EBOOK

Take Extreme's Zero Touch, Zero Trust Fabric to Branches at the Edge

Many organizations face challenges to scaling their networks rapidly and securely. Extreme Fabric to the Edge enables automated and secure solutions to undertake operational excellence and digital transformation initiatives with confidence.

Table of Contents

1 How Does a Fabric Help Organizations Now?

Many organizations are struggling to scale their networks securely

Organizations are struggling with risk and complexity

Complexity might take the form of an **increasingly distributed workforce,** an **unprecedented rate of change**, rapidly **rising network and security requirements,** and **the need to control costs,** or **all of the above, and all at the same time.** The right fabric can greatly **simplify operations and reduce risk** with a range of networking and security services.

However, most fabrics provide their capabilities locally, to a campus or a data center, rather than holistically across the network. This limits their scalability and utility. **Unlike campus-only fabrics, the Extreme Fabric** can extend services across data centers, campuses, and branches at the edge of the network in **a simple, secure, and efficient way.**

26%

struggle with **implementing security within the network**

25%

struggle with **provisioning network services**

24%

struggle with **providing network performance**

36%

struggle with **meeting budget constraints**

In research conducted by the Enterprise Strategy Group, IT leaders said they were struggling with cost control, security, provisioning, and network performance challenges.

2 What is Extreme's Approach to Fabric?

Automated, secure, and standards-based

The **inflexibility of legacy networks** and the **long wait times for manual network adds and changes** have made it challenging for IT teams to keep pace with **the current rate of business and technology change.** Extreme Networks helps organizations **simplify operations and reduce risk** with **and approach to Fabric** based on industry-standard IP and Ethernet technologies.

Unified

Flexible Fabric connects all places in the network and all technologies based on IEEE 802.1Q

Automated

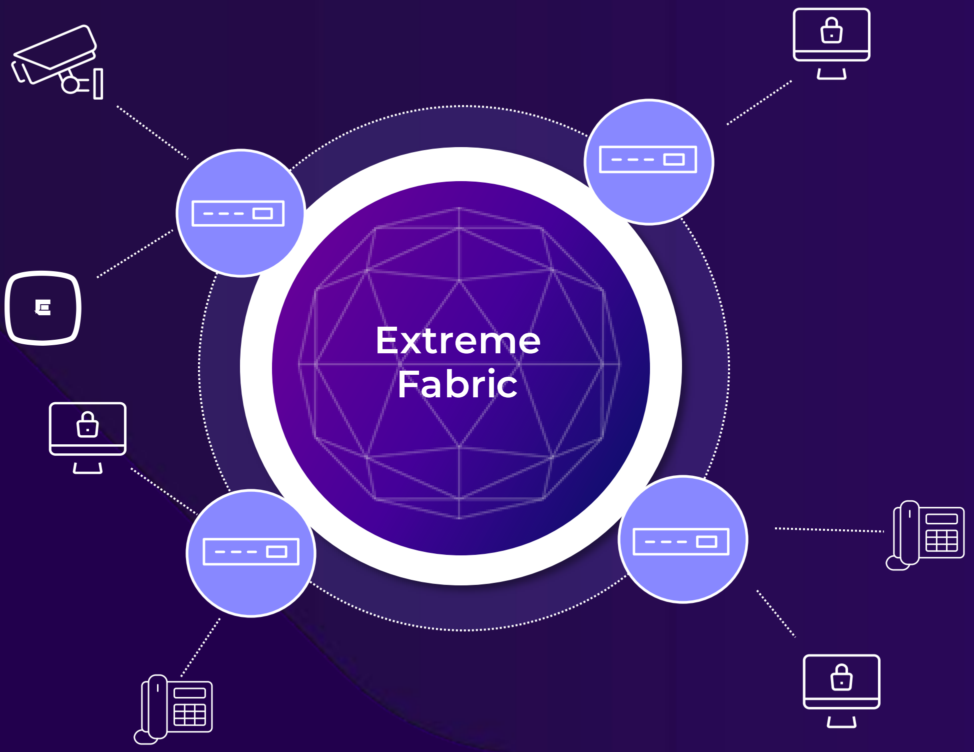
Fabric auto-provisioning of wired and wireless devices streamlines deployment and operations

Secure

Fabric reduces attack surface, minimizes risk from unsecured devices, and defends against lateral threat movement

Based on open industry standards, Extreme Fabric Connect reduces the cost, risk, and complexity of LAN networking and security

As organizations undertake network and business change, **manual per-device and per-site changes slow things down.** The automation and built-in security of Fabric Connect enable quick delivery of new sites and services in support of business goals.



