Forge Your **Modern Edge Solutions**

A complete guide to network architectures for control, cost and connectivity

For many organizations, IT environments have become highly dispersed with the expansive nature of business today. This ebook explores the advantages of the modern edge, and how organizations can use it to meet the needs of the modern network perimeter while optimizing costs and connectivity.

Table of contents

Leading with the modern edge

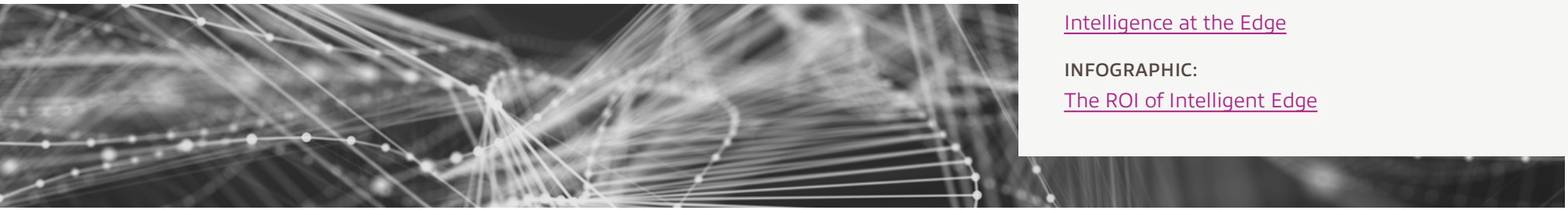
The modern edge plays an important role in optimizing control, costs and connectivity in today's highly dispersed IT environments. 39% of organizations are prioritizing the modernization of legacy infrastructure and networking technology in 2023,[1] and there are a number of modern edge solutions to help you solve today's toughest network challenges, support business operations and drive digital innovation.

The modern edge:

The modern edge is the evolution of the network perimeter. Made up of traditional networks, cloud networking, Wi-Fi connectivity, 5G and Virtual Private Networks (VPNs), it is the network environment that connects people, devices and data across a world of locations. The effective modern edge is characterized by automation, security integration and next-level service capabilities. Leveraging the Internet of Things (IoT) and compute at the edge for advanced network functionality is referred to as the intelligent edge.

Organizations that neglect to embrace modern methods of managing the network and the entities on it can easily find themselves left behind. Challenges like increasingly complex requirements, end-of-support technologies, lack of visibility, etc., can hinder your organization from doing business effectively and accomplishing your digital transformation goals.

As you navigate new network complexities and increased demands on connectivity and security, let this ebook be a resource to guide you through some of your available options and the benefits they offer.



Learn more about the modern edge.

Explore these resources for more context on what it means to implement and manage a secure, scalable and reliable modern network edge.

EBOOK:
Take Advantage of the Intelligent Edge to Leverage Valuable and Extensive Data

LINKEDIN LIVE:
Edge is the New Perimeter — How to Connect and Secure the Modern Edge

VIDEO:
Delivering Transformation to the Modern Edge

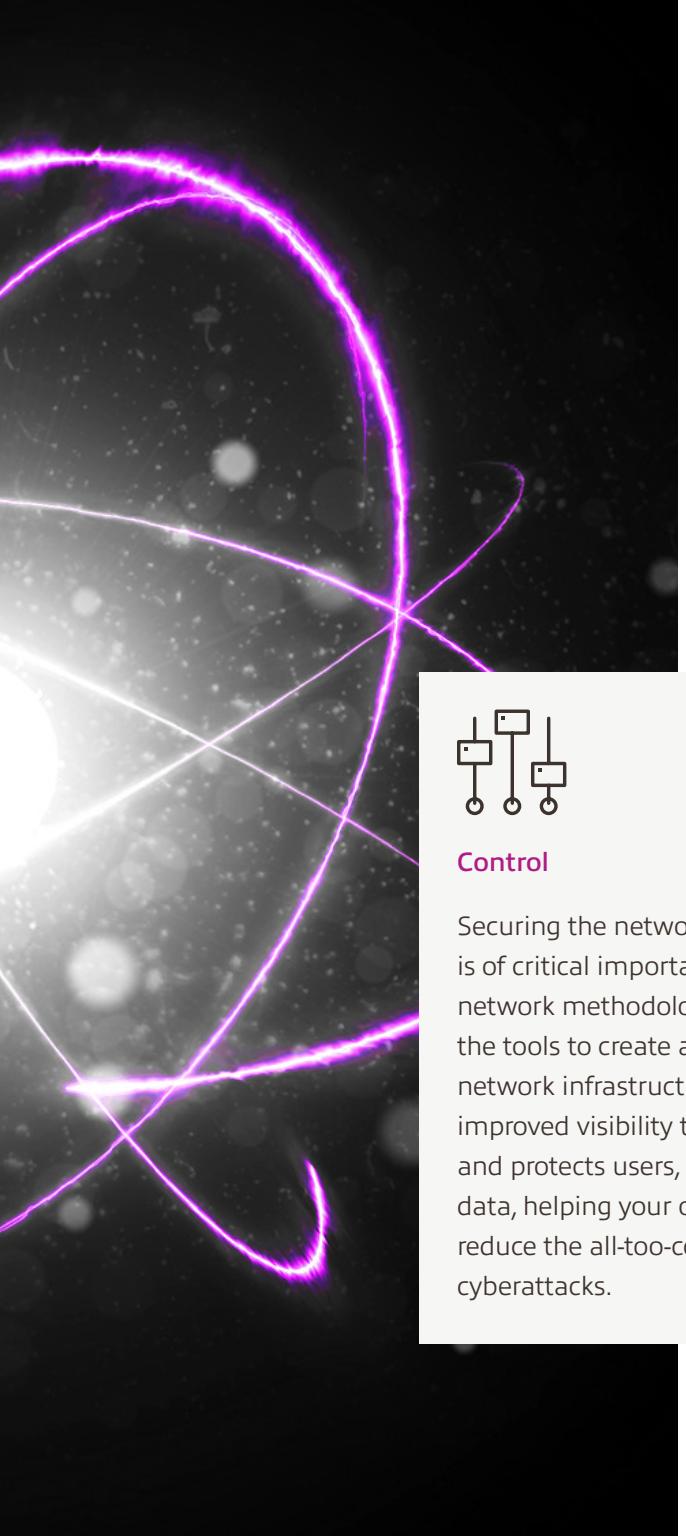
LINKEDIN LIVE:
Taking the Intelligent Edge From Idea to Deployment

