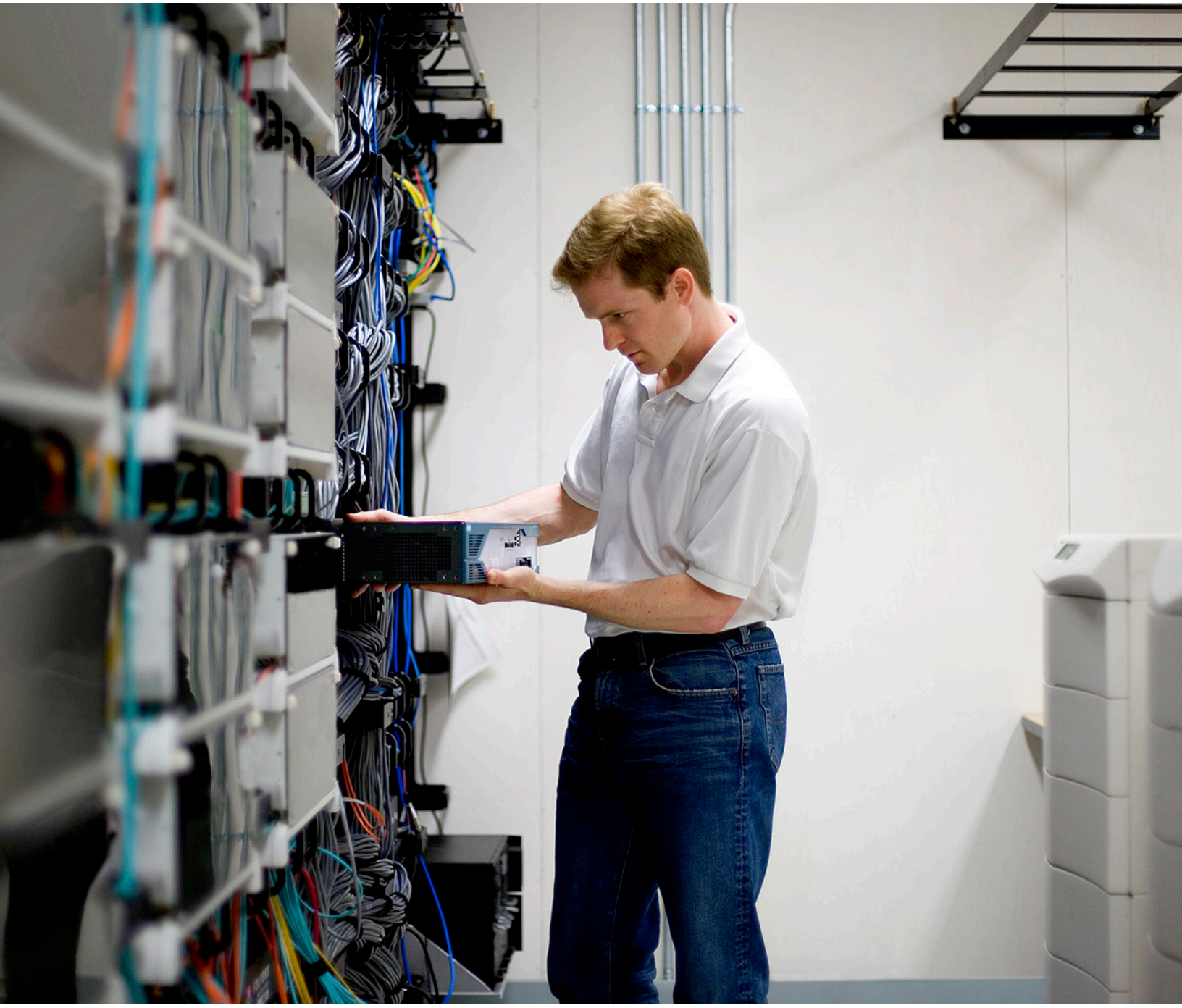
Make Your Network Edge Intelligent and Meet Tomorrow's Needs Today



