



**Rethinking secure
connectivity for
the multcloud
enterprise**

LUMEN®

Contents

Securing the modern enterprise network	3
Why connectivity has become a security issue	4
Managing network risk in a multicloud world	5
The four pillars of secure connectivity	6
The Lumen approach to secure connectivity	7
Secure connectivity use cases and solution paths	9
The secure connectivity checklist	11
Security starts with the network	13



Securing the modern enterprise network

The enterprise network has become one of the most strategic, and exposed, parts of the business. It carries more cloud traffic, AI workloads, applications, data, users and partners than ever before. As the network becomes more critical, threats are increasing in both scale and sophistication.

For network and cloud architects, connectivity is no longer just plumbing. It is part of the security, resilience and operational strategy itself.

Yet networking and security are often managed separately, even though the risks they address are increasingly interconnected. Bringing these disciplines together earlier can help organizations apply more consistent protection, visibility and policy across users, sites, clouds and applications.

This eBook explores why secure connectivity matters now, what it looks like in practice and how organizations can operationalize it across increasingly distributed environments.

Why connectivity has become a security issue

The network is no longer a neutral layer beneath the business. It is the foundation for digital operations, cloud adoption, AI initiatives and increasingly distributed work environments. As the risks surrounding connectivity become more interconnected, securing the business requires protecting not only the network itself, but also how users, applications, sites, clouds and data connect.

Four realities shaping connectivity decisions

- 1 More business activity depends on the network.**
Cloud adoption, AI initiatives, digital experiences and distributed operations all rely on connectivity. As the network becomes more critical, the impact of disruption, misconfiguration or compromise grows.
- 2 More environments are connected.**
Traffic now moves across clouds, data centers, remote users, partners, internet services and edge locations. Each new connection creates additional operational and security considerations.
- 3 Modern threats move faster and are harder to identify.**
AI-assisted attacks, automated reconnaissance and increasingly sophisticated threat activity can spread quickly across connected environments, placing greater importance on visibility, segmentation and control.
- 4 Complexity creates risk.**
As organizations add clouds, providers, security tools and connectivity models, maintaining consistent policy and control becomes increasingly difficult.



Managing network risk in a multcloud world

Connecting environments is only part of the challenge. Architects must decide how traffic moves between clouds, applications, users and sites; where policies are enforced; and how routing, segmentation, visibility and security remain consistent as environments change.

As organizations expand across clouds, regions, applications, users and providers, multcloud has become the default operating model. This reshapes the connectivity and security problem in five important ways.



Five realities of the multcloud era

- 1 | More clouds create more exposure.**
Every cloud connection adds new traffic paths that must be monitored, governed and protected.
- 2 | Inconsistent policies create risk.**
Different tools, providers and environments can introduce policy gaps, configuration drifts and operational complexities.
- 3 | Cloud routing and private connectivity must work together.**
Reaching cloud resources efficiently and securely depends on how public and private paths are combined. Organizations need both performance and protection across public, private and hybrid environments.
- 4 | Control matters as networks scale.**
As complexity increases, centralized visibility and policy management become critical to maintaining security and operational consistency.
- 5 | Connectivity and security must move at the same speed.**
When connectivity can be activated or changed in minutes, protection and policy enforcement must be able to keep pace.

The four pillars of secure connectivity

Secure connectivity means designing protection, visibility, resilience and simplicity into the way users, applications, sites, clouds and data connect.

Together, these four pillars provide a framework for evaluating any connectivity strategy.

Protection	Visibility	Resilience	Simplicity
Helps reduce exposure before traffic enters the enterprise network.	Helps teams understand traffic patterns and emerging risk.	Supports continuity through resilient network design and recovery from cyber disruptions.	Reduces operational burden and gaps from disconnected tools.

Protection

Protection decisions should be made in coordination with connectivity decisions. Applying the right controls at the right points in the traffic path can help organizations differentiate legitimate traffic from potential threats, reduce exposure, limit unauthorized access and contain malicious activity before it spreads.

