# The Ultralight Branch

*By John E. Burke*
*Principal Research Analyst, Nemertes Research*

## Executive Summary

*The distributed, virtualizing enterprise seeks to limit—or break—the relationship between physical location and the ability of a business to function. The ultralight branch helps enable this: a near-zero overhead location that can be lit up quickly, serve as long as it is needed, and powered down just as quickly. UBs let the business drive the placement and lifespan of branches while minimizing real estate, infrastructure, operational, and service costs. Such a branch requires connectivity to the Internet (for cloud services and VPN to the WAN), and/or to the WAN; must provide a local network for staff and supporting VoIP and wireless devices (company owned or BYO). It requires security to mitigate the risks of direct-access Internet as well as of wireless users and BYO mobility. It has to be remotely manageable, so it can work with little or no hands-on intervention by IT staff. It has to be cheap to light up and shut down, with a minimum of on-site network appliances or other IT infrastructure.*

## The Issue

Enterprises are shaking off the bonds that tie them to specific places. In a process echoing the virtualization of data center resources, they are beginning to decouple their ability to do business from the requirement that their staff be in a particular place.

On the one hand, they have rapidly embraced some key technologies to free staff from the need to be in the same place as each other in order to collaborate.

- They are deploying VoIP and are following up with unified communications and collaboration tools: 94% of organizations in Nemertes annual benchmark of enterprise technology (for which Nemertes interviews IT staff in hundreds of companies across more than 15 industries and all sizes from fewer than 20 staff to more than 100,000) are deploying VoIP now or planning to by 2012, and nearly three-quarters have deployed or will roll out UC. About two-thirds are also deploying or planning to deploy softphones. More than half plan to deploy desktop video conferencing.
- They are deploying virtual desktops: 52.3% of enterprises are deploying virtual desktops, with on average more than a quarter of the staff using them regularly already, and more than a third

projected to be doing so by 2012. A significant portion of these users is telecommuters.

- They are supporting mobile users: The rapid infusion into the workplace of iPhones and iPads (now supported by 53.3% and 46% of organizations, respectively) and Android phones (44.6% of organizations) and tablets (19.3% adoption in less than a year) is increasing enormously the number of people who have continuous access to mobile devices that can provide a platform for robust applications and even access to remotely-hosted virtual desktops.
- They are cloud and Internet empowered: eight in ten enterprises now use Software as a Service (SaaS) solutions that deliver enterprise applications to users over the Internet. Four in ten companies use more than five SaaS-delivered applications, and, overall, enterprises expect the number of SaaS applications they use to more than double.

