NETWORK SECURITY MATURITY MODEL

How Mature Is Your Network Security?

Most organizations don't set out to build a complex network. Complexity develops over time as users, applications, cloud platforms, locations and business requirements evolve.

As that complexity grows, so do the demands on the network.

- Visibility becomes harder to maintain
- Access becomes more difficult to manage
- Security controls become less consistent

Use this model to identify where your organization operates today. Then compare the characteristics of each stage to see what typically changes as network security matures.

	Reactive *Security reacts to change.*	**Protected** *Core controls are established.*	**Segmented** *Access is intentionally separated.*	**Unified** *Security is governed through architecture.*	**Adaptive** *The architecture is designed to evolve.*
Visibility	Limited visibility	Partial visibility	Critical assets are visible	Consistent visibility	Visibility evolves with the business
Segmentation	Limited segmentation	Basic separation	Risk-based segmentation	Consistent segmentation	Segmentation adapts to change
Access	Broad access	Core access controls	Role-based access	Consistent policy enforcement	Access scales without exception
Governance	Manual governance	Repeatable governance	Defined ownership	Governed by design	Governance scales with business

Few organizations move from Reactive to Adaptive overnight. Most mature one step at a time by improving visibility, creating clearer boundaries, applying more consistent access controls and building governance into the network architecture.

Know Your Next Move

Every organization has a next stage. The opportunity is identifying the architectural improvements that will move you there.

Visit segra.com or call 833.GO.SEGRA to talk to a local expert.

SEGRA

Moving to the Next Stage

Organizations don't become more secure by skipping stages. They mature by addressing the architectural gaps that have the greatest impact on visibility, access, governance and control.

Reactive →→Protected: Standardize Core Controls

Security decisions are often made one issue at a time. Start by identifying your most critical systems and applying consistent protections across the environment. This creates a stronger baseline for every improvement that follows.

Protected →→Segmented: Create Clear Boundaries

Core protections are in place, but broad access still creates unnecessary exposure. Separating critical systems and sensitive data by role, risk and business need helps contain threats and strengthen control.

Segmented →→Unified: Simplify Governance

As environments grow, isolated security decisions become harder to manage. Bringing network architecture, access policies and security controls together under a common framework strengthens governance, improves consistency and reduces complexity.

Unified →→Adaptive: Design for Change

Business requirements will continue to evolve. Networks designed with flexibility in mind can support new users, applications, cloud platforms and locations without introducing unnecessary complexity or weakening security.

Take the Next Step

Knowing your current stage is valuable. Knowing how to move forward is where the real value begins.

A Segra network review helps identify the architectural improvements that will move your organization to the next stage of network security maturity, with practical recommendations based on your environment, priorities and business goals.



Contact your local Segra team to schedule a network architecture review and start building a stronger foundation for security.

Visit segra.com or call 833.GO.SEGRA

SEGRA®