Executive Summary

In the new digital business reality, the network edge has never been more important. Often overlooked, the network edge is the cornerstone in which digital success is either realized or lost. Consider everything that occurs at the network edge:

- It's the first line of defense against untrusted or malicious devices infiltration.
- It's the conduit that delivers—often highly invested—applications and services to target audiences.
- It's the strategic gateway to connect widely distributed organizations.
- It's the bridge between your organization and your customers.
- It's the spot where new Internet of Things (IoT) devices are connected and managed.
- It's the optimal place to really understand what's happening with your business.

The network edge is sometimes deployed with the belief that all network solutions are essentially the same. Cisco disagrees and surmises that the new digital business requires vast intelligence at the edge.

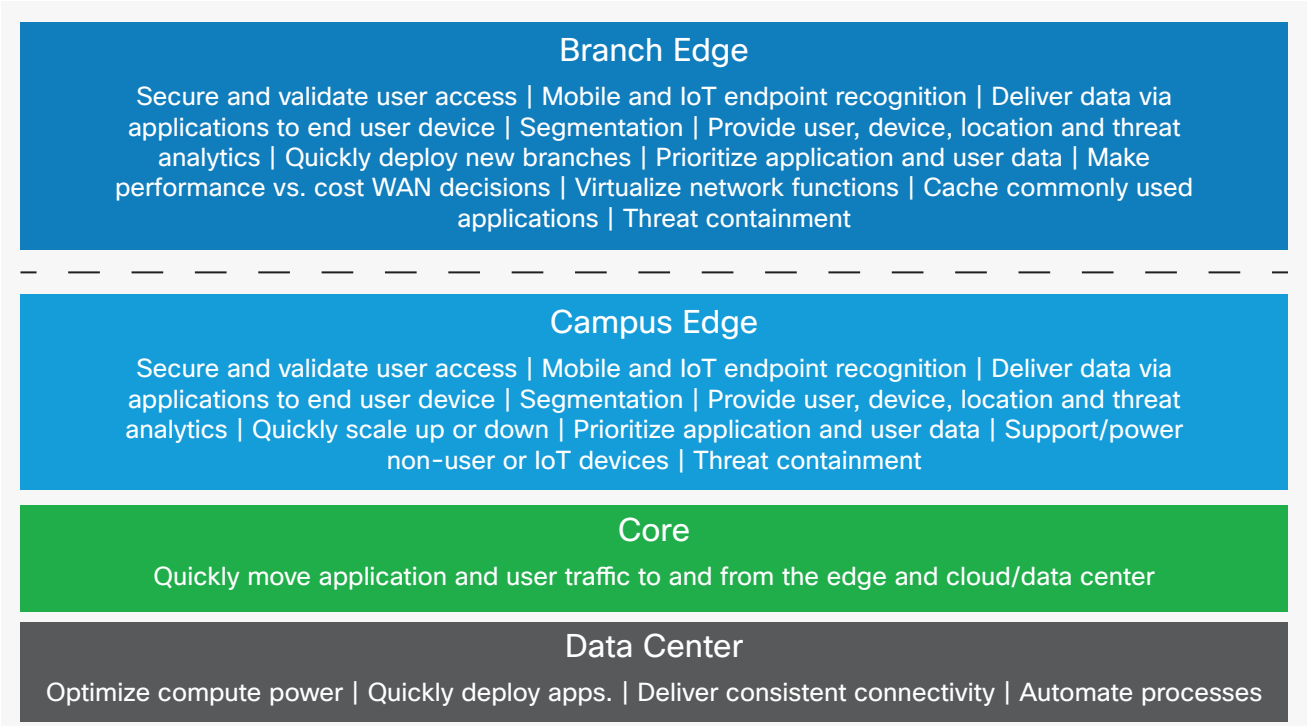
We deliver solutions and strategic functionality to drive business success. Cisco drives the new digital network edge with a focus on:

- Defending critical assets at the edge. Organizations can avert 99.2% of network breaches by leveraging the network as both a sensor and enforcer. This can be down while also delivering deeper insights to improve protection and faster response.
- Enabling application and device awareness with eight times faster roaming and visibility with more than 1200 applications. This is made possible through a strategic partnership with Apple and with Wi-Fi innovations.
- Quickly adapting the network as your business evolves with a software-defined approach in wireless LAN, LAN, and WAN. This results in a 79% reduction in deployment costs by decoupling software from hardware and virtualizing the WAN edge.
- A platform designed to meet future demands by establishing a standards-based, programmable foundation that can quickly add new functionality when it is needed.
- Delivering deeper and faster insights from retail and hospitality, gaining up to one meter in location data granularity to make better business decisions.

Today the network is critical in driving change in virtually all organizations as they take their digital transformation journey. This transformation journey will help organizations increase agility, improve productivity, better engage with customers, and protect key intellectual property and assets.

The network edge has a pivotal role to play in this transformation and carries perhaps the broadest set of responsibilities when compared to the core and to data center networks. As shown in Figure 1, when comparing each layer of the network, the network edge has a broad breadth of responsibility in the campus. This is also true for the branch.

Figure 1. Network Layers and Their Functions



The Role of the Network Edge

Digital transformation makes the network edge more important than ever before. Consider everything that happens at the edge of the network:

- **It's the first line of defense.** The edge is where policy is applied and validated, without limiting your ability to access the things you need. If access is not properly managed, then your business can be susceptible to infiltration or threat proliferation, and the criticality grows as the threat landscape grows. The device, firmware, and even the operating system are all points of compromise.
- **It's the conduit that delivers heavily invested applications.** The network edge is where prioritization occurs. A poor experience at the edge will slow application adoption, reducing return on investment.
- **It's a strategic gateway to the widely distributed organizations to connect.** Providing a seamless experience to your employees, partners, and customers—wherever they happen to be—is most important. A second-class network will deliver deviating levels of services to key audiences.
- **It is the bridge between the organization and their customers.** If you're a part of a retail or hospitality business, sub-par access will stunt your ability to connect with customers on a personal level and negatively impact your brand.
- **It is built to power and support growing IoT device demands.** The network edge adapts the physical environment by moving virtually all industries into the digital age by improving operations and lowering costs. Without the right functionality at the edge, organizations can be left behind in terms of cost reduction and operational efficiencies.
- **It is the optimal place to understand what is happening with the business.** In a distributed network, only the edge sees all the data traffic, by harvesting data and analytics from the edge. Data about users, applications, devices, and threats businesses can derive insights that truly help in making better decisions to support employees, reduces risk and cost, and deliver information to the targeted audience. Without the right level of consistent granularity, this data becomes skewed and untrusted.

Is Commoditization of the Edge a Good Thing?

Many edge solutions approach commoditization by relying on readily available components to build edge network devices and design directly to the industry standards. This is often done to reduce engineering and production costs of the equipment by leveraging readily available designs provided by the component manufacturers. This leads to the commoditization of the edge. The approach of putting cost and management ahead of delivering key innovations in growth and security opens your business to greater risk.

What Is the Risk?

Components and designs are not only available to the device manufacturers; they can find their way into the hands of people who are looking to infiltrate the network. Every device that attaches to the network is a point in which the network can be infiltrated. Today's organizations rely increasing numbers of mobile and Internet of Things (IoT) devices on their network to achieve business success. Organizations need to look at solutions that address securing access, starting at the edge and continuing to check and recheck traffic at every hop, from the edge to the data center.

There is also the risk of having to re-engineer the network if a new business requirement presents itself. Off-the-shelf solutions are designed to meet a large number of current use cases, but are limited in terms of flexibility and customization. They are also limited in terms of being ready for the unforeseen evolution of your network. The network platform needs to adapt to today's fast-moving digital world.

