White paper

AT&T Business

Quantum computing and AI may break digital security as we know it

Why carrier-scale networks are our best defense

This paper is for informational purposes only and does not constitute a guarantee or warranty of any security outcome, product performance, or service availability. No security solution can guarantee complete protection against all threats. Third-party data cited herein has not been independently verified by AT&T.

Executive summary

The cybersecurity landscape is undergoing a structural transformation driven by two converging forces: artificial intelligence and the impending advent of cryptographically relevant quantum computing. Artificial intelligence has collapsed the attacker kill chain from days or weeks into minutes, enabling automated reconnaissance, exploitation, lateral movement, and social engineering at machine speed. Quantum computing, while still emerging, poses an existential threat to the public key cryptography that underpins digital trust, identity, and secure communications across global enterprises.

This is not an argument that the network replaces identity, endpoint, or application security. Those layers remain essential and are converging on their own trajectories. The argument is narrower and stronger: the network is the only layer with the topology, scale, and inline position to absorb high-volume, machine-speed attack traffic before downstream controls are ever engaged, and it is the only layer where cryptographic transition can be governed centrally rather than negotiated application by application.

Traditional enterprise security architectures, built around discrete controls at the endpoint, perimeter, and application layers, are increasingly unable to operate at the scale, speed, and visibility required to counter these threats. Fragmented tooling, human-dependent response loops, and asymmetric visibility leave organizations reactive rather than resilient.

This paper argues that the network itself must evolve into a primary security control point. Carrier-scale networks uniquely combine global reach, pervasive visibility, and inline enforcement capabilities that no single enterprise can replicate. When infused with AI-driven analytics and designed for cryptographic agility, the network becomes an active and adaptive security fabric capable of detecting, deciding, and enforcing security controls at machine speed upstream of enterprise infrastructure.

We outline how AI-enabled and quantum-safe networks redefine defense in depth, reduce enterprise operational burden, and establish a foundation for security that is resilient not only to today's threats, but also to the next era of digital risk.

The evolution of cybersecurity

Rule-based and perimeter-centric security

Early enterprise security architectures assumed that a small number of controlled choke points could meaningfully separate trusted internal users from untrusted external traffic. Security programs relied on signature-driven detection, static access control lists, and perimeter firewalls that enforced policy on north-south flows. That model produced results when infrastructure was on premises, identities were relatively stable, and attacker tooling was less automated.

The limitations of this era are increasingly visible in modern incident data. Even in organizations with mature perimeter controls, compromise frequently begins with web applications, identity abuse, and externally exposed services not always related to malware on endpoints. Frontline incident-response data from Mandiant indicates that vulnerability exploitation and credential misuse dominate initial access vectors, while industry telemetry from Microsoft and CrowdStrike shows attackers increasingly operating through identity systems and trusted services rather than traditional endpoint malware.

Why not simply SASE?

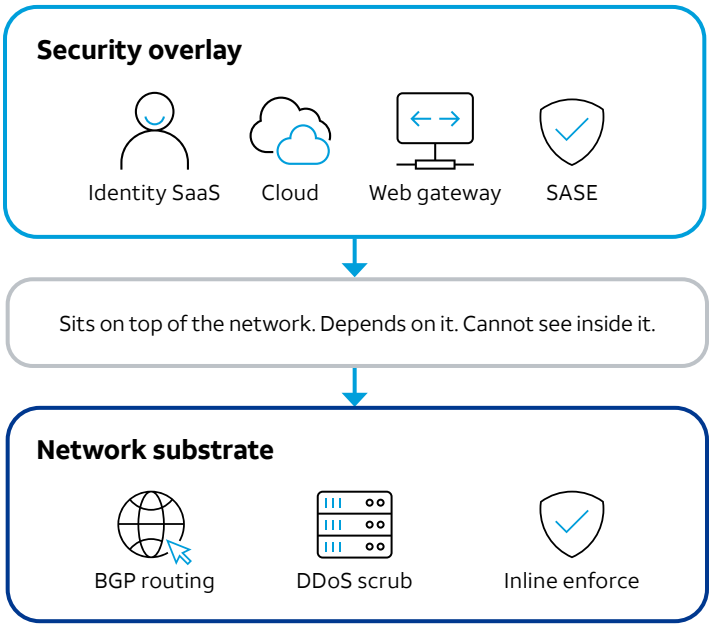
A natural question is whether Secure Access Service Edge (SASE) and Security Service Edge (SSE) platforms already deliver this model. They deliver part of it. Cloud edge security platforms collapse multiple enterprise controls into a single inspection point closer to the user, and that is genuinely transformative for Software as a Service (SaaS)-bound and remote user traffic. What they do not deliver is the underlying transport itself. They sit on the overlay and depend on someone else's Border Gateway Protocol (BGP) announcements, inheriting the carrier's view of malicious infrastructure rather than producing it.

