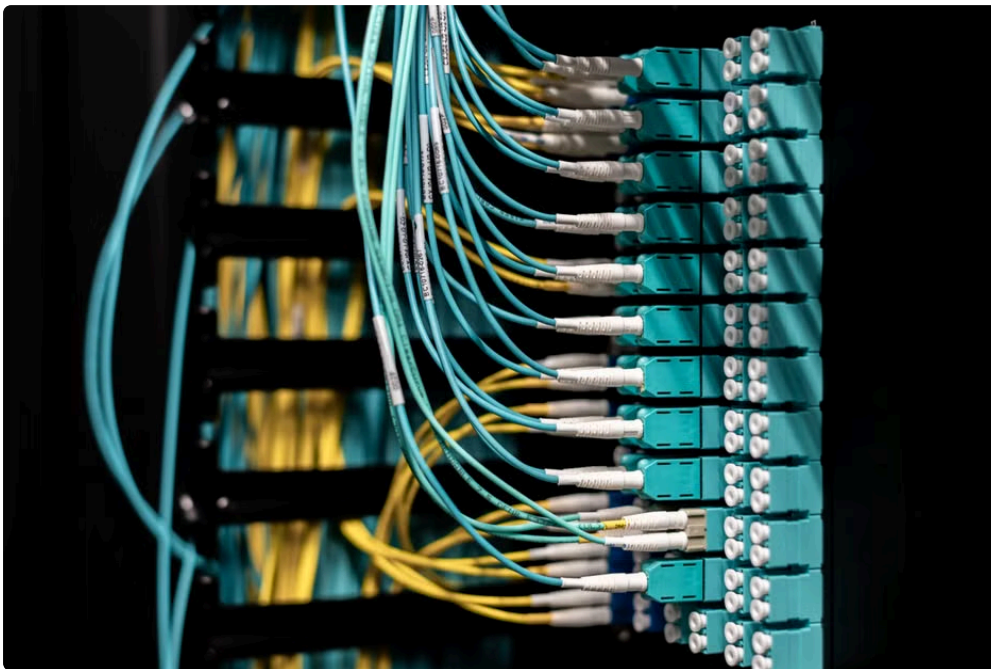
Network segmentation divides a network into separate zones or segments, then controls the traffic allowed between them. The design might separate user devices from servers, corporate IT from operational technology (OT), or production systems from guest Wi-Fi. Segmentation can be implemented using technologies such as VLANs, routing controls and firewalls, but simply creating VLANs does not guarantee effective separation. The rules, switching configuration and physical connections must all support the intended design.

Segmentation [cyberdaily](#) is useful because it can reduce the routes an attacker can take after gaining access to one device. A compromised workstation should not automatically have unrestricted access to every server, building system or industrial controller. Limiting permitted communications can reduce opportunities for lateral movement and make unusual traffic easier to spot.

It is a supporting control, not a substitute for the Essential Eight. A separated server zone does not patch an unpatched application. A firewall does not make a weak administrator account safe. Likewise, endpoint detection platforms can provide valuable signals about suspicious activity, but they do not create boundaries between networks. Each control has a different job.

## Essential Eight and infrastructure dependencies

The Essential Eight focuses heavily on endpoints, applications, privileges, authentication and backups. Those controls depend on infrastructure working as intended. This is where infrastructure dependencies become important: identity services, management systems, security tools and protected endpoints all communicate over physical and logical networks.