Most off-the-shelf solutions are built to align directly to industry standards, which are important to deliver a core set of requirements and functionality. However, the standards can change. The standards process is often a lengthy one and the rate in which device manufacturers, application developers, and user demands are constantly shifting. Those that use a standards-based approach could find themselves left behind when it comes to meeting higher user expectations. There are times when a solution can start by meeting the standard, but then have the capability to develop additional functionality on top of those standards when needed. These meet the new demands of the digital world without being bound by standards, which could take years to improve upon and ratify.

There is also a risk of the device integrity being compromised. Malicious organizations intercept devices when shipped globally, then alter the components, such as swapping out processors or integrating monitors to acquire sensitive data.

What Is the Real Cost?

Often the commoditization of the edge is done to reduce engineering and production cost, and allows some solutions to be sold at a lower price point. However, when measuring cost we should not look at pure capital or even operational cost, but also at the cost associated with risk. Each organization is different, so determining actual costs that would represent everyone is not possible. But consider:

- The cost of a security breach. Many organizations' intellectual property and assets are the livelihood of the organization. If they fall into the wrong hands what are the ramifications? Malicious organizations are incredibly good at monetizing intellectual property through ransoming, extortion, and resale to the highest bidder. Some studies reveal that medical records have been ransomed for $40.00 per record. With thousands of records, hospitals can potentially be on the hook for a lot of money to get their property back.
- The cost of a business-critical application not being adopted by employees. Many organizations invest a large part of their budget on new applications and systems to improve productivity. If employees have poor experiences with these applications or services, then they will abandon them and the return on the investment will plummet.
- The cost of lost opportunity. If you're a part of a retail or hospitality organization, then you are engaging customers through their mobile devices. But if your customers have difficulty connecting, then your organization has lost the opportunity to engage with that customer and influence desired behavior.
- The cost of lack of visibility. The edge network holds a wealth of information regarding users, their devices, what applications they use, where they go, and even information about where potential threats exist. Without this visibility your organization may spend countless hours trying to understand how users interact with the environment, how they access and consume information, and even miss a potential threat that could have been mitigated early.

Cisco Delivers Intelligence at the Edge

Cisco takes a different approach than commoditizing the edge. We are heavily invested in developing innovations that are positioned to help move organizations into the digital age. We are laser-focused on defending critical assets, to support a higher level of application and device awareness and to deliver deeper and faster insights. Cisco helps you adapt as your business evolves and prepare for whatever the future holds. We do this by building unique functionality from the ground up or improving the functionality of battle-tested components. Cisco provides the functionality to help you meet the demands of the network edge both today and in the future.

Defending Critical Assets at the Edge

The network edge is the number one point for unauthorized or hostile access because it's where users and devices are on-boarded. It has to be trusted to identify and control what's getting on the network.

To accept that commoditizing edge security will be effective suggests that off-the-shelf security is working. If that's true why are information theft, extortion, and ransoming quickly growing into a $1 trillion industry?

Current edge security approaches are not working. Cisco is the market leader with innovative technologies to know what and who something is, as well as its health before letting it on the network and allowing it to roam.

Here are a number of Cisco® network edge security innovations for Cisco customers and how it's being used:

- **Device and user identity and health**. Cisco edge devices integrate the most extensive endpoint profile probe technologies. Additionally, the Cisco AnyConnect® Security Agent conducts a posture and policy compliance health check before production network access is allowed. The most accurate endpoint identity keeps unauthorized, unhealthy (malware infected) devices completely off the network until proven clean and authorized.
- **Access privileges that change by threat score**. With integration with Cisco Identity Services Engine, users and devices can have their access privileges changed automatically as their STIX threat or CVSS vulnerability score changes. STIX and CVSS are commonly used expressions to describe the severity of security threats and vulnerabilities.
- **Software-defined segmentation integration**. Creating and managing segmentation with virtual LANs and access control lists (ACLs) are typically difficult and prove to be more difficult as segmentation becomes a key to secure IoT operations. Cisco edge devices ship with embedded Cisco TrustSec® software-defined segmentation in the operation system as well as an ASIC to ensure easy, high-performance identity and segmentation from point to access to an application in the data center.
- **Network as an Enforcer**. This is software-defined segmentation embedded in the edge devices that allow instantaneous and consistent enforcement of security policy to control access and contain threats. Working through integration with Identity Services Engine, Cisco Stealthwatch, and Cisco Security Technology Associate technologies can invoke policy to contain a threat, all from one pane of glass – or one product.
- **Network as a Sensor**. Get advanced end-to-end visibility with NetFlow and interpretation by Cisco Stealthwatch.
  Since all Cisco edge devices include Flexible NetFlow you can have end-to-end flow visibility to discover anomalous behaviors. With commodity technologies you are blinded to behaviors that show you what users do when they come onto the network and what they are doing on the Internet.
- **Stealthwatch Learning Network integration**. This innovation can enable all branch devices to share behavioral data and get smarter on what is permissible which makes it faster, easier, and more scalable.
- **Zero-minute defcon policy enforcement**. This means you can have preset policies to respond to catastrophic events, such as a day-zero malware or hacking event that spreads quickly. With one push of a button you can invoke access policy changes for every device on the network to restrict or stop all communications until the threat can be reconciled.

- **IoT endpoint identity and automatic segmentation**. The probes in Cisco edge devices help identify the largest collection of medical IoT devices today and the technology is expanding into many other industries. Through integration with advanced technologies such as Identity Services Engine, the edge network devices will be able to better identify and automatically segment the most obscure endpoints and automatically add them in discrete network segments to protect them from attack. So when a worker puts a device on the network, it is identified, classified, and dropped into its respective and security network segment.
- **Rapid threat containment**. Cisco edge devices integrate with Identity Services Engine and TrustSec so when a Cisco or technology integration partner detects an attack they can put the threatening endpoint in a network segment, either by an IT command or automatically. Threats are detected faster and containment response is instantaneous.
- **Malware detection in encrypted traffic**. As hackers find more undetected ways to access the network, Cisco is using our ability to examine network frames to identify malware—even in encrypted traffic.
- **Cloud, malware, and ransomware protection**. The integration with Cisco Umbrella for Branch makes Cisco edge devices the critical part of Cisco's Ransomware Solution. Umbrella prevents employees from accessing suspicious, compromised, or malware web sites. It also prevents malware and ransomware bots from reaching their parent, which is normally required to operate.
- **Mobile worker protection**. Mobile workers are probably the most prevalent malware infiltration points because they are often free to access the internet when they are remote. The Cisco AnyConnect security agent with VPN can be augmented with Cisco Advanced Malware Protection and Cisco Umbrella for Mobility to keep safe when off-net. It also allows connection via VPN to many Cisco edge devices. None of this single-agent mobile device security will operate in a commodity environment.
- **Network device integrity**. Hackers have more ways to infiltrate and compromise systems than just breaking vulnerabilities in applications and operating systems. They attack the hardware and software stack of networking devices, so securing the networking device is critical for security. As it has with operating systems and applications, network device vulnerabilities will likely continue to be discovered. Cisco operates stringent rules for software and hardware development, complete with regression testing to help ensure Cisco customers can continue to operate a trustworthy network.

Deeper Data and Faster Insights

The Cisco edge serves as a wealth of knowledge about what's truly happening in your business, with insight into your users, the devices they use, and the applications that they access. It has the ability to understand and learn from the devices on the network to automatically adapt to changes and needs. It provides location-based data to better understand how users interact with the environment to make better business decisions, and can deliver threat forensics to understand how threats infiltrate the business.