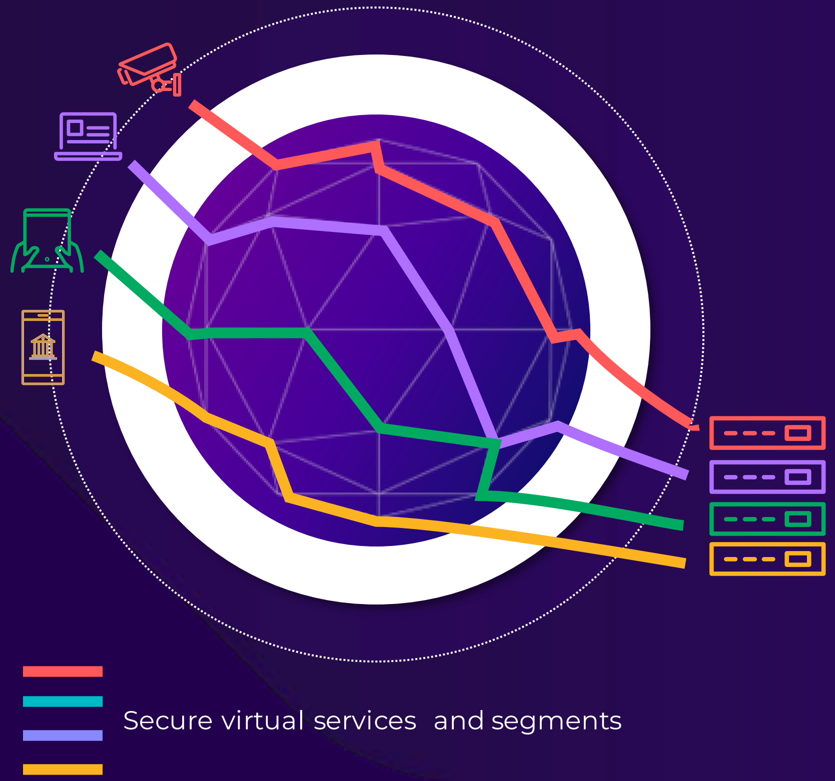
Fabric Connect has been deployed in thousands of customer networks and can extend services from the data centers all the way to branches at the network edge. Fabric enables **faster time to service** with simplified operations and automation; it also **reduces cybersecurity and compliance risk** with **hypersegmentation** and **stealthy design.**

Fabric is a self-forming and self-provisioning solution **based on open industry standards:** IEEE 802.1Q Shortest Path Bridging (SPB) and IS-IS as the Layer 2 and Layer 3 control plane. **Auto-sensing and onboarding** of Extreme switches and access points (APs) speed deployment. **Configuration and management** happen at the edges. Core and aggregation network nodes are built out once and then **changes are dynamically propagated** throughout the network.

Fabric also **improves network performance and resilience. Both north-south and east-west** traffic optimization reduces latency. A typically 200-millisecond failover **improves network resilience** and **enables network scaling** to tens of thousands of video streams with predictable performance

Fabric Connect helps secure the network

Cybersecurity risks are increasing as attackers become more agile and more aggressive. **Attacks can be catastrophic.** Fabric Connect helps network and security operations teams **reduce the risk and damage of attacks by reducing the attack surface and the ability of threats to move across an unsegmented network behind the security perimeter.**



Secure virtual services and segments

Fabric reduces the risk and impact of breaches with hypersegmentation, stealthy design, and elasticity. **Unlike perimeter-focused approaches** to security, in which the network behind the perimeter is flat and open, **built-in hypersegmentation** enables convergence of multiple, physically separate networks into one.