WHITEPAPER:
From Edge to Center: Key IoT Considerations for Enterprises

BLOG:
Simplifying the Conversation Around Edge Security

INFOGRAPHIC:
Intelligence at the Edge

INFOGRAPHIC:
The ROI of Intelligent Edge



Addressing network challenges at scale

As you scale, your edge is the number of devices on your network and the surface area of those devices. While most are familiar with standard networking practice, the scope and scale of today's networks makes it very challenging to keep devices up to date, patched, managed and secure. The challenges themselves are not new — the magnitude is.

Modern network management offers solutions for today's top network challenges at any scale: control, cost-effectiveness and connectivity.

Control

Securing the network environment is of critical importance. Modern network methodologies give you the tools to create a defensible network infrastructure with improved visibility that prioritizes and protects users, endpoints and data, helping your organization reduce the all-too-common risks of cyberattacks.

Cost-effectiveness

Technical debt is the result of adopting shortcut solutions that create more work and added costs in the long run. If you have EOL or EOS hardware or software, refreshing your network infrastructure can help you pay off technical debt with efficiencies that pay dividends over time and reduce costs overall.

Connectivity

In today's work-anywhere environment, enabling the modern workforce is a pillar of business success. You need network solutions that enable your employees to work anywhere, with secure and reliable access to the data and applications they need to stay productive.

The tenets of modern network management

To address the above challenges requires following best practices for an effectively managed network, including segmentation and microsegmentation, identity and access management, automation and solutions for visibility and control.

Segmentation & microsegmentation

Modern network segmentation practices and technologies rely on logical, dynamic groupings of different users with different access rights to company systems. Deployed correctly, segmentation makes it easier to automatically grant access to only those systems that are needed for different groups — from corporate executives to human resources, down to guests and contractors who may access the network from external devices. The level of granularity of network segmentation now available also allows organizations to deploy fine-grained microsegmentation of different groups and resources.

Explore additional solutions for network security in our whitepaper Transforming Network Security: How to Win Against Cyberthreats.