Visibility

Teams cannot protect what they cannot see. Visibility helps organizations understand traffic patterns, identify emerging risk, and make more informed security and operational decisions across distributed environments.

Resilience

When disruptions can't be prevented, secure connectivity supports both network and cyber resilience. Network resilience helps maintain connectivity during infrastructure failures, while cyber resilience helps organizations withstand, respond to and recover from cyber incidents. Together, they help ensure that connectivity remains available, secure and recoverable under most conditions.

Simplicity

Complexity creates risk. Consistent policy management, streamlined operations and fewer disconnected tools help reduce operational burden while maintaining control across distributed environments.

These four pillars are not independent features to be purchased separately. They reinforce one another: protection is stronger when you have visibility, resilience is easier when the architecture is simple.

The Lumen approach to secure connectivity

Lumen helps organizations align network and security strategies so protection, visibility, resilience and control are considered together as environments connect and evolve.

Protection that activates and scales with connectivity

Different connections require different security approaches. Lumen helps customers align protection with the way applications, users, sites and clouds connect. With Lumen® Intelligent Internet, for example, customers can activate proactive threat blocking and DDoS mitigation in the same rapid, self-service process used to activate new connectivity. When protection is built into how environments connect, security can scale with the network instead of chasing it.

Visibility powered by the #1 peered global IP backbone

Visibility is only as powerful as the network behind it. Lumen operates the #1 peered global network¹, enabling insight into traffic patterns across a broad portion of the internet ecosystem (99% of all public IPv4 addresses² via transit traffic). This unique vantage point helps the Lumen threat intelligence team, Black Lotus Labs®, identify emerging threats, malicious infrastructure and suspicious activity before they reach customer environments.

Black Lotus Labs tracks an average of 43,000 command-and-control servers, monitors billions of network signals daily and proactively blocks more than 600 critical-severity command-and-control threats each day, helping organizations strengthen risk awareness and improve proactive protection strategies.





Resilience backed by global reach

Backed by the world's #1 most peered global IP network, Lumen helps organizations build resilient connectivity with broad reach across networks, cloud providers and destinations worldwide. Combined with diverse routing options and approximately 340,000 route miles of fiber, this foundation helps organizations design for continuity while reducing dependence on any single path, provider or location. Lumen also supports recovery-focused strategies through solutions such as Lumen® Data Protect, Lumen® Network Storage and validated recovery architectures designed to help restore critical workloads and data after a cyber event.

Simplicity through owning both the network and control layers

Consistent policy enforcement, multicloud connectivity options and simplified management help organizations reduce operational complexity while maintaining control across distributed environments. With Alkira, customers can manage connectivity, segmentation, routing and security policies across clouds, sites and partners through a unified operating model, helping reduce policy drift and improve operational consistency as environments scale. Lumen is uniquely positioned to help customers simplify, secure and manage their environments by owning both the network underlay and control overlay.

The goal: Help security, visibility, resilience and connectivity scale together as the business grows.

Secure connectivity use cases and solution paths

Every organization has different connectivity requirements. The examples below illustrate common objectives and secure connectivity approaches that can help support them.

Business objective	Integrated connectivity and security approach	Relevant Lumen services	Expected outcomes
Protect internet-facing traffic from malicious activity	Internet connectivity with upstream DDoS mitigation and network-embedded threat blocking	Lumen® Intelligent Internet; Lumen® DDoS Mitigation; Lumen Defender SM	Helped preserve internet availability, reduced malicious traffic reaching downstream controls, improved security efficiency
Protect business-critical site, data center, apps and cloud traffic	Private connectivity paths to reduce internet exposure combined with segmentation and appropriate Layer 3 security controls	Lumen® Ethernet Fabric Connect; Lumen® IP VPN On-Demand; Lumen® Cloud Interconnect; Lumen® Managed Firewall Service; Lumen® SASE Solutions	Reduced exposure, predictable access, operational flexibility
Reduce multicloud risk and policy drift	Private and software-defined cloud connectivity with centralized routing, segmentation, policy enforcement and visibility across cloud environments	Lumen® Ethernet Fabric Connect; Lumen® Multi-Cloud Gateway; Lumen® Cloud Interconnect	Less complexity, more consistent control, reduced misconfiguration risk