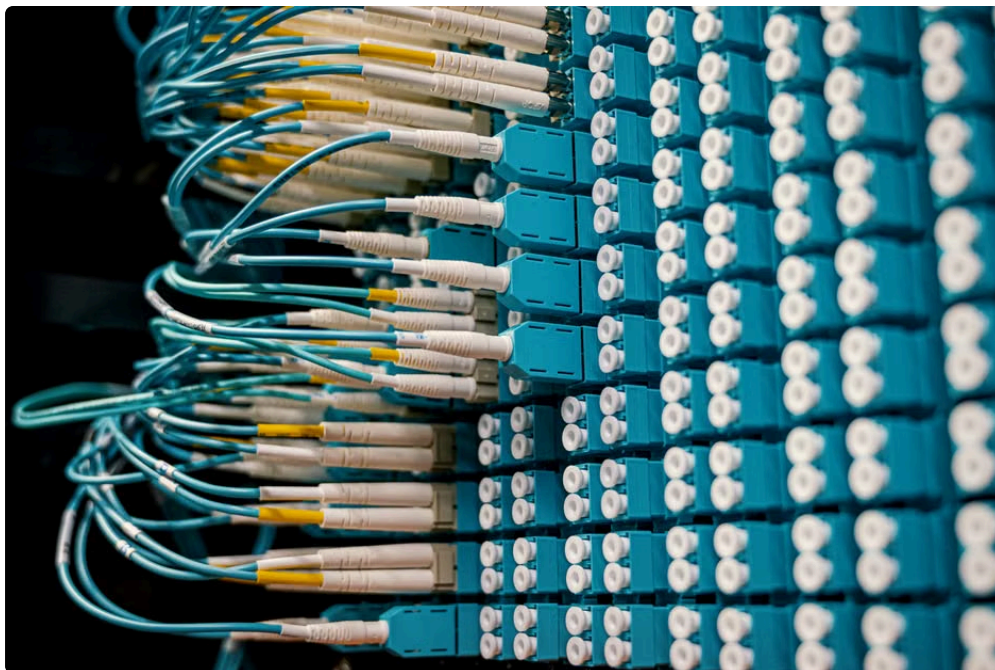


For example, endpoint detection platforms need reliable connectivity to send telemetry and receive updates. Patch management systems need to reach the devices they manage. Backup systems need access to the systems they protect, but that access should be designed carefully so a compromised endpoint cannot simply reach and destroy every backup. Network design can help constrain and observe those communications.

The same principle applies to administrative access. Restricting administrative privileges is harder to enforce consistently if management interfaces are reachable from broad, poorly controlled network areas. A dedicated management segment, tightly governed access paths and appropriate firewall rules can reinforce that strategy. They do not replace the Essential Eight's requirements, but they can help make its controls more robust.

## Segmentation is only as good as its enforcement

A network diagram may show neat zones, but the real question is what happens to traffic at the switch ports, routers and firewalls. Incorrect trunking, an unintended route, a permissive firewall rule or a temporary cable left in place can defeat the intended separation. Unmanaged switches in production are particularly problematic: they can introduce paths and devices that are difficult to govern or audit.



Equipment from vendors such as Cisco may provide the switching, routing and policy capabilities needed for a particular design. In industrial environments, MOXA equipment may be used to connect OT devices and support industrial networking requirements. The brand alone does not make a network secure. Device selection, configuration, lifecycle management and documentation matter more than the logo on the front of the switch.

Visibility matters as well. Where suitable, network TAPs or packet visibility products from providers such as Garland can help security teams observe traffic without relying solely on endpoint telemetry. That visibility is useful only when it is planned: monitoring points must cover the relevant links, feed the right tools and be maintained as the network changes.

## **Physical infrastructure is part of cybersecurity**

It is tempting to treat cabling as “just plumbing”. That is a mistake. A patch lead can connect the wrong device to the wrong network. A damaged fibre link can cause intermittent faults that make security monitoring unreliable. A switch with undocumented uplinks can create a blind spot in traffic analysis. Physical access to network cabinets can also provide an opportunity to bypass logical controls.

Physical layer faults create both outages and security blind spots. If a link flaps, monitoring may show incomplete data. If a switch is mispatched, traffic may take a path that nobody expects. If a sensor or appliance is connected after a design change but the change is not documented, the security team might not know it is missing from the monitoring plan.

Those conditions affect incident response. When an alert arrives, responders need to establish which device was involved, what network it was on, and what it could reach. Unlabelled patch panels and mystery cables turn that work into guesswork. A label maker is not a cybersecurity product, but accurate labelling and current records can save precious time during an outage or investigation.

## **What ACSC guidance assumes about network foundations**

ACSC guidance on the Essential Eight sets out the strategies and maturity expectations; it should not be read as a complete blueprint for every part of an organisation’s network. Organisations still need to assess their own risks and implement suitable controls for systems, data and operating environments that the Essential Eight does not cover in detail.