Carrier-embedded security is differentiated where the network is the substrate: anti Distributed Denial-of-Service (DDoS) at scrubbing capacity an enterprise overlay cannot reach, BGP and route origin defense, protective Domain Name System (DNS) at resolver scale, and inline enforcement on private connectivity such as dedicated internet, Multiprotocol Label Switching (MPLS), Software-Defined Wide Area Network (SD-WAN), and 5G network slices that never traverse an SSE point of presence. The two models are complementary, not competing, and most mature enterprise architectures will use both.

Network architecture

Why the carrier network is different from SASE

SASE and SSE deliver real value as a security overlay. What they cannot deliver is the underlying transport and the enforcement that lives inside it.



SASE delivers real value on the overlay

Cloud edge security platforms collapse multiple enterprise controls into a single inspection point closer to the user. That is genuinely transformative for SaaS and remote user traffic.

The overlay sits on someone else's network

SASE only secures what it sees on top of an underlay it doesn't control. It can't touch MPLS, private 5G slices, or locally-broken-out internet that bypass the PoP entirely.

The carrier is the substrate, not the overlay

The carrier is the substrate, not the overlay, which provides two things no overlay can replicate: it defends the routing layer itself, BGP origin validation, hijack and route-leak defense beneath anything SSE can see, and it enforces inline on private paths that never reach a PoP. It also brings underlay-scale DDoS scrubbing and resolver-scale protective DNS, where the edge is volume rather than exclusivity. The models cover different layers; mature enterprises run both.

Zero Trust and identity-centric models

Zero Trust shifted policy enforcement toward identity, device posture, and continuous authorization. Practically, this produced distributed control planes: identity providers, conditional access policies, endpoint posture agents, and cloud access enforcement. The model is directionally correct, but it introduces operational fragmentation when policies are split across identity systems, endpoint management, SaaS controls, secure web gateways, and multiple cloud providers.

This fragmentation also increases the number of telemetry pipelines, alert streams, and integrations the Security Operations Center (SOC) must maintain. IBM's "Cost of a Data Breach Report" shows that detection and response remain major cost drivers in breaches, and the average cost of a breach was $4.44M in 2025.

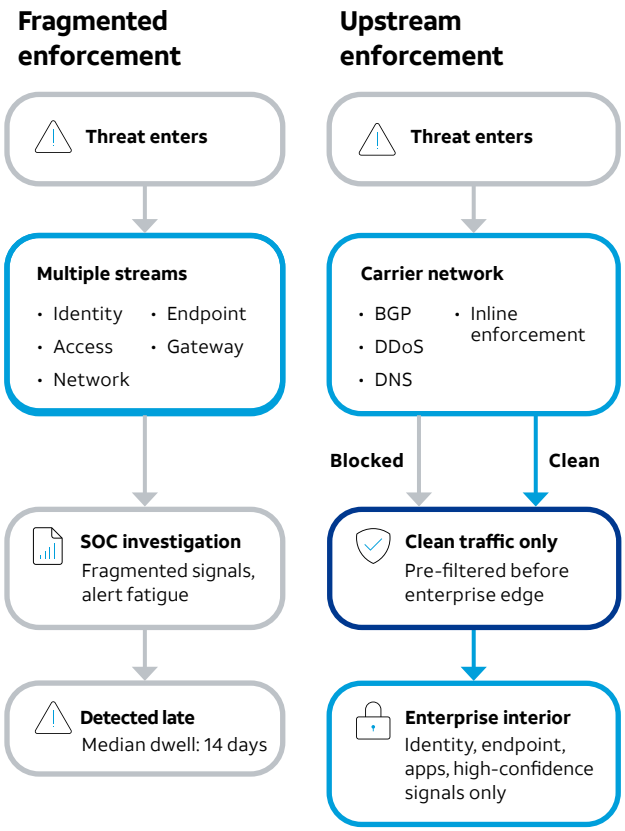
The limits of endpoint and identity saturation