With Cisco IOx Fog Computing, the edge can decide the optimal place, whether on premises or in the cloud, to process this data, allowing the organization to improve performance and reduce costs. Location analytics found in Cisco Connected Mobile Experiences (CMX) delivers granular Wi-Fi and Bluetooth Low Energy (BLE) driven location analytics to deliver a realistic view of how people interact with the environment.

Business-to-consumer (B2C) organizations such as retail, hospitality, and education have been able to achieve less than one meter location accuracy with Wi-Fi + BLE and drive direct revenue increases. Some examples include 20% non-room revenue by Hyatt Regency, a three times increase in customer dwell time, and an 80% improvement in user experience at Stary Browar mall – all while delivering personalized mobile experiences.

In addition, Cisco Prime™ provides a 360-degree view of your end users, their devices, and the applications used on the network. This allows for a better network planning, measurement of application adoption, and lower costs.

Adapt as the Business Evolves through Automation

With more users, more devices, and more locations to manage, the need to automate processes and new services with day-zero and day-one capabilities becomes more of a requirement. In the wired and wireless access space, a campus and data center fabric with decoupled software overlay running on custom application specific integrated circuits (ASICs) allows:

- Enhanced scale
- Service assurance
- Security
- Other services for both physical and virtual devices, applications, and users

Network virtualization can enable network and policy management by user type to quickly launch and customize applications and contain threats faster. It is a centralized approach for securely deploying new remote locations in minutes instead of days over any connection type.

The Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) delivers centrally controlled plug and play (PnP) and easy quality of service (QoS) functionality for zero-touch deployment at the edge. It also allows dynamic application prioritization for your critical applications.

Cisco delivers software-enabled agility for customization. Through tightly integrated software and hardware platforms, we can provide significant benefits to your organization, which will be evident at the WAN and access edge. WAN-customized components include fast ASIC, and cloud management software makes Cisco Enterprise Network Functions Virtualization (Enterprise NFV) a reality, where you can turn on network services in minutes instead of months. Enterprise NFV provides the compute, storage, networking infrastructure, management, and assurance capabilities to run network services so you can reduce complexity in the branch and enable new services on demand at the edge.

Organizations have seen a 79% reduction in deployment costs with APIC-EM PnP, and 85% faster provisioning with APIC-EM Intelligent WAN apps.

With the vast numbers of users and devices connecting from all types of sites, the network edge can be in large campuses or small remote sites. Global topology views with automated PnP capabilities significantly lowers the cost of onboarding or upgrading a network device such as a switch, router, or access point. Additional apps on the controller enable network-wide QoS provisioning, quickly protecting business-critical traffic from non-critical bandwidth consumers. Specialized apps like the Intelligent WAN (IWAN) app enable provisioning, monitoring, and troubleshooting of security, encryption, path selection, and application visibility and control over the WAN.

Additionally, Cisco ONE™ Software delivers a valuable and flexible way to buy software for your edge. At each stage of the product lifecycle Cisco ONE Software helps make buying, managing, and upgrading your network easier. Realize a strong ROI as your investment grows through ongoing innovation, updates, and upgrades for physical and virtual machines.

Application and Device Awareness

Cisco is the only vendor to partner with mobile device industry leader, Apple, to deliver a better mobile experience. This strategic partnership for both companies leverages the intelligence in the network to provide the best Wi-Fi experience through optimal roaming. In other words, it's a fast lane for business-critical applications on Apple iOS devices at the workplace to improve employee productivity.

Enterprises can expect up to eight times faster roaming and 66% more reliable Wi-Fi calling, 50% reduction in network management overhead due to fewer SSIDs, and end users can save their iOS device battery life by 30%.