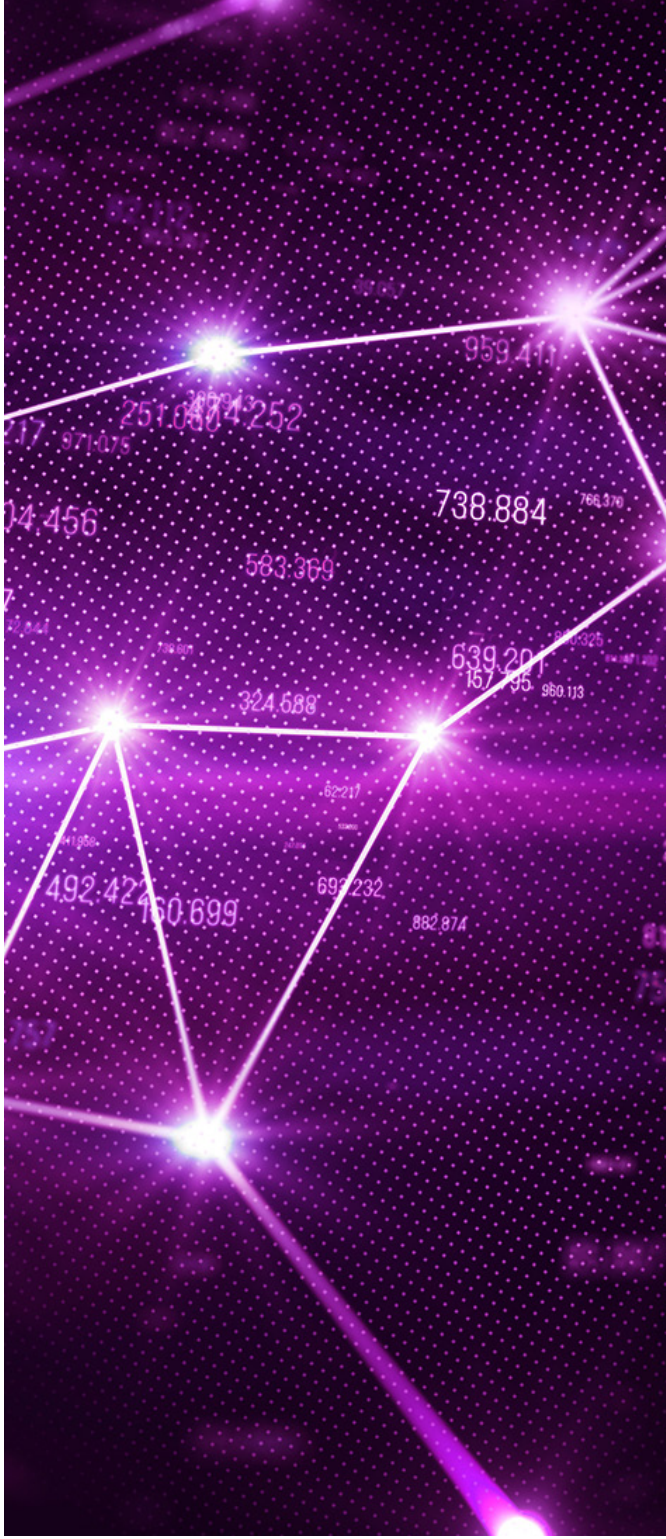
Identity & access management

A secure edge comes down to network access control — which is identity-based permissions and IT access. And one of the biggest takeaways in the edge security discussion is that identity is the key to assigning policies and permissions that will protect your network and data.

This includes implementing solutions such as:

- Multi-Factor Authentication (MFA)
- Device fingerprinting
- User profiling
- Behavioral analysis

You can read more about leveraging solutions for identity and access management in our blog post Simplifying the Conversation Around Edge Security.



Automation

Using software-enabled instructions and repeatable, scalable processes, you can simplify your networks with automation. Automation works to streamline processes like policy creation, governance and threat containment, helping you reduce manual tasks, increase security, deliver more resilient network resources, and improve provisioning speed and network efficiencies. Additionally, the system and process efficiencies gained from automation can ultimately help reduce technical debt both short and long term.

Learn more about automation.

Browse these resources to learn more about how automation can help you modernize your network infrastructure.

WHITEPAPER:
Ready to Modernize IT? Start With Automation.

CLIENT STORY:
Pharmaceutical Research Organization Overhauls and Upgrades Entire Network Infrastructure

VIDEO:
Modernization Through Network Automation

Visibility & control

As traffic on enterprise networks increases, it's common to lose visibility of exactly what and who is on the networks. 35% of organizations cite a lack of visibility into the threat landscape as the main business challenge with respect to cybersecurity.[2] When you can't see what's accessing your networks in real time, you face an even bigger challenge proactively securing your networks, devices and users against threats. The scope of the modern network results in a larger attack surface, which makes organizations more vulnerable to cybersecurity incidents.

Visibility is not only tied to security concerns; effective management requires optimization of resources and traffic. Knowing what is happening on your network at all times gives you increased control over threats and over utilization, performance and related costs.

Learn more about increasing your visibility and control.

Browse these resources to learn how Cybersecurity Mesh Architecture can help your organization streamline security insights.

BLOG:
Leveraging Decentralized Intelligence & Security: Cybersecurity Mesh Architecture

INFOGRAPHIC:
Putting Expansive Intelligence to Work: Cybersecurity Mesh Architecture

Three core approaches to network modernization

In addition to these key principles of modern network management, there are three core approaches to modern networking that come up in our conversations with clients around control, cost and workforce connectivity. These are Secure Access Service Edge (SASE), modern wireless solutions and the Zero Trust framework. These approaches help organizations solve security, technical debt and remote work challenges with technology solutions that strengthen, secure and unify the network architecture.