Enterprises now deploy large security stacks yet still struggle with speed and scale. A key constraint is that endpoint and identity controls often detect too late in the sequence. Well after initial access has already occurred and lateral movement has begun. Mandiant reports a global median dwell time of 14 days in 2026, with specific categories like cyber espionage having an average dwell time of 122 days. It also notes that red team operators often need only 5 to 7 days to achieve objectives, meaning many environments can still be operationally compromised before defenders can intervene.

This is the strategic gap that shifts attention back to upstream control points. The closer security enforcement is to the traffic entry point, the earlier malicious flows can be disrupted, reducing the probability that an attacker ever reaches identity systems, endpoints, or internal application tiers.

Zero trust architecture

Fragmented vs. upstream enforcement



Zero Trust is right

Zero Trust is the right architecture. But independent systems produce independent alert streams with no shared upstream view. The SOC absorbs all of it, correlating signals across tools that were never designed to talk to each other. Threats do not break through controls. They navigate the gaps between them. Every hour a threat spends in those gaps is time it uses to establish persistence, expand access, and cause the kind of disruption that takes months to fully remediate.

Upstream enforcement reduces the blast radius

The carrier network is the one enforcement point that sits upstream of all of them. It sees the threat before it reaches any downstream control. Those gaps do not close by adding more controls downstream. They close by intercepting them at the carrier layer, before high-volume attack traffic, credential abuse, scanning, and DDoS ever generate a downstream alert. The downstream controls are no longer crowded with noise they were not built to absorb; the SOC operates on a smaller, higher-confidence signal set.

The two models are complementary, not competing

Upstream enforcement does not replace Zero Trust. It does not handle identity policy, device posture, or application-level access control. What it removes is the volume problem that makes those controls expensive to operate. The network determines whether traffic reaches the door. Zero Trust determines what it is permitted to do once inside. Organizations that operate both reduce SOC load during attack conditions and shorten mean time to containment. Analysts investigate fewer false positives and more real ones. Security teams do more with what they already have.

AI-driven threat acceleration

Compression of the attack lifecycle

AI changes attacker economics in three practical ways.

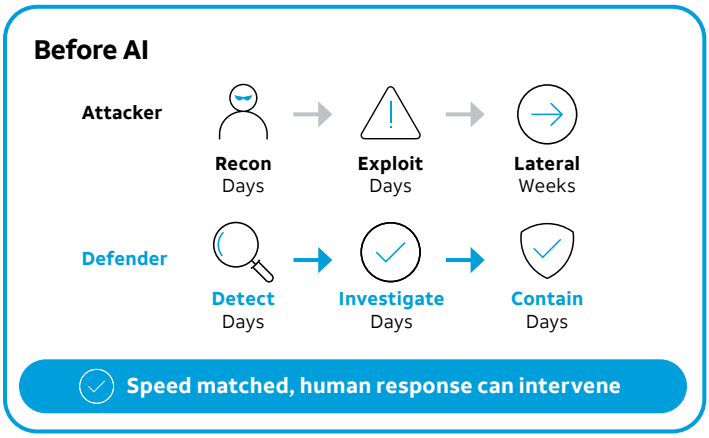
First, reconnaissance is now massively parallel. Adversaries can enumerate exposed assets, test credential reuse, and identify vulnerable service versions at scale with automation pipelines. Second, social engineering is becoming more targeted and linguistically convincing because message generation and personalization costs approach zero. Third, exploitation and post-exploitation can be orchestrated with automation frameworks that select tactics dynamically based on defender responses.

Modern reporting reinforces that speed is decisive. IBM reports that organizations using security AI and automation had a 108-day shorter breach lifecycle in 2023 than those that did not, demonstrating that time to detect and contain is a measurable business outcome, not a theoretical goal.