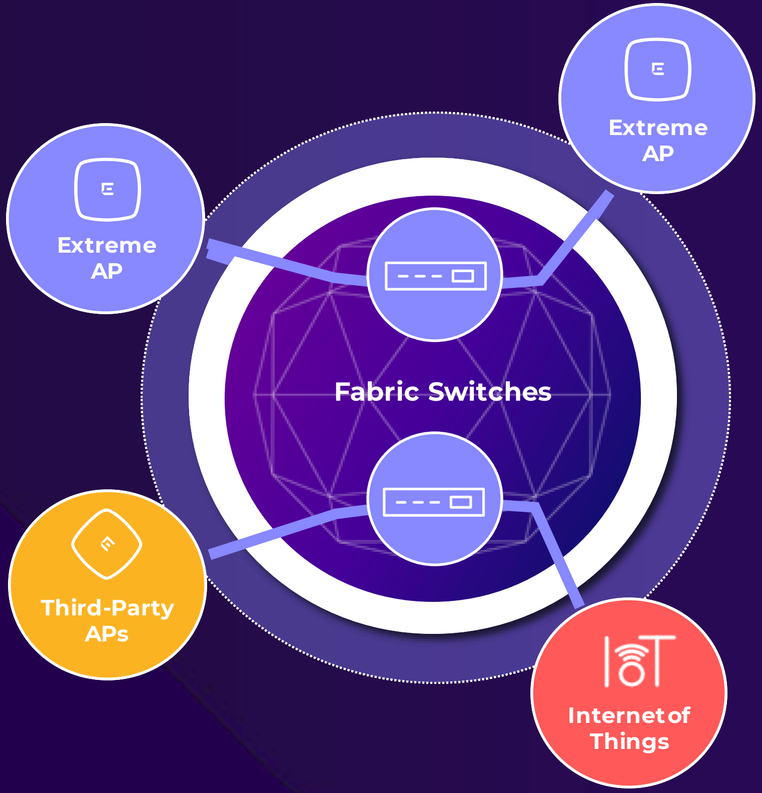
Each segment then functions as its own logical network. Users and applications are dynamically mapped to segments, while network policies are dynamically mapped to users. This enables a **zero trust approach** in which **the right users have access to the right resources. Fabric enables rapid isolation of breaches when they do occur, and limits the impact of an attack**, Fabric-enabled fast failover enables organizations to recover more quickly. **Optional MACsec encryption** at the Ethernet link layer can also protect traffic.

Stealthy design means attackers cannot attack what they cannot see. In the core, Ethernet switch paths keep IP addresses invisible to IP scanning attacks. The Fabric, virtual services, and segments appear dark when scanned.

Elasticity reduces potential network entry points. When no longer in use, the configuration of network services extended to remote branch devices are automatically deleted.

Extreme Fabric Attach makes it simple to connect Extreme Wi-Fi Access Points, non-Extreme devices, and roaming wireless users

Wireless connectivity is the cornerstone of many modern networks, enabling a wide variety of **business processes,** from inventory control to hot-desking.



Fabric Attach extends the value of Fabric Connect to **Extreme wireless access points, non-Extreme devices, and roaming wireless users.** This increases network agility and better enables network architecture to **scale business transformation initiatives sustainably.**

Fabric Attach enables organizations to seamlessly extend policy and Fabric services to access points, devices, and users. This provides IT teams with **greater control while reducing complexity.**

When plugged into the Fabric network, Extreme **Wi-Fi access points connect to and extend Fabric services automatically.** Negotiation of Fabric Attach client VLAN assignments to Fabric-enabled switch ports is automatic.

Provisioning a non-Extreme or non-Fabric-enabled device to Fabric Connect is as simple as physically connecting it to a Fabric switch.

Fabric Attach also delivers services to roaming wireless users, regardless of their location. Dynamic auto-attach and segmentation of connected things, users, and devices further simplifies secure connectivity.