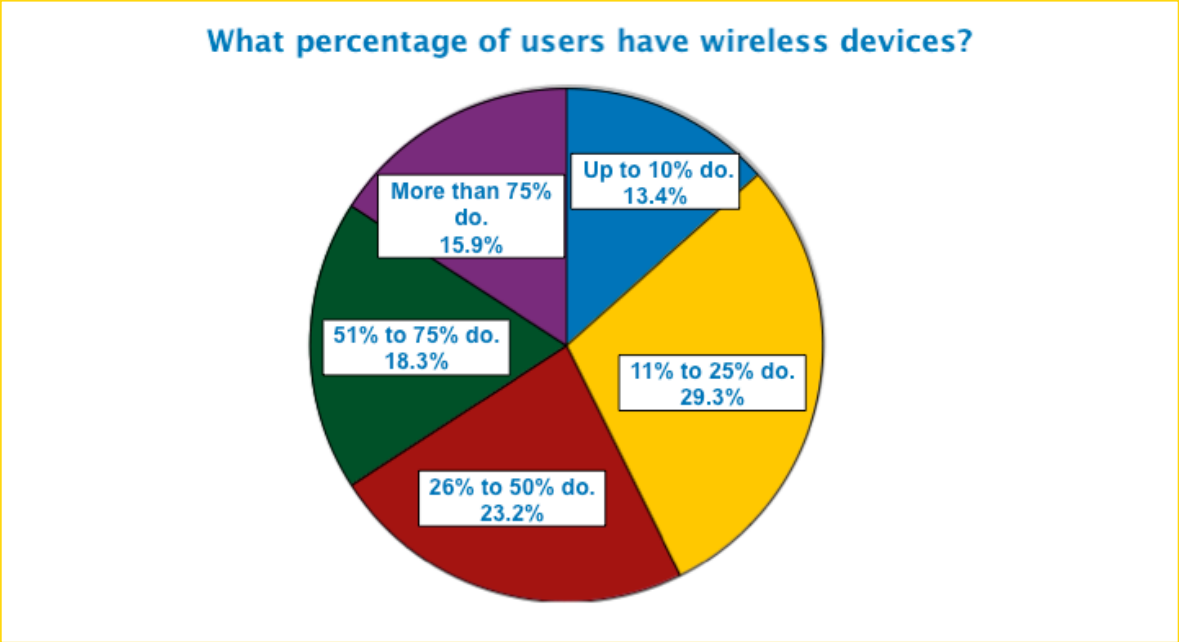


**Figure 1: Penetration of Smartphones and Tablets into Enterprise**

On the other hand, enterprises are making their use of physical space more flexible and agile, to match the agility with which they now seek to respond to shifting business conditions. Instead of establishing branches with the expectation that they will anchor (and grow with) a growing presence in an area, they increasingly wish to establish branches they expect to be short-lived and focused. They fully expect offices to have a lifecycle measured in months to years rather than years to decades. Some reasons for transient offices include to support a merger or acquisition, an outsourcing contract or other major project, a large engineering, construction or renovation job, an election campaign, a convention, or even a natural disaster.

They also seek to make perceived-permanent offices (existing offices, and those not created with a definite lifespan in mind) more manageable and modifiable. They seek to place (or move) smaller offices outside major or regional business centers, either to put them closer to pockets of staff, or to pools of customers and prospects; or to save on real estate costs; or all of these.

In sum, the distributed, even virtualizing, enterprise needs a branch strategy that can support the new classes of mobile, highly collaborative staff and the technologies that empower them, while at the same time supporting a business model increasingly focusing on branch agility. It needs a branch strategy that minimizes both capital and operating expenses, supports desired security, and creates minimal amounts of drag or inertia in deployment, redeployment, and retirement of branch resources. It needs an ultralight branch.

## Connectivity for Branch and User

The primary enabler of any branch office in the modern enterprise is connectivity. For a small branch, connectivity averages 8.5Mbps now, thanks to the rapid shift to Carrier Ethernet, DSL, and cable modems (steadily displacing the old fractional or full T1 connection). Moreover, that connectivity is increasingly delivered solely via an Internet connection: 50% of companies use direct-to-branch Internet for some or all branches, and 44% of branches use an Internet VPN as either primary WAN connectivity or backup in case a WAN connection fails. (Please see Figure 2, below.) The ultralight branch will often plan on short-contract access, and Internet via consumer and/or wireless last-mile is emerging as a popular choice as prices continue to decline while reliability increases.