For many years Cisco has delivered Wi-Fi innovations that go beyond the current standard and serve as proof points for the next standard. Cisco Aironet® wireless technology delivers high-density experience innovations that improve the airwaves, device performance, and application experience. Cisco has also pioneered Flexible Radio Assignment technology that optimizes the performance of the Wi-Fi network without limiting radio availability. This ability allows the wireless access points to identify sudden needs for wireless bandwidth and automatically adapt the wireless network to meet that need. This is critical in areas where large numbers of users congregate and battle for wireless bandwidth.

The digital business depends upon the applications it uses to increase productivity and to engage with customers. Cisco delivers Application Visibility and Control that detects applications at the wired and wireless edge. We use intelligent path control to select the best path over your WAN while optimizing the delivery over your wired or wireless LAN so your users enjoy the best possible application experience.

Organizations can get deep application visibility for over 1200 applications and prioritize business-critical apps with a click of a button with APIC-EM and Cisco Prime Infrastructure.

The edge has the ability to control and improve employee experience in the physical space. The Cisco Digital Ceiling extends the benefits of the IoT by converging multiple building networks, including:

- Lighting
- Heating and cooling
- IP video
- IoT sensors
- And much more through a secure and intelligent network platform

A Digital Ceiling unlocks new experiences and efficiencies for workers, and lowers facilities operating costs.

Designed for Whatever the Future Holds

Designed with the future in mind, without a Cisco IOS-XE operating system that has standards-based, model driven programmability, the Cisco edge prepares the network to add new functionality and adapt as changes in the environment, the business, or the industry. This makes the edge network open, programmable, and extensible.

The edge is transitioning from a customized device-by-device model where segmentation and access control are added onto a network configuration, to a full policy automated solution. In the future, networks will not need to be directly provisioned. You will be able to express policy as a simple intent. Further, you can determine what user or groups have access to certain privileged groups of applications or data, whether on premises or in the cloud. The network will get automatically provisioned to enforce this policy, while still allowing massive flexibility to monitor, troubleshoot, remediate, or apply additional services to certain traffic.

The edge is also becoming fully programmable. Orchestration solutions can interface with the edge using standard model-driven APIs, Python scripting, or other Linux style tools. This makes integration of the edge into modern software development methods simpler, enabling agility and customization like never seen before.

Continued Innovation at the Network Edge

With the expected explosion of connectivity bringing significant opportunity, companies are starting to recognize that this transformation will require fundamental changes to their network infrastructure and the ability to manage and analyze the data. We are leading the way through this transformation by driving innovation in network infrastructure, management of infrastructure, and analytics to extract actionable insights from the data.

Cisco aims to transform troubleshooting that is reactive to proactive, and reduce resolution time from days to minutes. We will do so by treating every device in the network as a sensor and a distributed data processing element. By getting data from devices in the edge, distributing processing closer to the source of the data, we can perform analytics at line speed to generate actionable insights through machine learning.

With the largest installed base and custom ASIC solutions, Cisco is uniquely positioned to design hardware and software optimized for analytics. Harness the power of installed base. Wired and wireless combined in one network will mean that intelligence on the edge can help you troubleshoot problems, whether they happen at the edge or not, in seconds. And over time, correct potential problems even before they occur. This will help IT departments deliver on the service-level agreement (SLA for the network and application performance required for the future.

Conclusion

With so much depending on the network edge, the commoditization of the wired and wireless LAN and WAN introduces risk that could result in security breaches, loss of productivity and revenue, loss of opportunity, and lack of visibility. The Cisco network edge allows organizations to go beyond an off-the-shelf, standard-bound approach, delivering high-value intelligence at the edge.

This approach allows organization to:

- Protect the business with a strong first line of defense
- Confidently deliver applications to target audiences
- Deliver a seamless experience to employees anywhere
- Engage with customers to drive new revenue streams
- Better manage IoT devices and optimize the physical environment
- Provide the optimal view as to what is truly happening in the business

For More Information

To learn more, visit our Cisco Unified Access Technology page at http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

C11-737691-00 08/16