3 Why Extend Fabric to Branches?

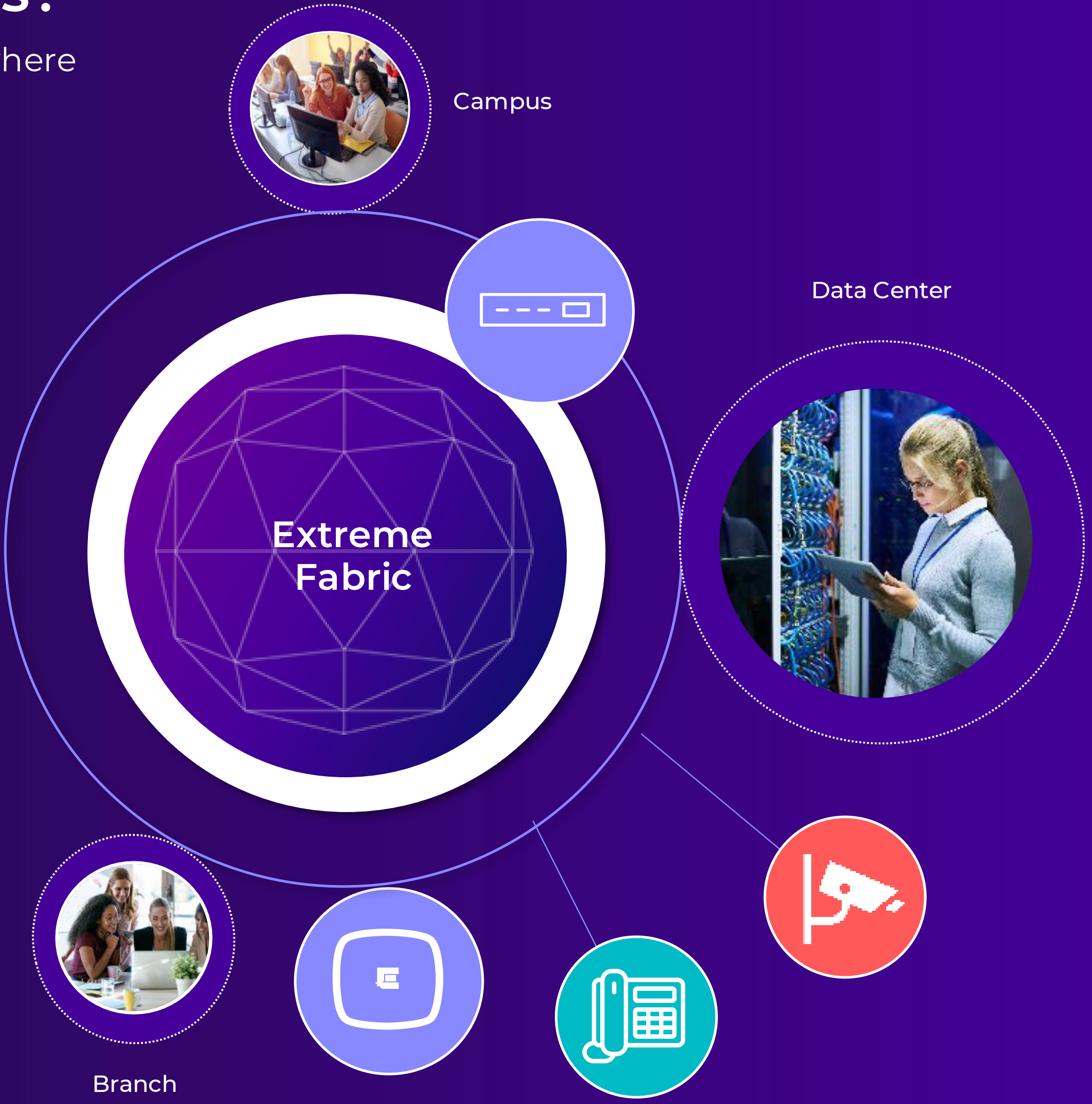
Fabric can reduce risk and simplify operations everywhere

Extend all the cost and operational benefits of Extreme Fabric Connect to branch locations over low-cost internet access transport

Unified: Extend Fabric services over even the largest of networks and enable centralized configuration of Ethernet switches, wireless access points, SD-WAN appliances, and more.