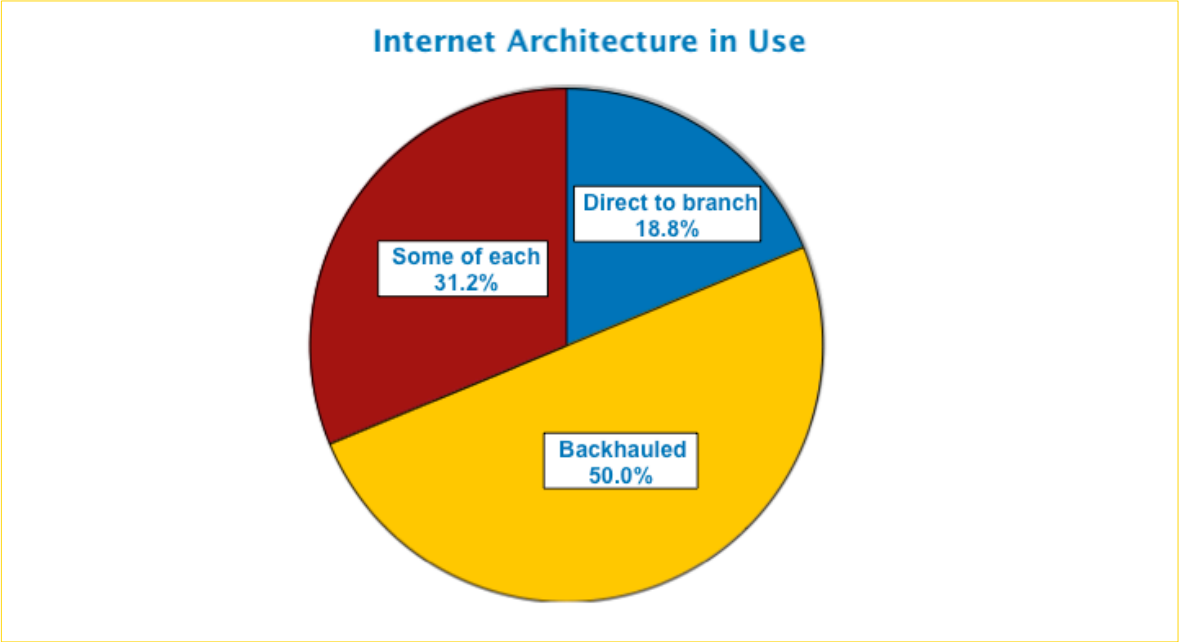


**Figure 2: Direct-to-Branch Internet**

Of course, external connectivity is only useful in so far as it passes through to end users. IT will not want to have to cable (or get cabled, or check the cabling in) each new location; that's too much overhead, too much drag. Instead, the ultralight branch will rely on wireless LAN for internal connectivity. Already, 90% of companies support a wireless LAN based on the 802.11a/b/g standards, and 67% support 802.11n use.

This rapid uptake of 11n wireless is crucial in an enterprise increasingly dependent on VoIP and UC: the higher bandwidth and superior traffic management possible with 11n WiFi make the use of advanced multimedia communications over wireless practical and high-performing instead of unreliable and frustrating, as was so often the case with older WiFi versions. It makes WiFi acceptable as the sole means of connectivity for laptops and desktops for nearly all workers, and even outside the small-branch context we see its use spreading. (Please see Figure 3.)