AI-driven threat acceleration

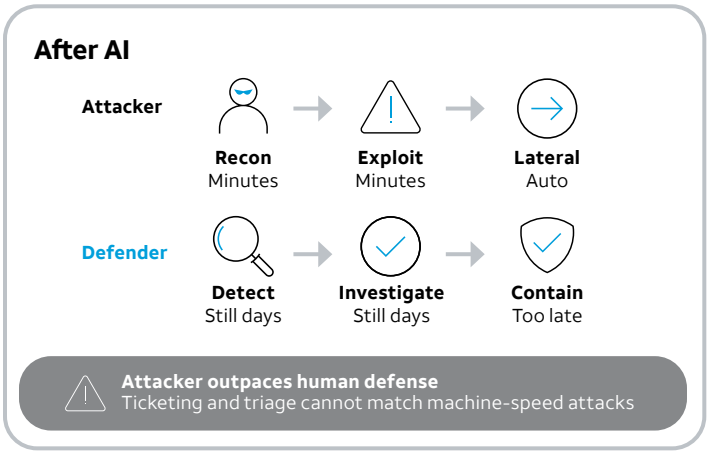
AI compresses the attack lifecycle

The attacker's kill chain has collapsed from days to minutes. Defender response times have not kept pace. Without automation, the gap is structural.



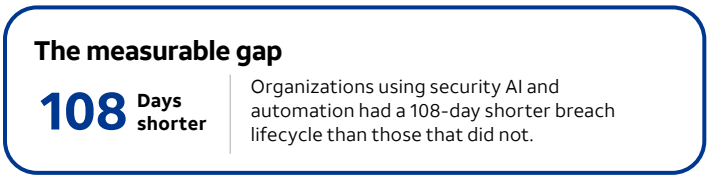
Before AI, attacker and defender operated at similar speed

Manual reconnaissance took days. Exploit development took days. Lateral movement took weeks. Defenders had imperfect time, but enough to detect and respond before full compromise. Human response loops could intervene.



After AI, the kill chain collapses to minutes

Reconnaissance is now massively parallel. Exploitation frameworks select tactics dynamically based on defender responses. Lateral movement is orchestrated automatically. Defender response times have not changed. The gap is structural and the first layer of defense must autonomously to close it.



Speed is a measurable business outcome

IBM's "Cost of a Data Breach Report" quantifies the gap: organizations using security AI and automation had a 108-day shorter breach lifecycle. A network-embedded control plane applies policy at wire speed before internal systems incur load or logs explode into alert fatigue.

Human-in-the-loop is no longer viable at scale

Humans remain essential for investigation quality, governance, and high-impact decisions, but the first layer of defense must operate autonomously. This is especially true for high-volume events such as scanning floods, credential stuffing attempts, and volumetric DDoS. Industry reports indicate that global DDoS activity now reaches millions of attacks within months, with individual events scaling to 30 Tbps and beyond, underscoring both the frequency and magnitude of modern attacks and the need for automated mitigation at machine speed.

The practical implication is that defenses dependent on ticketing workflows and manual triage cannot match the event rate. A network-embedded control plane can apply policy at wire speed, upstream of enterprise infrastructure, before internal systems incur load or logs explode into alert fatigue.

AI-enabled attack patterns that stress traditional controls

- **Adversary-in-the-middle credential theft:** Attackers proxy authentication flows to capture tokens and session artifacts, bypassing basic multi-factor prompts. The initial signal often appears as normal web traffic until correlated with identity telemetry and device posture. The earlier suspicious traffic patterns are flagged, the less likely token replay becomes operationally useful.
- **Rapid vulnerability exploitation:** Industry research highlights how quickly threat actors move from discovery to active exploitation compared with enterprise remediation timelines. Studies from Mandiant indicate attackers can weaponize vulnerabilities in as little as five days on average, while organizations often require significantly longer to remediate exposures at scale, creating a persistent risk gap.
- **Botnet-sourced DDoS and service degradation:** When attacks peak at multi-terabit rates, control must exist in provider infrastructure, not only on customer premises. The carrier's distinct contribution includes scrubbing at peering ingress, BGP and route origin defense against attacks that target the transport itself, and inline enforcement on private connectivity such as SD-WAN, 5G slicing, MPLS, and dedicated internet.