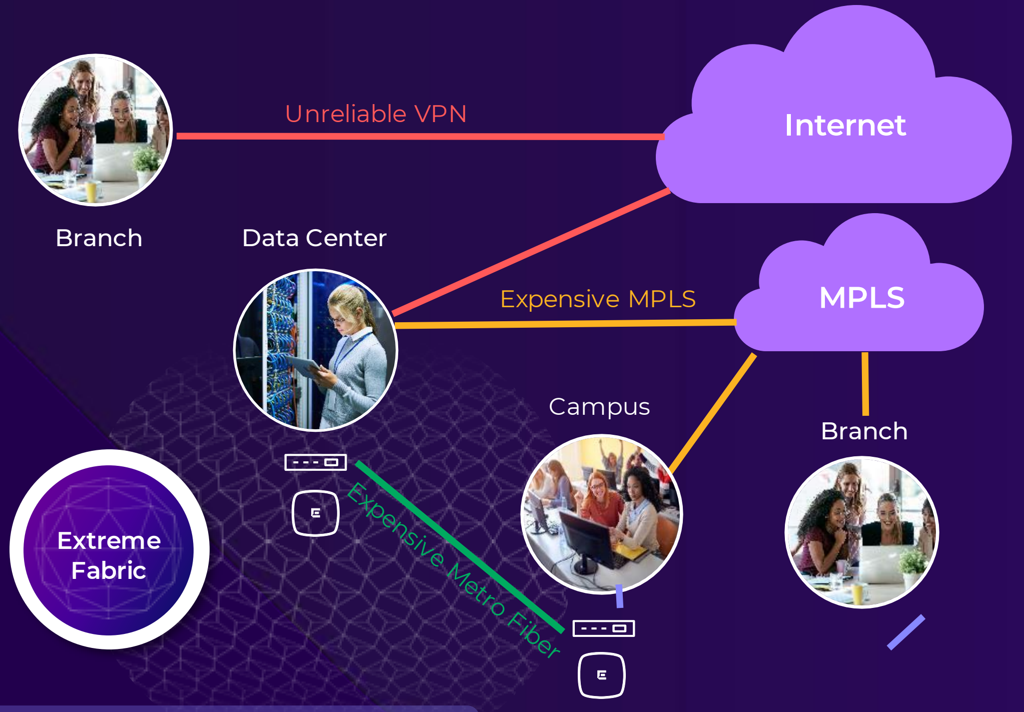
Automated: Orchestrate wired, wireless, and SD-WAN from the cloud, enabling automated delivery of the best application performance for the lowest cost, even for remote branch users.

Secure: Fabric hypersegmentation provides secure connectivity and simplifies compliance at branches. It also reduces the risk of lateral threat movement as employees return to branch and campus networks with potentially infected laptops and other devices used in insecure home networks.



Branch connectivity for many organizations is more complex and expensive than it should be

Networks are often built up over time, with a mix of technologies and approaches to connectivity. Eventually, this makes network adds and changes at local branches costly and time consuming. Fabric Extend over ExtremeCloud SD-WAN reduces that cost and complexity at the branch by extending fabric over low-cost, flexible internet access transport.



▭ Universal Switches ⓔ Universal APs

By default, Fabric Connect works centrally in a network's data centers and campuses. Fabric over SD-WAN extends the security, scalability, and automation of Fabric Connect to the entire network. **Extending zero touch provisioning and secure connectivity** to branches and other remote locations offers extraordinary value to distributed organizations.