1. SASE & SD-WAN

The Secure Access Service Edge (SASE) model unifies traditionally siloed networking and security services in a cloud-centric environment with a single management point to help organizations move away from legacy data center-oriented security models and create a comprehensive, cloud-first security posture.

Understanding SASE

Rather than a singular tool or technology, SASE is a concept that defines the convergence of networking and security services within a cloud-based architecture that unifies security and delivers reliably secure connectivity for endpoints and remote offices to private and cloud-hosted services. The SASE approach builds in familiar security architectures and capabilities, including:

- DNS-Layer Security
- Secure Web Gateways (SWG)
- Next-Generation Firewalls (NGFW)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)
- SD-WAN

The goal of SASE is to combine these architectures for a scalable environment that delivers direct internet access, secure applications, and stronger protection against cyberthreats and security concerns. Ideally, a well-architected SASE approach will enable organizations to:

Reduce latency

Improve visibility

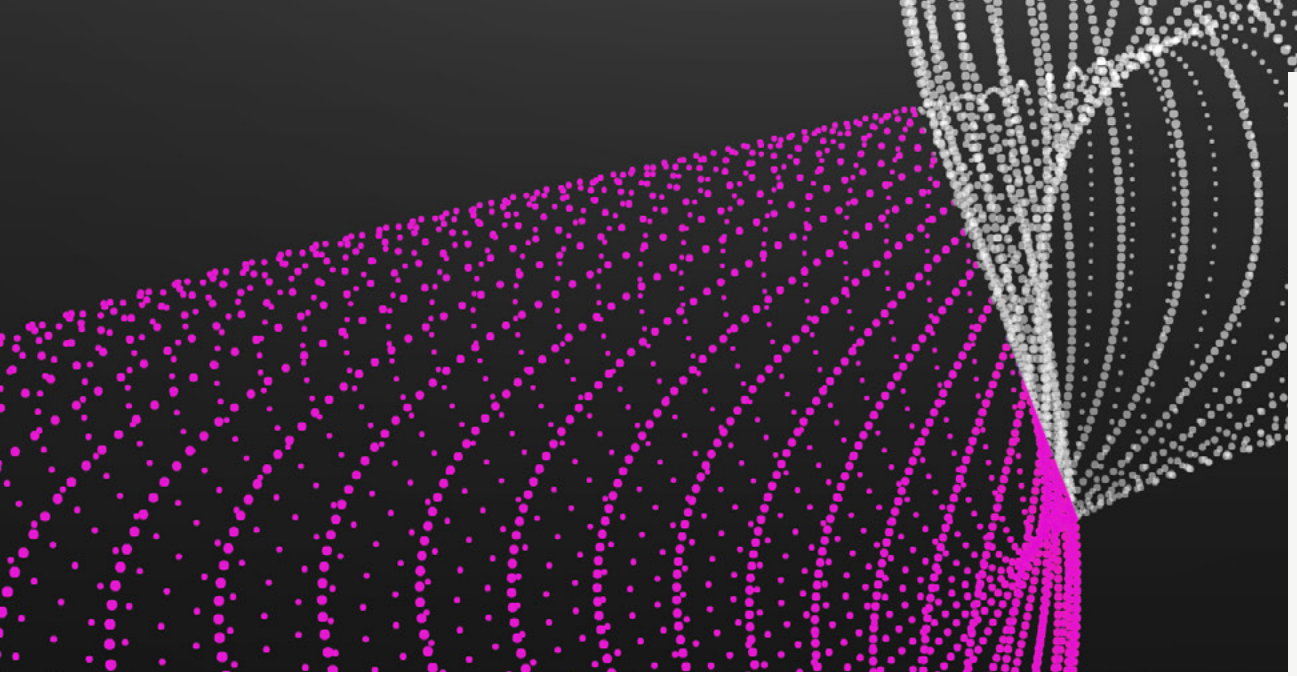
Protect on-premises and remote users

Gain insights for developing access policies

Streamline security management and operations

Reduce technical debt with SASE.

Enabling the convergence of network and security, SASE works to complement many solutions clients currently have in place, including SD-WAN. As a cloud-hosted solution, SASE also offers many organizations the opportunity to replace or consolidate redundant or legacy tools that contribute to operational inefficiencies and technical debt and hinder progress in transformation.



Understanding SD-WAN

Software-Defined Wide Area Networks (SD-WAN) are a cloud-based network technology designed to provide increased bandwidth at lower costs, enhanced security and other benefits. The shift to SD-WAN runs tandem with the widespread adoption of cloud and hybrid cloud models, representing a major shift in network strategy as a more effective way to securely connect all users and devices in a multicloud environment.

