CableLabs®

SECURING AMERICA'S BROADBAND FUTURE

The Cable Broadband Industry's Cybersecurity Commitment

September 2025

The cable broadband industry is a cornerstone of America's digital infrastructure, delivering secure, high-speed broadband connectivity to millions of homes and businesses nationwide. Our multifaceted networks support economic growth, educational access, telehealth and public safety. These networks are powered by a robust mix of physical infrastructure such as fiber, coaxial cable, hybrid fiber-coaxial and wireless technologies like Wi-Fi, mobile broadband and Citizens Broadband Radio Service (CBRS).

CableLabs — the industry's leading R&D lab — and broadband providers invest heavily in developing and driving innovation in advanced security solutions to protect consumers and critical infrastructure. We work closely with the U.S. government to align on security priorities and stay ahead of emerging threats.

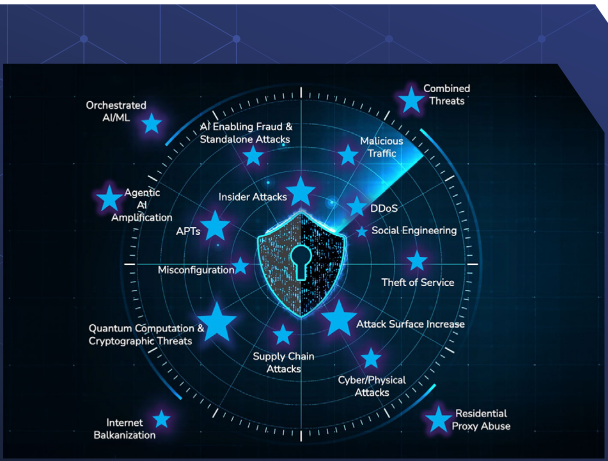
Facing Evolving Cyber Threats Head-On

Cyber adversaries — including nation-state actors like China, Russia, Iran, North Korea and global organized crime syndicates — pose persistent and sophisticated threats to broadband networks. These cyber adversaries never rest, and neither does the broadband industry. Through constant vigilance and collaboration, we work tirelessly to anticipate, analyze and respond to evolving threats that target broadband infrastructure. Cybersecurity experts across the industry coordinate in real time to detect, assess and respond to vulnerabilities and malicious activity, ensuring rapid, unified action against emerging threats.

Key areas of focus include:

- Countering advanced persistent threats (APTs)
- Securing the hardware and software supply chain
- Ensuring infrastructure, Internet of Things (IoT) and device security
- Advancing secure internet routing and ecosystem resilience

Through continuous innovation and collaboration, we are committed to ensuring a secure, resilient broadband future for all Americans.



» **Immediate Threats**
- Increase in attack surface
- Insider, supply chain and DDoS attacks
- Social engineering
- Misconfiguration
- Advanced persistent threats (APTs)

» **Midterm Threats**
- Quantum computation and cryptographic threats
- Malicious traffic
- Cyber/physical attacks
- Theft of service
- AI enabling fraud

» **Horizon Threats**
- Orchestrated AI/ML
- Internet Balkanization
- Combined threats (e.g., AI and social engineering)
- Agentic AI amplification

Advancing Cybersecurity Capabilities Across the Cable Industry

To stay ahead of advanced cyber threats, the cable broadband industry leverages CableLabs' research and development, technical risk assessments, tooling, technologies and lab-based testing, accelerating the deployment of scalable, real-world security solutions.

INFRASTRUCTURE STANDARDS AND TRUST

DOCSIS® is the foundational technical standard for secure broadband in the cable sector. As cyber threats grow more sophisticated, the industry is evolving beyond perimeter-based defenses, building on DOCSIS to implement zero trust architectures and modern trust ecosystems that secure every layer of the network.

CRYPTOGRAPHY

Classical cryptography is increasingly vulnerable to advanced cyber threats. We are developing frameworks for industry migration to new cryptographic solutions that include transitioning to post-quantum cryptographic algorithms, prioritizing cryptographic agility in digital certificates and shaping emerging industry standards to stay ahead of next-generation cyber threats.

SECURE SMART HOMES AND DEVICES

We shape industry standards to enable secure, seamless and ubiquitous connectivity for connected devices across mobile and fixed access networks. These efforts ensure that our networks can support interoperable security across private networks, smart homes, enterprises and advanced Wi-Fi environments.

IDENTITY AUTHENTICATION AND ACCESS

Conveying security information across networks is paramount to communications sector success in a future of converged services. As authentication becomes central to access for our subscribers, we are advancing new protocols that empower users to prove identity while enabling robust data security controls.

INTERCONNECTION, ROUTING AND OPERATIONS SECURITY

The industry is advancing secure routing protocols for distributed autonomous systems and applying zero trust security principles and intelligent telemetry standards from interconnection points to endpoints.

AI SECURITY

We are leveraging AI to enhance cybersecurity, as well as secure tooling and automation. This requires developing trusted security models for AI systems, agents, models, training data and operations.

Setting the Standard for Security Leadership

The cable broadband industry has more than three decades of experience operating and securing broadband networks. Across the home, enterprise, network infrastructure and the broader internet ecosystem, broadband providers are advancing security through real-world deployment and technical leadership.

HOME

We published the widely adopted CableLabs Gateway Device Security Best Common Practices for home routers and access points, and we lead efforts to standardize IoT security in the home.

ENTERPRISE

Our contributions to enterprise security include addressing ransomware threats and developing tools to mitigate the impact of Distributed Denial of Service (DDoS) attacks on businesses.

NETWORK INFRASTRUCTURE

For network infrastructure security, CableLabs published Zero Trust and Infrastructure Security Best Common Practices, and contributed substantially to 3GPP mobile security specifications and IEEE optical networking specifications.

INTERNET ECOSYSTEM

CableLabs' Cybersecurity Framework Profile for Internet Routing, which provides actionable guidance on routing security measures to mitigate vulnerabilities in the Border Gateway Protocol (i.e., the core routing protocol for exchanging information on the internet) is now a cross-industry benchmark. Our DOCSIS security standards continue to evolve to protect broadband subscribers when they use our networks to connect online.

> Our technologies are helping advance, enhance, leverage and transform the future of both wired and wireless networks.

Driving Innovation in Cybersecurity and Public-Private Collaboration

We lead the development of technical specifications and cybersecurity standards that underpin secure and resilient digital infrastructure through active engagement in public-private working groups. CableLabs' contributions have shaped national policy and are frequently recognized and cited by federal agencies — including the National Institute of Standards and Technology (NIST), the National Cybersecurity Center of Excellence (NCCoE), the National Telecommunications and Information Administration (NTIA), the Office of the National Cyber Director (ONCD), the Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Communications Commission (FCC) — reinforcing our role as a trusted partner in securing America's digital infrastructure.

CableLabs actively contributes to the work in key standards development organizations and public-private working groups (see representative logos below). We also collaborate closely with federal, state and local governments — as well as cross-sector partners such as the Communications Sector Coordinating Council (CSCC) — to advance critical information sharing and incident response initiatives in direct support of national security and emergency preparedness efforts to protect critical infrastructure.