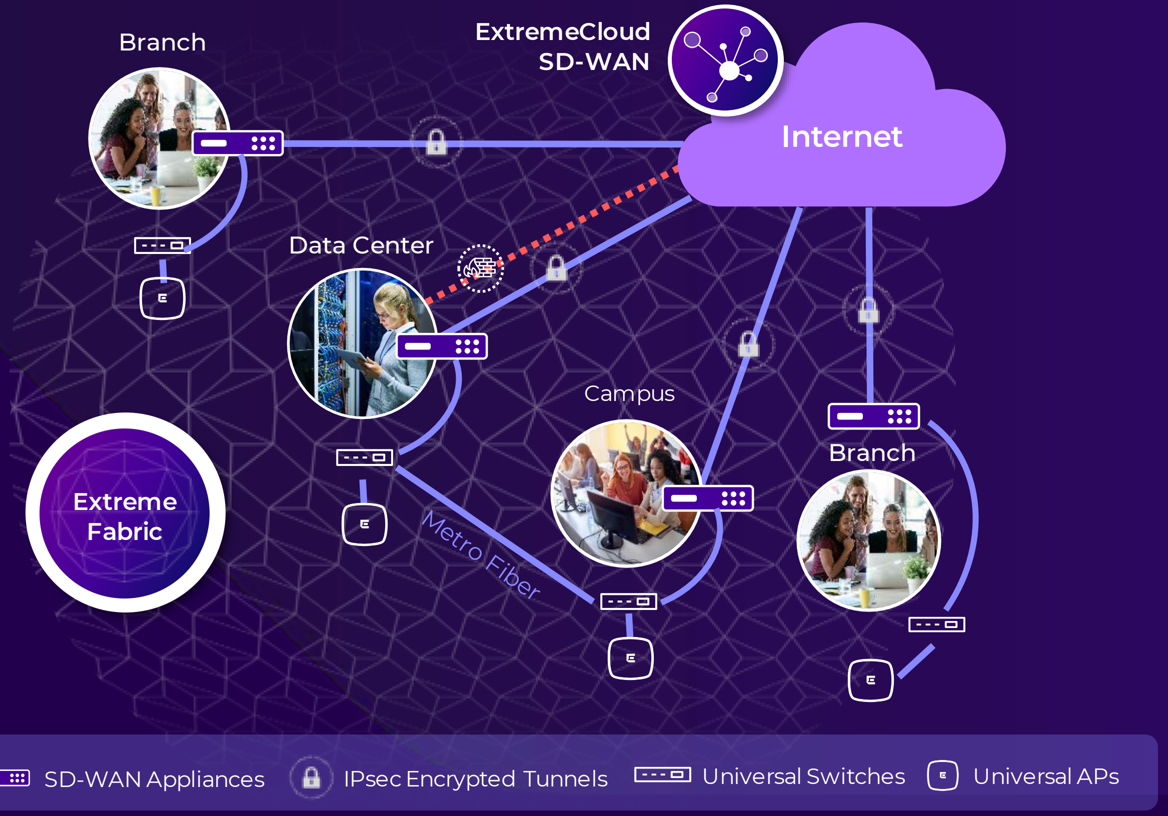
ExtremeCloud SD-WAN provides a secure, cost-effective, and low-risk means to connect sites and extend Fabric services globally, from the smallest branches to the largest data centers, over low-cost internet access transport.

Fabric Extend facilitates **auto-discovery and configuration of fabric-enabled switches and access points** across SD-WAN connected sites, enabling a zero touch provisioned, centrally managed fabric across the entire network. **This also extends Fabric Connect's enhanced security capabilities to remote locations,** enabling consistent policy across the entire network.

Fabric Extend works over both the public internet and private WAN services. For example, an organization might choose to use both metro fiber and SD-WAN in combination to extend Fabric.

Fabric to the Edge via SD-WAN provides organizations with cost-effective, granular control over their networks

Fewer and fewer applications run in the data center, and the public internet connectivity now provides more than good enough connectivity for most applications.



The core of Extreme's 1 Network, 1 Cloud vision is **a single control plane** featuring unified, cloud-native management of a **Fabric-enabled data plane** that enables security and automation across **wired, wireless, SD-WAN, and other devices.**

For organizations that want a cost-effective, agile, and flexile means to extend Fabric, SD-WAN is the optimal choice for connectivity.