Many organizations are more familiar with SD-WAN than SASE and wonder how they differ architecturally. SD-WAN provides the greatest benefit when there are multiple links at single locations to prioritize, selecting the best path for specific business-critical applications. While SD-WAN enables optimal cloud connectivity through dynamic path selection and Direct Internal Access (DIA), modern SASE solutions are built cloud-focused and are able to provide the mechanism for secure connectivity for both remote users and branch locations to consume cloud applications as a service from the cloud.

While SASE can help consolidate some security tools, it is not a replacement for SD-WAN and other common security technologies and protocols; rather, it is an approach that unifies these existing technologies. As such, SASE will never remove the critical need for dynamic traffic steering or application-aware routing within the enterprise — primary reasons for SD-WAN implementation.

Explore SASE and SD-WAN solutions.

Learn how SASE and SD-WAN are making modern networks more flexible, resilient and secure in these resources covering everything from the basics to implementation, integration and management.

INFOGRAPHIC:
Streamline Network Security with SASE

BLOG:
Unlock Scalable and Flexible Connectivity With SD-WAN as a Service

WHITEPAPER:
Assess and Adopt Secure Access Service Edge (SASE) With Insight

LINKEDIN LIVE:
Understanding the Role of SASE vs. SD-WAN in Cloud Security

BLOG:
Understanding the Difference Between SASE and SD-WAN

WHITEPAPER:
Flexibility First — The SDDC and Modern Data Center Strategies

WHITEPAPER:
The Truth About SD-WAN and the Business Transformation Journey

VIDEO:
SD-WAN, SASE — What's What, and When

2. Modern wireless technologies

Organizations often find it necessary to quickly implement new solutions to address urgent challenges. But without optimizing architecture and deployment upfront to ensure maximum ROI long term, this introduces technical debt wherein an organization fails to realize the full benefit of a solution in its environment, resulting in loss of potential benefits.

Businesses with outdated network technologies are finding themselves unable to support the demands of hybrid work — which in turn impacts the customer experience and business viability. Rather than patching existing solutions, exploring refresh options that can better support your organization's applications may be a smarter next step; many organizations are finding wireless technologies like Wi-Fi 6 and Citizens Broadband Radio Service (CBRS) strong options for implementing secure, reliable, high-performance networks that enable productive work and positive user experiences.

Making it work from home (and anywhere).

Most of the technologies we have for working from home (video conferencing, for example) have been around for years. What's new, however, is the scale at which these applications are now used. If an entire organization's employees all returned to the office after a year of working from home, could the network continue to support all the high-bandwidth applications required of today's business environment? A wireless network architecture capable of supporting your business-critical applications not only promotes business continuity, but also drives a stronger ROI from your entire IT environment.

Wi-Fi 6

Wi-Fi 6 is the latest specification standard from the Wi-Fi Alliance — and a vital migration for enterprises that want to digitally transform their operations. Compared to earlier iterations of wireless networking technology, Wi-Fi 6 provides the capabilities needed to compete in today's business environment.

The new standard is designed to deliver quality connectivity in locations with hundreds or thousands of connected devices, as well as enterprise networks that use time-sensitive, high-bandwidth applications. Networks using this latest technology ensure that each connected device performs at an optimum level.

Because Wi-Fi 6 devices meet the highest standards for security and interoperability and allow lower battery consumption, the Wi-Fi Alliance says that Wi-Fi 6 can support virtually any type of environment, including IoT.

The benefits of the technology include:

Higher data rates

Increased capacity

Better performance in environments with many connected devices

Improved power efficiency

Want more on advanced Wi-Fi solutions?