Business objective	Integrated connectivity and security approach	Relevant Lumen services	Expected outcomes
Secure distributed users, apps and clouds	Software-defined connectivity combined with identity-aware access, segmentation and centralized policy enforcement across users, applications, clouds and sites	Alkira; Lumen® IP VPN On-Demand; Lumen® Intelligent Internet; Lumen® SASE Solutions; Lumen® Managed Firewall Service	More consistent access control, reduced unauthorized access risk
Maintain continuity during outages or cyber events	Resilient connectivity designed with diverse paths, redundant connections and failover capabilities, combined with cyber recovery services, data protection and recovery planning to support both continuity and restoration	Lumen® IP VPN On-Demand; Lumen® Intelligent Internet; Lumen® Data Protect; Lumen® Network Storage	Reduced disruption, improved recovery posture



The secure connectivity checklist

Secure connectivity is easier to operationalize when network, security and infrastructure teams evaluate it together. Use these questions to identify strengths, gaps and opportunities across your environment.

Network foundation

- ✓ What are we connecting: users, sites, apps, clouds, data centers or partners?
- ✓ Which connections require private, public internet or multicloud connectivity?
- ✓ Where do we need redundancy, failover or diverse paths?

If unanswered: Your connectivity strategy may not map clearly to business-critical priorities or risk exposure.

Visibility and intelligence

- ✓ Can we see enough traffic to understand risk across the attack surface?
- ✓ Where do current tools leave blind spots?
- ✓ How can network-level threat intelligence inform security decisions?

If unanswered: You may have blind spots between environments that make policy enforcement and incident response harder.

Layered protection

- ✓ Which connections need embedded protection, add-on protection or both?
- ✓ Where are we exposed to DDoS, malware, unauthorized access or misconfiguration?
- ✓ Where should security teams be involved earlier?

If unanswered: Protection may be arriving too late in the connectivity decision process.

Operational simplicity

- ✓ Can we apply consistent policies across sites, clouds, apps and users?
- ✓ Are policies managed centrally or fragmented across tools?
- ✓ Can policies keep pace with digital, on-demand connectivity?

If unanswered: Complexity may be increasing operational effort and creating room for gaps or policy drift.

Resilience and recovery

- ✓ What happens if a connection, provider, cloud or security control fails?
- ✓ How quickly can we restore service?
- ✓ Where do network resilience and cyber resilience need to work together?

If unanswered: Continuity planning may not be fully connected to the architecture decisions that shape risk.

Secure connectivity is a team sport.

Team	Primary concern
Network	Connectivity, performance, availability
Security	Threat protection, visibility, risk reduction
Infrastructure	Resilience, continuity, recovery
Leadership	Business risk, operational simplicity

Security starts with the network

The network has become foundational to modern business operations. That growing importance, combined with network sprawl and increased exposure to threats, makes it difficult to treat connectivity and security as separate conversations.

Organizations that build protection, visibility, resilience and simplicity into the way environments connect can create a stronger foundation for cloud adoption, AI initiatives, business continuity and future growth.

For network and cloud architects, the opportunity is to bring connectivity and security decisions into closer alignment, creating a shared strategy for control, resilience and business agility.

Explore how Lumen can help you build secure connectivity into your environment from the start.

¹The Center for Applied Internet Data Analysis (CAIDA), *AS Rank*, January 2025.

²Black Lotus Labs, *The 2026 Lumen Defender Threatscape Report*, 2026.