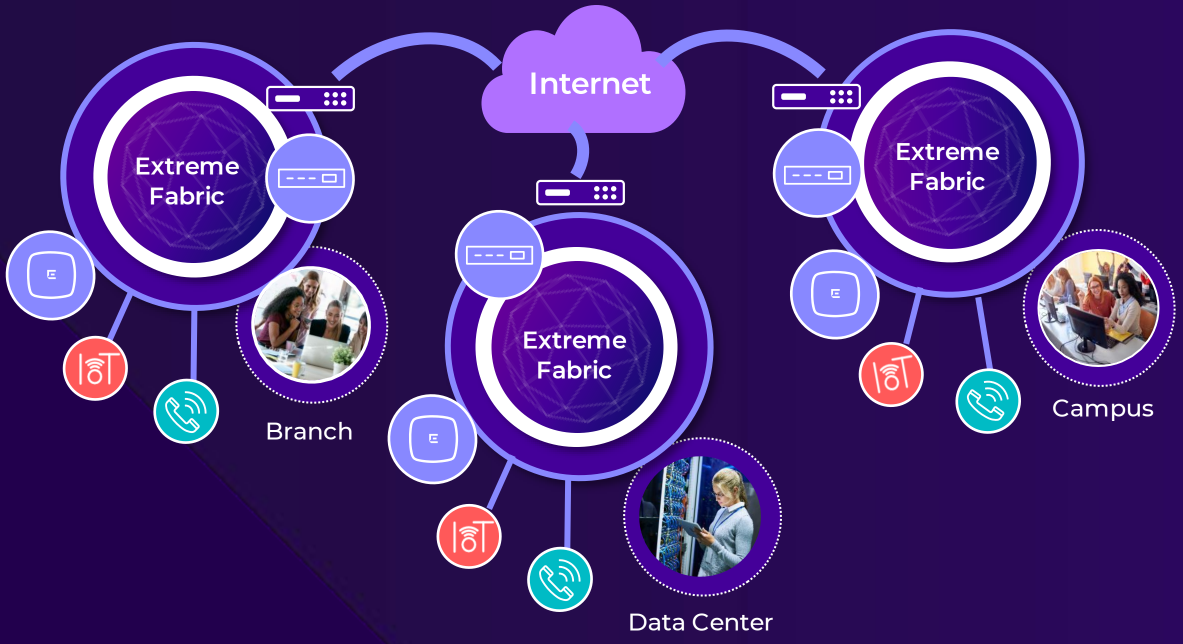
In this model, Fabric and SD-WAN connect LANs across multiple locations together into a single topology. SD-WAN provides the underlay.

Internet-bound traffic is backhauled through to a central hub for egress. Fabric switches in the campus or data center can be connected to an enterprise firewall for policy-based internet access.

A centralized approach to internet access enables employees to use the SaaS and IaaS applications they need to do their best work. This also enables **consistent policy and enforcement, better cost control, and simpler compliance.**

Control WAN cost, improve operational efficiency, and reduce unplanned downtime with Extreme Fabric over ExtremeCloud SD-WAN

Fabric to the Edge via SD-WAN provides organizations with granular control over their network in ways that enable operational **efficiency and productivity as well as services availability and resilience.**



▬ Fabric traffic over SD-WAN via IPsec encrypted tunnels

To achieve business goals, organizations need to improve productivity and efficiency while controlling costs. No organization wants unplanned downtime.

Control cost and reduce risk: ExtremeCloud SD-WAN enables centralized configuration and management, zero touch provisioning, reduction of MPLS, Metro Fiber, or other, more expensive WAN technologies, right-sizing site bandwidth, and other cost controls.

Improve IT efficiency: ExtremeCloud SD-WAN enables **improved branch security, visibility, and performance.** When paired with ExtremeCloud IQ, centralized configuration and management for Wi-Fi access points, Ethernet switches, and SD-WAN devices reduce complexity. Cloud-native SD-WAN orchestration enables consistent policy and intelligent automation.

Reduce downtime: Automatic traffic steering across multiple IP access links improves uptime. IPsec encrypted tunnels reduce the risk of internal threats. Fabric and an additional SD-WAN appliance extends Fabric's subsecond failover time to SD-WAN connectivity at data centers, campuses, and branches.

ExtremeCloud SD-WAN's advanced application performance management enables the best application performance for the lowest cost

E Applications provide the glue between people, processes, and data. ExtremeCloud SD-WAN provides the **granular application visibility, control, and reporting that organizations need.**

Application performance is critical to productivity, but **not all applications require the same QoS.** Identifying and classifying applications according to their business critical is an important part of ensuring consistent, exceptional performance. SD-WAN solutions must enable consistent, high-quality user experiences that improve productivity in ways that align with business goals.

Granular performance visibility into over 5,000 application services on a site-by-site basis enables quick understanding of user experience and evidence-based decisions about network refinement.

Intelligent application performance control analyzes and optimizes network traffic, bandwidth availability, and application demand across the WAN, **reallocating bandwidth as needed** to meet performance goals. Built-in advanced **WAN optimization** accelerates large data flows via TCP/IP optimization and deduplication of traffic.