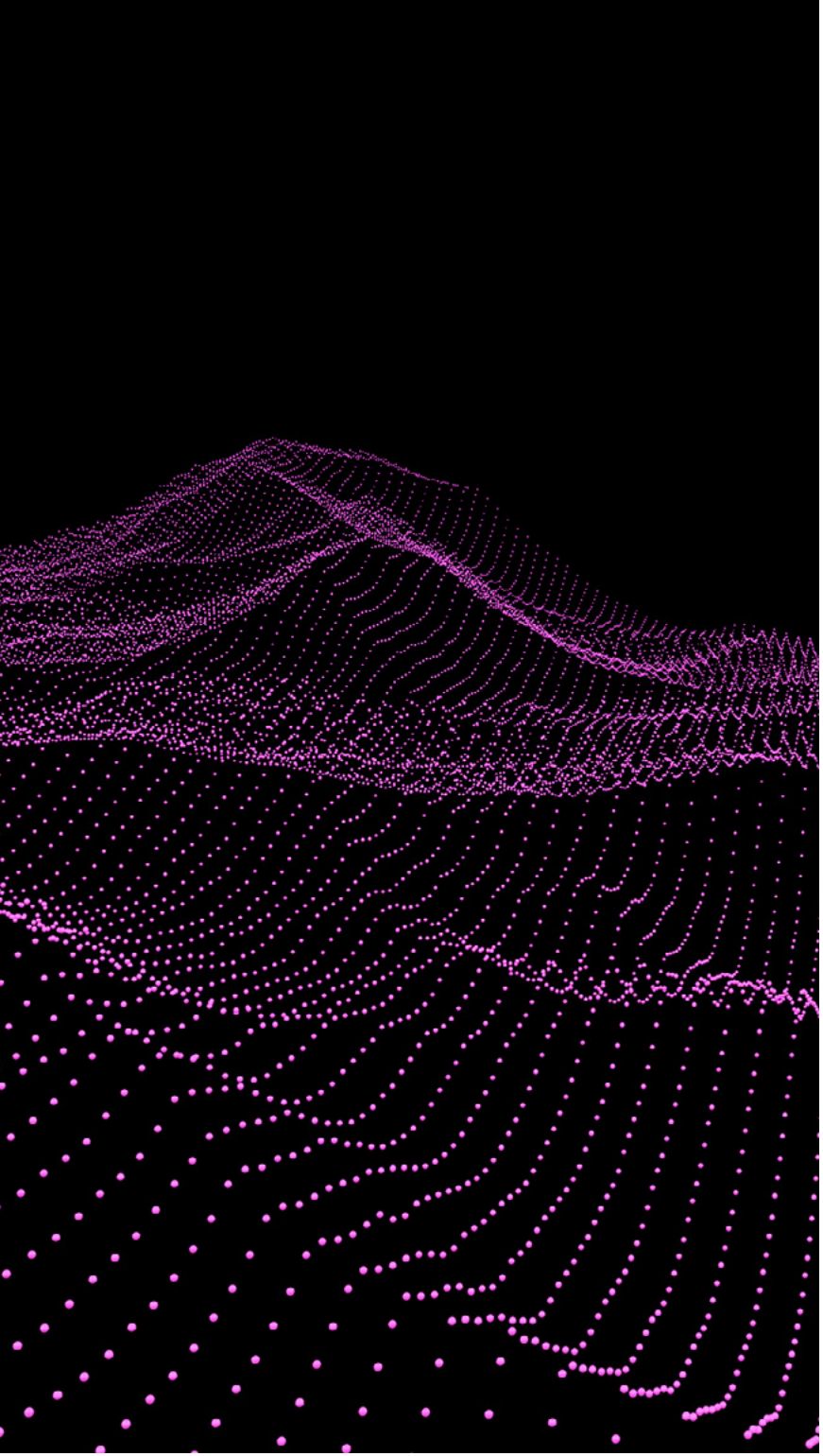
These resources explore the benefits of Wi-Fi 6, outcomes with AI-driven wireless technology and more.

INFOGRAPHIC:
5 Things You Need to Know Before Migrating to Wi-Fi 6

WHITEPAPER:
Migrating to Wi-Fi 6: An Enterprise Guideline

VIDEO:
New Frontiers in Wireless Connectivity

CLIENT STORY:
Multinational Grocery Chain Transitions to AI-Driven Wi-Fi



Citizens Broadband Radio Service (CBRS)

For industries that need to connect users and technologies across a significant geographical area where traditional wireless technologies would be cost-prohibitive or impractical due to physical barriers, Citizens Broadband Radio Service (CBRS) provides a cost-effective and reliable solution.

For large-scale applications, traditional Wi-Fi is often limited in coverage, capacity, speed and security. CBRS, also known as private LTE, runs in the 3.5 gigahertz space, an uncrowded cellular radio frequency spectrum. CBRS networks are deployed with dedicated equipment for increased data and device capacity and include built-in controls that deliver a level of practicality unavailable at scale through traditional Wi-Fi.

Scalability and strength — With a broad geographic reach, extensive network capacity and exceptional signal strength, CBRS is the perfect solution for reliable connectivity in both indoor and outdoor areas.

Security and manageability — Combining foundational network infrastructure with modern security solutions and wireless mesh technologies, CBRS delivers greater network security than traditional Wi-Fi with fewer nodes for coverage, making it not only more secure, but simpler to manage.

CBRS benefits and use cases

With signal strength capable of penetrating large structures, built-in security features, and a reduced infrastructure footprint, CBRS helps large-scale private sector organizations enable wireless access and IoT applications in challenging environments.

As a result, these organizations can maintain a high level of network service and embrace digital transformation while realizing reduced IT burden, improved operational efficiency and lower costs for connectivity.

Industries driving success with CBRS

Energy | Manufacturing | Shipping | Agriculture | Transportation

CBRS powers uninterrupted service.