Quantum computing and cryptographic risk

The cryptographic dependency problem

Public key cryptography underpins almost every trust decision in enterprise computing. Transport Layer Security (TLS), Internet Protocol Security (IPsec), Secure Shell (SSH), code signing, certificate-based authentication, and secure email depend on primitives such as RSA and elliptic curve cryptography. Quantum algorithms such as Shor's algorithm can theoretically break these primitives once cryptographically relevant quantum computers exist, which would undermine confidentiality, integrity, and non-repudiation at scale.

Standards are now concrete and actionable

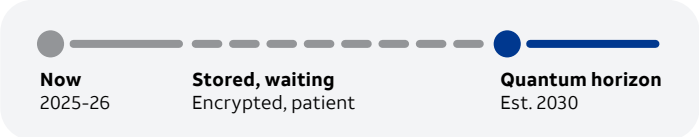
Quantum readiness is no longer abstract because standards exist. The National Institute of Standards and Technology (NIST) released its first finalized post-quantum encryption standards on August 13, 2024, and encouraged organizations to begin transitioning as soon as possible. These standards are FIPS 203 for general encryption using ML-KEM, FIPS 204 for digital signatures using ML-DSA, FIPS 205 for digital signatures using SLH-DSA, and FIPS 206 related to FALCON.

The National Security Agency (NSA) sets explicit milestones for software and firmware signing and for updates to traditional networking equipment.

Quantum computing risk

Harvest now, decrypt later

Adversaries are capturing encrypted data today and storing it until quantum computers can break the encryption. The threat is active now, not in the future.



Adversary captures encrypted data

Traffic is intercepted and stored wholesale today. The encryption is irrelevant. The attacker just needs the data to outlive the algorithm protecting it.

Happening now

Unreadable today. Waiting for a key that does not yet exist.

Quantum breaks RSA and ECC

Shor's algorithm renders RSA, elliptic curve, and current TLS-protected data readable. Years of stored encrypted traffic become exposed simultaneously.

Est. 2030s

Data most at risk today

- **IP and trade secrets** — Competitive intel
- **Customer records** — Personally Identifiable Information (PII), identifiers
- **Healthcare data** — Protected Health Information (PHI), clinical records
- **Regulated financials** — Transactions, accounts

The threat is active today, not in the future

Adversaries do not need quantum computers to start this attack. They can capture and store encrypted traffic now and wait. Any data with a secrecy lifetime longer than the quantum timeline is already at risk, regardless of how strong today's encryption is.

When quantum arrives, years of stored data become exposed

Shor's algorithm breaks RSA and elliptic curve cryptography, the primitives underpinning TLS, IPsec, SSH, and code signing. NIST finalized post-quantum standards on August 13, 2024: FIPS 203, 204, 205, and 206. These are not experimental. Migration should begin now.

Long-lived data is the highest priority to protect first

Start with the highest-sensitivity, longest-lived data flows: executive communications, regulated data exchanges, and high-value IP replication. Migration timelines are dictated by protocol readiness. TLS 1.3 is required for post-quantum mechanisms. Most enterprises are further behind than they realize.

Harvest now, decrypt later makes this a current risk

Adversaries can capture encrypted data today and decrypt it later once quantum capabilities mature. This is particularly relevant for data with long secrecy lifetimes: intellectual property, customer records, healthcare information, and regulated financial data. CISA, NSA, and NIST guidance emphasize the need for early planning and migration roadmaps precisely because long-lived data can be targeted now.

Why the migration is hard

The hard part is not only swapping algorithms. The hard part is inventory and dependency discovery. Cryptography exists in libraries, appliances, embedded firmware, hardware roots of trust, signed boot chains, third-party SaaS, and private application code. Best practice is a Cryptographic Inventory and Agility approach: discovery of cryptographic artifacts across repositories and infrastructure, centralized policy management, and a cryptography Application Programming Interface (API) layer to abstract algorithm choices.

Why the network is the strategic control point

Visibility at a scale enterprises cannot replicate

Large-scale service provider networks observe threat activity at a scope that individual enterprises cannot replicate. These networks carry hundreds of petabytes of traffic each day across global infrastructure, creating broad visibility into emerging attack patterns, malicious behaviors, and systemic risk trends. Over the next five years these numbers are forecasted to cross into the exabytes. This level of traffic scale directly improves the ability to identify threats early and apply protective controls upstream before malicious activity reaches enterprise environments.