When paired, ExtremeCloud SD-WAN and ExtremeCloud IQ provide deep application performance visibility across the entire network, as well as visibility into network performance across devices, sites, links, and users. This enables **faster root causes analysis and reduces MTTR.**

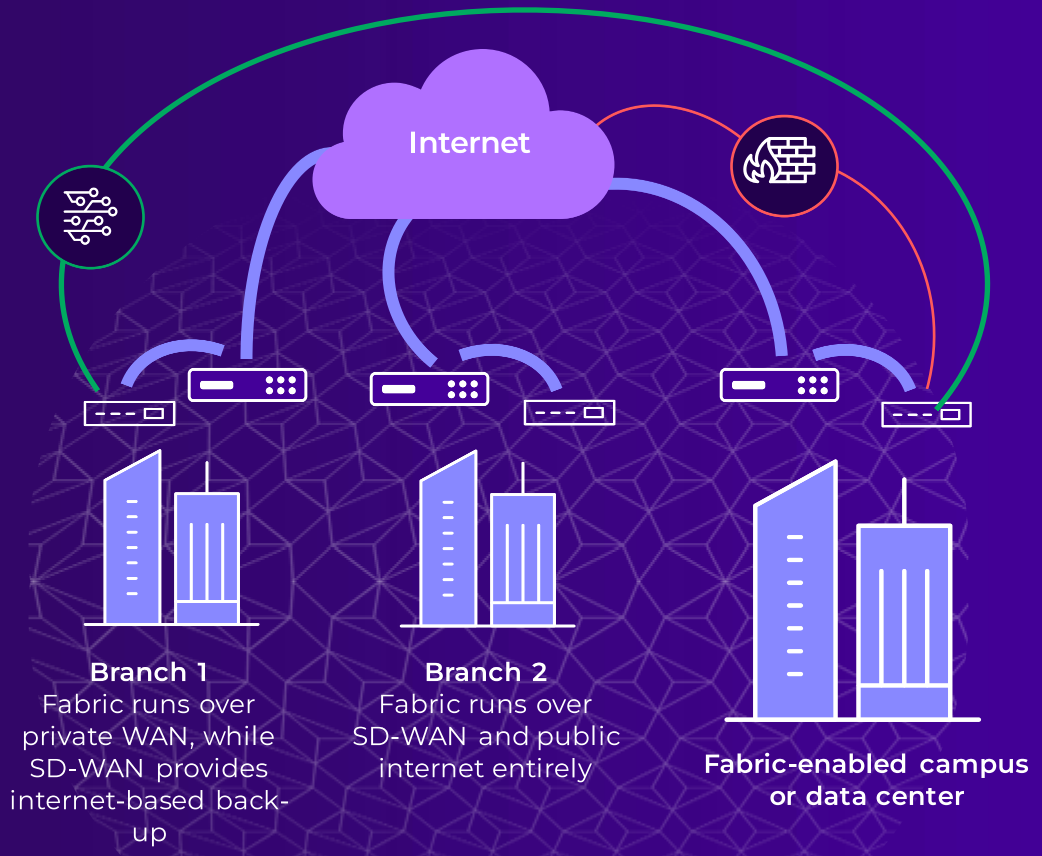
4 How Does Fabric over SD-WAN Work?

Fabric over ExtremeCloud SD-WAN provides a flexible, cost-effective solution

The Fabric traffic is routed much like other packets

ExtremeCloud SD-WAN receives traffic from a Fabric switch. The SD-WAN appliance routes Fabric traffic to its destination, applying its advanced application performance management. Dynamic WAN selection as well as application and session-specific performance control ensure QoE. SD-WAN and Fabric peering is also visible in the SD-WAN orchestrator.

IPsec encrypted tunnels transport traffic securely over the internet. To support links with a small maximum transmission unit, larger TCP and UDP packets are fragmented when needed (via MSS clamping and IP payload fragmentation, respectively). When packets arrive at the remote site, the SD-WAN appliance inspects the packet headers and hand-off traffic to a Fabric switch. A central firewall can route authorized egress traffic, enabling consistent policy and reducing the need for and cost of branch firewalls.



Internet

Branch 1
Fabric runs over private WAN, while SD-WAN provides internet-based back-up

Branch 2
Fabric runs over SD-WAN and public internet entirely

Fabric-enabled campus or data center

▬ Fabric over SD-WAN via IPsec encrypted tunnels
▬ Fabric over Metro Fiber via VXLAN
▬ Internet access via firewall
▭ SD-WAN Appliance
▭ Fabric Switch

ADVANCE WITH US™