In other words, the Essential Eight assumes neither that every network is flat nor that segmentation is automatically present. It also cannot make a poorly managed network safe by itself. Effective implementation relies on sound foundations: assets that are known, systems that can communicate reliably with required services, and administrative and security controls that can be deployed and monitored consistently.

For an OT environment, those foundations need extra care. Industrial devices may have long lifecycles, limited patching options, strict availability requirements or protocols that do not behave like ordinary office traffic. Segmentation between corporate IT and OT can be an important risk treatment, but it must be designed around operational needs and tested carefully. A change that looks tidy on a diagram can still interrupt a process at 2am.

## How to assess whether segmentation is needed

Rather than asking only whether the Essential Eight requires segmentation, ask what the organisation needs its network to prevent, permit and reveal. A practical assessment can start with the following steps:

1. **Identify important assets and dependencies.** Record critical endpoints, servers, identity services, backups, management systems and OT devices, including the network paths they require.
2. **Map actual connectivity.** Compare the intended design with switch configurations, firewall rules, routing and physical connections. Do not assume the diagram reflects the live network.
3. **Define trust zones and permitted flows.** Specify which systems need to communicate, why they need to communicate, and which paths should be blocked.
4. **Check enforcement points.** Confirm that switches, routers and firewalls can enforce the design and that configuration changes are controlled and reviewed.
5. **Plan monitoring and recovery.** Ensure security tooling can see relevant activity and that teams know how to investigate or isolate a segment without causing avoidable operational harm.
6. **Test the design and keep it current.** Validate both security boundaries and business-critical flows. Update records when devices, links or rules change.

This work should be proportionate. A small office does not necessarily need the same architecture as a hospital, data centre or industrial site. The objective is not to create the maximum number of network zones. It is to apply boundaries where they reduce meaningful risk, while keeping the design understandable and supportable.

## Common mistakes to avoid

- **Calling VLANs segmentation without checking the controls.** VLANs create logical separation, but inter-VLAN routing and access rules determine whether traffic is actually restricted.
- **Building zones without an ownership model.** Someone needs to approve, document and review firewall rules and network changes.
- **Leaving unmanaged switches in production.** They can make topology, access control and troubleshooting harder to trust.
- **Forgetting the physical layer.** Port labels, cabinet access, patch records and cable paths all affect the real network.
- **Assuming security tools see everything.** Endpoint detection platforms and network monitoring each have coverage limits. Understand where those limits are.
- **Ignoring failure modes.** Ask what happens at 2am when a link, switch, firewall or monitoring feed fails. A secure design must also be operable and recoverable.

## So, does the Essential Eight require network segmentation?

No. Network segmentation is not one of the Essential Eight's eight named mitigation strategies, and an organisation should not claim that segmentation is an explicit Essential Eight requirement when it is not. But that does not make segmentation optional in every risk context. It may be an important supporting control for limiting compromise, protecting sensitive or operational systems, and improving visibility.

The better question is whether the organisation's network architecture supports its security objectives and the Essential Eight controls it has chosen to implement. I've seen this play out countless times: thought they could save money but ended up paying more.. That means looking beyond policies and endpoint settings to the switches, firewalls, cabling, monitoring paths and operational processes underneath them.

ACSC guidance provides a valuable security baseline. Strong network foundations help that baseline work in the real world. When segmentation is needed, it depends on capable switching, correct design and ongoing management—not just a diagram or a new firewall rule. And when the physical infrastructure is labelled, monitored and understood, the security team is far less likely to discover a mystery cable at the worst possible time.

Question Practical answer Is segmentation one of the eight Essential Eight strategies? No. It is not a named strategy. Can segmentation support Essential Eight outcomes? Yes. It can help constrain access, limit lateral movement and support monitoring. Do VLANs alone guarantee separation? No. Routing, access rules, switching configuration and physical connections also matter. Does meeting Essential Eight maturity mean the whole network is secure? No. Organisations need to assess wider risks and infrastructure dependencies separately.