Two structural caveats are worth naming directly: (1) Encryption is reducing payload visibility, especially with TLS 1.3, and (2) the share of enterprise traffic traversing a carrier WAN is shrinking as workloads move to SaaS and as cloud-to-cloud private interconnects bypass the public internet entirely. The case for carrier relevance holds because what the carrier uniquely sees is not packet contents but infrastructure behavior: BGP anomalies and route hijacks, DNS resolution patterns at resolver scale, and the early shape of volumetric attacks before they reach a target's edge. These signals do not require payload inspection and remain unavailable to controls positioned inside the enterprise.

Inline enforcement before customer infrastructure

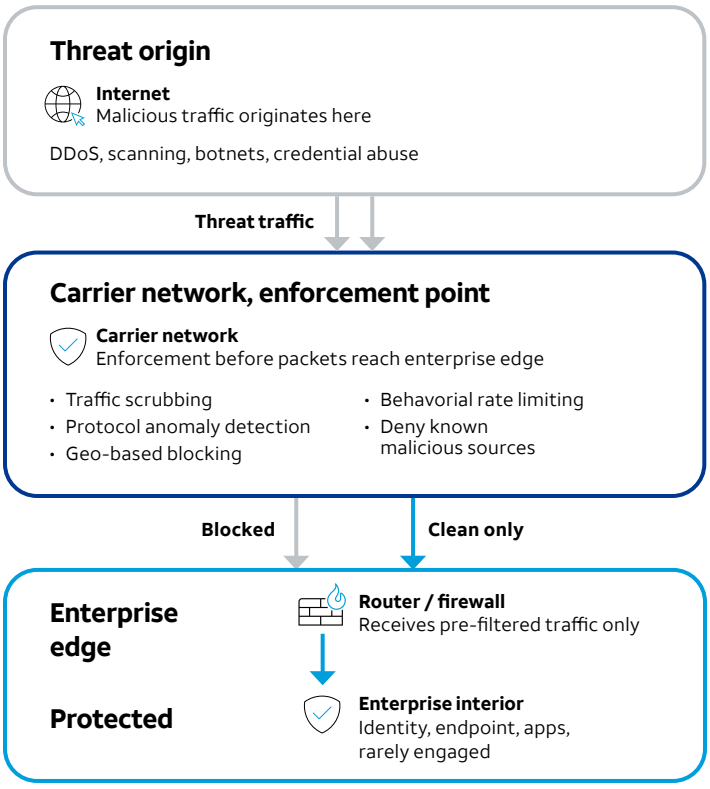
The most significant security advantage of network-embedded defense is not simply broader detection, but inline enforcement that occurs upstream of customer infrastructure. When malicious traffic is filtered, rate-limited, or blocked within the service provider network itself, threats can be mitigated before they consume enterprise bandwidth, reach exposed services, or generate downstream alerts. This enforcement model consolidates protection into the connectivity layer, reducing dependence on additional on-premises appliances or cloud-based overlays and ensuring controls are applied consistently across all traffic entering the enterprise environment.

This upstream positioning is critical because many high-impact attacks depend on touching a vulnerable surface inside the enterprise perimeter. Examples include volumetric and application-layer DDoS attacks that exhaust edge capacity, automated scanning and exploitation of unpatched VPNs or management interfaces, credential stuffing against externally exposed authentication endpoints, and bot-driven abuse targeting public web applications. Inline network enforcement can disrupt these attack classes through traffic scrubbing, protocol anomaly detection, behavioral rate limiting, geo-based blocking, and automated denial of known malicious sources before packets ever reach customer routers, firewalls, or servers.

Network-embedded defense

Enforcement upstream of your infrastructure

The most significant security advantage is not broader detection. It is enforcement that occurs before threats reach enterprise bandwidth, services, or downstream controls.



High-impact attacks depend on reaching your perimeter

Volumetric DDoS, automated scanning of unpatched VPNs, credential stuffing against externally exposed endpoints, and bot-driven web abuse all require touching a vulnerable surface inside the enterprise perimeter. Upstream enforcement removes that opportunity before packets ever arrive.

Enforcement inside the carrier network is the key difference

When malicious traffic is blocked within the service provider network itself, threats are mitigated before they consume enterprise bandwidth, reach exposed services, or generate downstream alerts. This consolidates protection into the connectivity layer and reduces dependence on additional appliances or cloud-based overlays.