An Insight client in the energy industry needed a wireless solution that would enable maintenance personnel to service sensitive equipment using secure, connected wireless devices to access proprietary maintenance procedure documents. Outfitting the plant with standard Wi-Fi solutions would have been extraordinarily cost-prohibitive, requiring extensive cabling to create a network architecture capable of providing uninterrupted service in such a challenging environment.

CBRS allowed the power company to install only a few nodes to create reliable connectivity throughout the plant, with little to no interference from the plant's many structures and built-in security to help keep the client's proprietary information safe.

See what's possible with wireless broadband services.

Discover how cities, communities, schools and more are creating connectivity with wireless broadband network solutions in these resources.

BLOG:
Creating More Community Bandwidth: Wi-Fi Access Points vs. Citizen Broadband Radio Services (CBRS)

WHITEPAPER:
Community Wireless Broadband: Bridging the Digital Divide

INFOGRAPHIC:
Creating Connectivity in Hidalgo County With a Wireless Mesh Network

INFOGRAPHIC:
How It Works: Community Wireless Broadband

CLIENT STORY:
Hidalgo County Brings Free Public Wi-Fi to More Than 30,000+ Rural Students and Workers

VIDEO:
Closing the Digital Divide With Public Wi-Fi

CLIENT STORY:
Free Public Wi-Fi for a Western U.S. City

3. Zero Trust

To ensure the highest level of network security, the trust you extend to connected users, devices and applications should be neither binary nor permanent. That's the foundational principle of the Zero Trust framework, an approach to methodically and comprehensively integrating identity-based access policies across entire operations based on their unique requirements.

Zero Trust methodology lays the groundwork for a highly defensible IT environment, considering all endpoints to be untrusted until proven otherwise — requiring identity verification, among other factors, to elevate trust and provide access to networks and resources accordingly.

A Zero Trust approach:

Establishes trust in every access request, regardless of where it comes from

Secures access across all applications and networks

Extends trust to support a modern enterprise across the distributed network

Zero Trust implementation is broken down into three main areas of application: the workforce, workloads and the workplace.

The workforce

Zero Trust principles applied to the workforce ensure that only verified users and secured devices can access enterprise applications by improving device visibility, assessing device security posture and enabling continuous risk assessment.

Workloads

Adopting Zero Trust to secure workloads means verifying trust for applications, services and microservices communicating with databases, containers and servers across your enterprise environment — whether on-premises, in the cloud or hybrid infrastructures.

The workplace

Specific access protocols must be in place to ensure secure access for any and all endpoints and IoT devices connecting to the enterprise network. Appropriate network security solutions enable users to securely connect to enterprise networks while restricting access from noncompliant devices.

Explore Zero Trust resources.

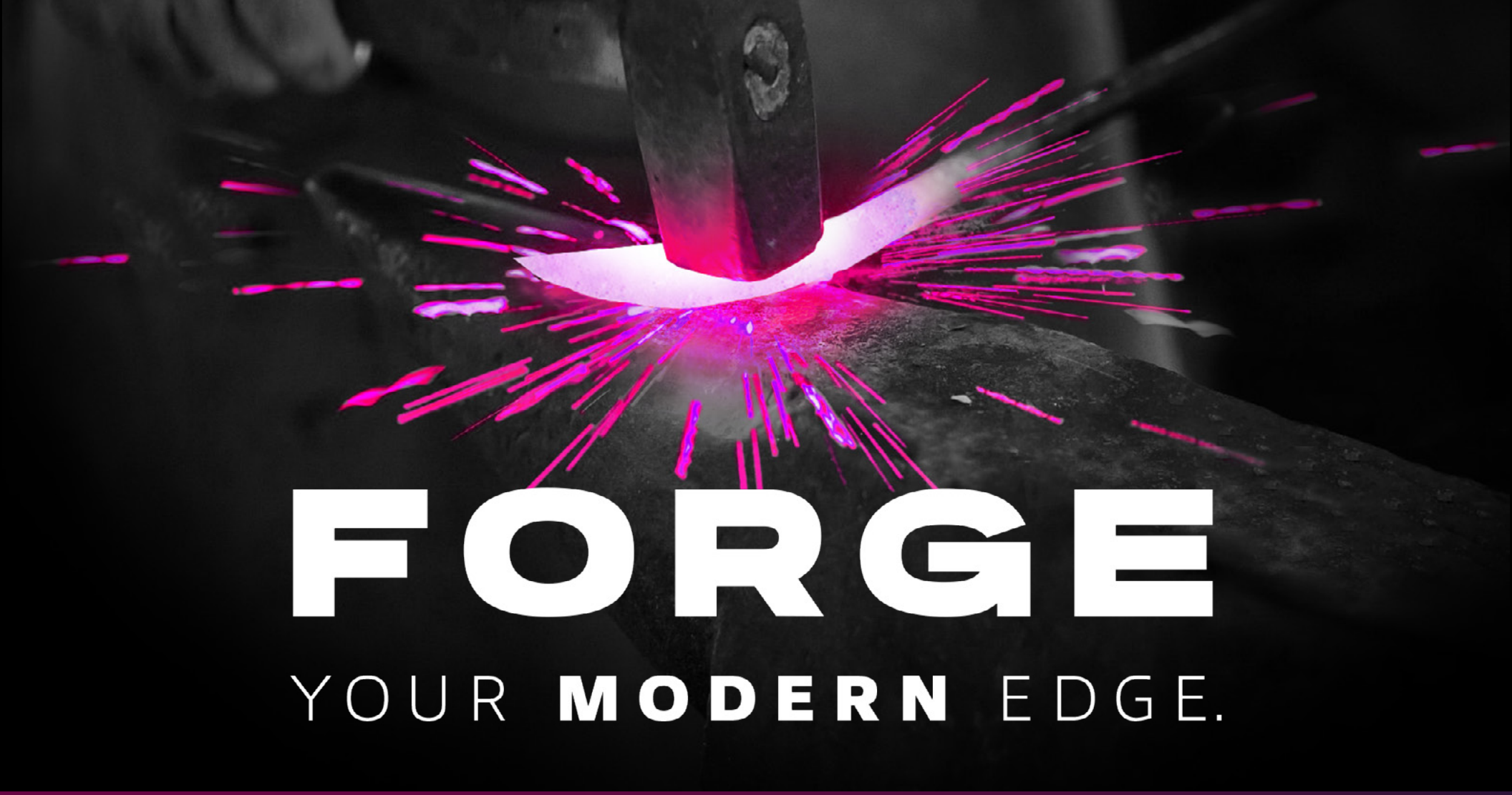
Browse these assets to learn more about what it takes to implement a Zero Trust approach, how to get started and how Insight can help.