Upstream filtering benefits even mature security stacks

Even enterprises with mature endpoint detection, identity protection, and Security Information and Event Management (SIEM) platforms benefit from removing low-fidelity, high-volume attack traffic early in the traffic path. Suppressing noise before it generates downstream alerts preserves analyst capacity for higher-confidence investigations and shortens mean time of containment.

Blocked at carrier, never reach enterprise

- Volumetric DDoS
- Automated scanning
- Unpatched VPN exploits
- Credential stuffing
- Bot-driven abuse

Operational outcomes

Analysts on higher-confidence signals, infrastructure load reduced, mean time to containment shortened, attack sequences stopped before initial success

Measurable outcomes in network-embedded security

Real-world deployments of network-embedded security demonstrate the operational impact of upstream enforcement at scale. Large service provider networks routinely process and analyze trillions of data flows daily, often identifying tens of thousands of threats per day, and mitigate billions of malicious events per month, including scanning traffic, credential abuse, botnet-sourced attacks, and volumetric denial-of-service attempts, well before those flows ever reach enterprise environments. Because enforcement occurs inline within the provider infrastructure, mitigation can often be deployed within seventeen minutes of service activation, rather than relying on customer-side appliance deployment or manual configuration.

Independent industry analyses and practitioner case studies consistently show that upstream controls achieve high efficacy against high-volume commodity threats such as automated exploitation, post-exploitation command-and-control traffic, and abuse originating from known malicious regions or networks. In healthcare and financial services, organizations have reported hundreds of millions of malicious connection attempts blocked within the first day of activation when network-level protections are enabled ahead of enterprise ingress points.

These outcomes illustrate why upstream enforcement is operationally efficient. Even enterprises with mature endpoint detection, identity protection, and SIEM platforms benefit from removing low-fidelity, high-volume attack traffic early in the traffic path. By suppressing noise before it generates downstream alerts, network-embedded controls preserve analyst capacity for higher-confidence investigations, reduce infrastructure load during attack conditions, and shorten mean time to containment.

AI-enabled networks

What “AI-enabled” means in a network context

In networking, AI-driven security is not only about classification models. It is about a full closed-loop system:

- Telemetry ingestion at scale across network edge and core
- Feature extraction from flow metadata, protocol behavior, and anomaly patterns
- Detection decisions with confidence scoring
- Policy enforcement through automated controls such as dynamic blocking, rate limiting, and routing actions
- Feedback loops that validate outcomes and reduce false positives over time

Service provider threat intelligence platforms increasingly leverage machine learning and artificial intelligence to continuously adapt detection logic as attacker techniques evolve. Rather than relying solely on static, signature-based controls, these systems incorporate behavioral analysis, anomaly detection, and feedback loops to update models in near-real time, enabling security controls to respond dynamically to new attack patterns, infrastructure shifts, and changing traffic behaviors.

Behavioral analytics without decrypting payloads

Increasing encryption reduces payload visibility, pushing security programs toward metadata and behavior. Flow analytics can detect scanning behaviors, beaconing patterns, impossible travel characteristics in session establishment, and protocol misuse without decrypting content. The network sees the earliest timing and volumetric indicators, which is critical in high-speed attack sequences.

Autonomous response and self-healing

Autonomous response in network-embedded security should be narrowly scoped, reversible, and governed by explicit policy. Mature implementations support capabilities such as geo-based traffic filtering, configurable web and protocol controls, stateful firewall enforcement, application-aware policy, and comprehensive reporting and logging. These capabilities are typically integrated with configuration versioning and change control mechanisms that allow security teams to restore prior policy states quickly if unintended disruption occurs.

That version control capability is critical in practice. Modern SOC operations require rapid response to emerging threats, but rapid change also increases the risk of misconfiguration or over-blocking. Safe automation depends on controlled policy deployment, staged rollout where appropriate, and the ability to rapidly roll back changes. Without these safeguards, autonomous controls can introduce operational instability even as they improve defensive speed.

Protecting AI workloads themselves

AI workloads increase both value and risk. They create new high-value data sets and APIs, and they amplify the consequences of data leakage. Network-embedded controls can protect training data movement, restrict access to inference endpoints, and enforce segmentation between AI components and the rest of the enterprise. This is increasingly relevant as AI services become distributed across clouds, edge sites, and on-premises environments.

Quantum-safe network architecture

Crypto agility as a network capability

Crypto agility means the ability to change algorithms without rewriting everything. In practice, this requires three capabilities:

- Cryptographic discovery and inventory to identify where vulnerable cryptography is used
- Policy-based algorithm selection so enforcement is centrally governed
- Abstraction layers so application teams are not forced to do large rewrites for every transition

Together, these elements allow organizations to introduce new cryptographic primitives—including post-quantum algorithms—without requiring extensive application rewrites by development teams.

TLS version and protocol prerequisites

Post-quantum adoption is constrained by protocol support. Modern implementations require TLS 1.3 or higher to support post-quantum cryptographic mechanisms for secure communication between clients and servers. Earlier TLS versions lack the extensibility and handshake properties necessary to integrate hybrid or post-quantum algorithms in a standards-compliant way.

This constraint matters because many enterprises continue to operate legacy TLS deployments, embedded systems, and third-party integrations that cannot be readily upgraded. As a result, cryptographic migration timelines are often dictated by protocol readiness rather than algorithm availability. Network platforms that can discover, classify, and report TLS versions in use across traffic flows provide a practical mechanism to accelerate post-quantum readiness.

Post-quantum cryptography (PQC) in transit

A phased approach is the only workable approach:

- Start with the highest-sensitivity, longest-lived data flows: executive communications, regulated data exchanges, and high-value IP replication
- Adopt hybrid approaches where classical and PQC mechanisms coexist, so compatibility is maintained while migration progresses
- Expand coverage to broad traffic categories once client and server dependencies are remediated
- NIST emphasizes that the new standards are ready for immediate use and encourages administrators to begin transitioning

Managed quantum-safe connectivity

Managed quantum-safe connectivity can be understood as a control plane for cryptographic transition rather than a collection of point solutions. Such an approach reduces enterprise burden by standardizing cryptographic inventory and discovery, providing protocol and algorithm compatibility guidance, centralizing enforcement and policy control, and supporting ongoing policy updates as standards evolve. By abstracting cryptographic changes behind managed controls, organizations can migrate incrementally without forcing immediate, large-scale application or infrastructure rewrites.

Industry roadmaps commonly describe quantum readiness capabilities such as automated cryptographic inventory services, quantum-resistant identity and keying mechanisms, quantum-safe point-to-point or virtual private network connectivity, and network-mediated key establishment or distribution models. Together, these capabilities reflect an architectural shift toward managed cryptographic services that help organizations transition to post-quantum standards while minimizing operational complexity.

Conclusion

Reshaping enterprise security

Artificial intelligence and quantum computing are driving a fundamental redesign of enterprise security architecture. AI compresses the attack lifecycle by enabling automated reconnaissance, exploitation, and lateral movement at machine speed, while quantum computing threatens the public key cryptographic primitives that underpin authentication, confidentiality, and integrity across digital systems. Together, these forces expose structural limits in security models that rely primarily on downstream detection and human-paced investigation after compromise has already occurred.

The network is increasingly positioned as a primary security control point because it provides upstream visibility and the ability to enforce policy inline before malicious activity reaches enterprise infrastructure. At this layer, security controls can observe traffic behavior at scale, correlate signals across large and diverse traffic populations, and apply preventative actions such as filtering, rate limiting, or traffic shaping prior to consumption of customer bandwidth or processing resources. This upstream enforcement reduces the probability that attacks reach identity systems, endpoints, or application tiers and limits the operational impact of high-volume threats.

In the next phase of cybersecurity architecture, resilient organizations will emphasize earlier intervention in the traffic path, automated response for high-frequency and high-velocity attack classes, and cryptographically agile designs that support incremental migration to post-quantum standards. These approaches shift security outcomes from reactive containment toward proactive risk reduction by minimizing attacker opportunity, reducing dwell time, and maintaining trust as cryptographic assumptions evolve.

Why AT&T Business

See how ultra-fast, reliable fiber, protected by built-in security, and 5G connectivity give you a new level of confidence in the possibilities of your network. Let our experts work with you to solve your challenges and accelerate outcomes. Your business deserves the AT&T Business difference—a new standard for networking.

To learn more, contact your AT&T Business representative or click here.