WHITEPAPER:
Implementing a Zero Trust Security Framework

VIDEO:
Zero Trust: An Identity-Centric Approach to Securing the Enterprise

BLOG:
Zero Trust: What's Driving Its Adoption in Enterprise Environments?

VIDEO:
How to Get Started With Zero Trust



To move forward with modernizing your network edge requires understanding the answers to the following questions:

What's in your network infrastructure today?

Which users and applications are connected to your network infrastructure, and how?

What does your business need or expect from IT?

How can you transform your network edge to meet those needs?

Insight can help you start finding the answers to those questions and guide your adoption of new network and security solutions.

The distinctive benefit of Insight is that our teams have talent across the entire spectrum of networking and integrated security solutions, and we bring that experience into every client conversation.

We combine innovative services with strategic partner solutions to help clients navigate new complexities and increased demands on connectivity and security. By taking a services- and architecture-led approach, we drive business solutions that go beyond IT.

Client story: Creating a scalable, manageable and efficient global network

After years of mergers and acquisitions activity, a global construction and development firm was dealing with challenges resulting from a large, diverse and aging network spanning 500+ remote sites. More than two-thirds of its existing network infrastructure was end of life or end of support, creating risk and instability endangering business continuity and often requiring unplanned resource investments.

With a goal to globally standardize IT operations, repair all existing network architecture and leverage technology to improve delivery on key business objectives, the client reached out to Insight to establish and execute a plan.

Challenges:

- ✕ Disparate IT solutions
- ✕ 500+ locations
- ✕ End-of-life technology
- ✕ Costly maintenance

Outcomes:

- **Improved visibility** of network activity and performance
- **Better change management processes**, reducing outages and resource strain
- **Foundation laid** for transformation and innovation
- **Ensured network access** at 14 corporate and 50 building sites

Read the client story to see how we helped deliver a scalable, efficient and easy-to-manage network with dynamic routing and plans for continuing remediation and SD-WAN implementation.

The Path to Digital Transformation: Where Leaders Stand in 2023

We have the knowledge and expertise to guide your transformation through today's toughest challenges. Learn more about the top challenges IT leaders are facing in this ebook, which highlights key findings from our survey:

THE PATH TO DIGITAL TRANSFORMATION: WHERE LEADERS STAND IN 2023

The modern edge starts here.

The network is directly tied to business outcomes more than ever before. Secure your future; leverage Insight's expertise to implement flexible, cost-effective, high-performance modern edge technologies that serve your business and forge your competitive advantage. Go from strategy to reality with Insight — contact us to get started.

Insight

solutions.insight.com | insight.com

Sources:
[1] Marketpulse Research by Foundry Research Services. (January 2023). The Path to Digital Transformation: Where Leaders Stand in 2023. Slide 21. Commissioned by Insight.
[2] Marketpulse Research by Foundry Research Services. (January 2023). The Path to Digital Transformation: Where Leaders Stand in 2023. Slide 38. Commissioned by Insight.