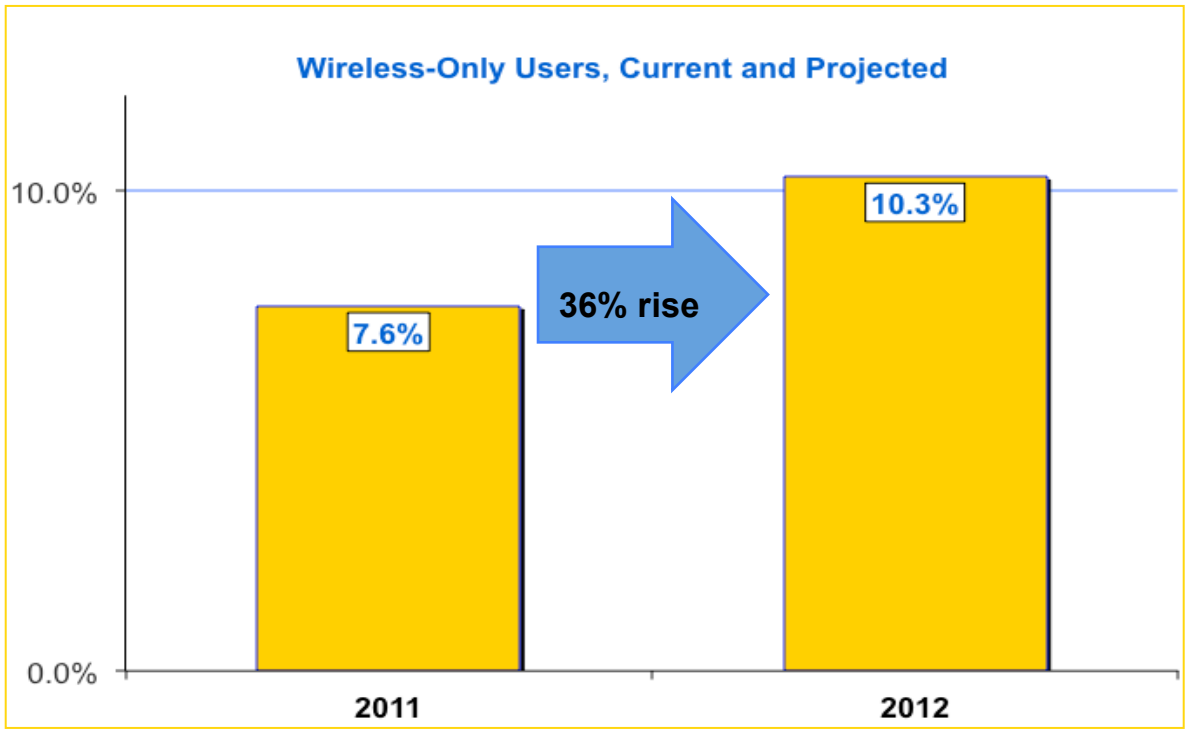


**Figure 3: Rising Wireless-only Population**

Another shift in the enterprise that is placing increasing emphasis on the quality of the branch WLAN is the arrival of those data-thirsty smartphones and tablets on the company network. What is most significant about it from a support and architecture standpoint is not the volume of data these devices want to consume (although this is something that needs to be planned for) but rather the fact that nearly half of all companies (48.4%) are allowing or requiring a "bring your own device" (BYOD) model for at least some groups of users. They may have

employees paying for devices, or have a combination of employee- and company-paid models.

BYOD has significant implications for security in the ultralight branch, since devices over which IT has little or no control are being invited onto the company WLAN. About 65% of organizations have authenticated network access or some other form of network access control for laptops, desktops, and sometimes other devices connecting to the company WLAN. By contrast, only about 35% of companies use or have any plans to use mobile device management (MDM) tools to assert some degree of security presence on the personally owned mobile devices their staff bring on to the WLAN. To make the ultralight branch a mainstay of company organization, IT will have to implement security either on the device or in the WLAN to deal with the flood of new devices: authenticated network access at a minimum, but with more robust health checks and flexible virtual LAN management desirable.

## Security

Of course, BYOD is not the only aspect of security the ultralight branch needs to take into consideration. Even though it contains only a few people, typically, the work accomplished in ultralight branches can still be crucial work. To the business, it doesn't matter from a security perspective whether a thousand people are jammed into one branch rather than spread across 25; what matters is the work they are doing. Half of all enterprises say the work function of a branch, not the number of people at it, is the prime determiner of how the branch is equipped and what services are provided to it and through it. This dictates security parity between the ultralight branch and other location types.

So, IT will want to bring to bear all the same technologies in defense of the branch that it uses to protect any data center or other major facility. They will want this to work without having anybody at all onsite to deal with the security systems—the ultralight branch won't have a security staff. Luckily, most enterprises are well prepared to take this on, at least procedurally: 72% already have complete centralized control of security, while only 25% allow some degree of local control.

Sitting on the "perimeter" of the enterprise network—to whatever extent the idea of perimeter still has meaning—the ultralight branch will first and foremost want to have the full spectrum of perimeter-type security systems in place. This includes firewalls, web filters, and IPS systems. It is not just position that makes this compelling: about a third (32.5%) of enterprises consider their edge defenses to be their most successful security technologies. Another 23.5% say identity-based security systems are their most successful security technologies. Network access control, as discussed above for BYO mobile devices, will be the "teeth" of identity management within the ultralight branch; most organizations (65%) are planning on or already using authenticated network access, the most basic form of network access control, on their WLANs, although many want and hope to implement fuller health and trust checks later.

IT will want a very complete set of security technologies brought to bear in the ultralight branch…but in order for that branch to remain ultralight, it will need

to deliver them in a very compact way. IT will not want to replicate (and manage) a stack of 6 different security appliances in a branch meant to be lit up and torn down at the drop of a hat. So, it will need to turn its attention to all-in-one appliances that integrate all key functions, router to WLAN to security (firewall, IPS, web filter, network access control, etc.), or it will need to use cloud services to provide them, or it will need to use some hybrid strategy embracing both. The hybrid strategy allows IT to balance the capabilities built into a box with supplemental function delivered in the cloud: the less it wants in the hardware, the more it will need to use the cloud. Moreover, cloud services could mean either dedicated security embedded in WAN/Internet links, or public cloud security systems accessible over the Internet, or both. The "firewall in the cloud" is an ideal model for such services. In this model, the network link provides both direct (not backhauled through the data center) access to the Internet for the branch, an IPSEC WAN connection into the company WAN, and the provider uses its position in the cloud to filter traffic through firewalls and other systems. (Please see Figure 4.) IT can also use other kinds of Internet-based Security as a Service (SecAAS) tools, e.g. for web filtering, directly from/for the branch to supplement services provided in a branch device.

However it is achieved, it is important that the enterprise not have to give up required security functionality to achieve horizontally scalable, low-overhead, highly agile branching. The only thing the branch should have to give up due to its size is the ability to scale to the highest throughputs, since a small branch won't have those.

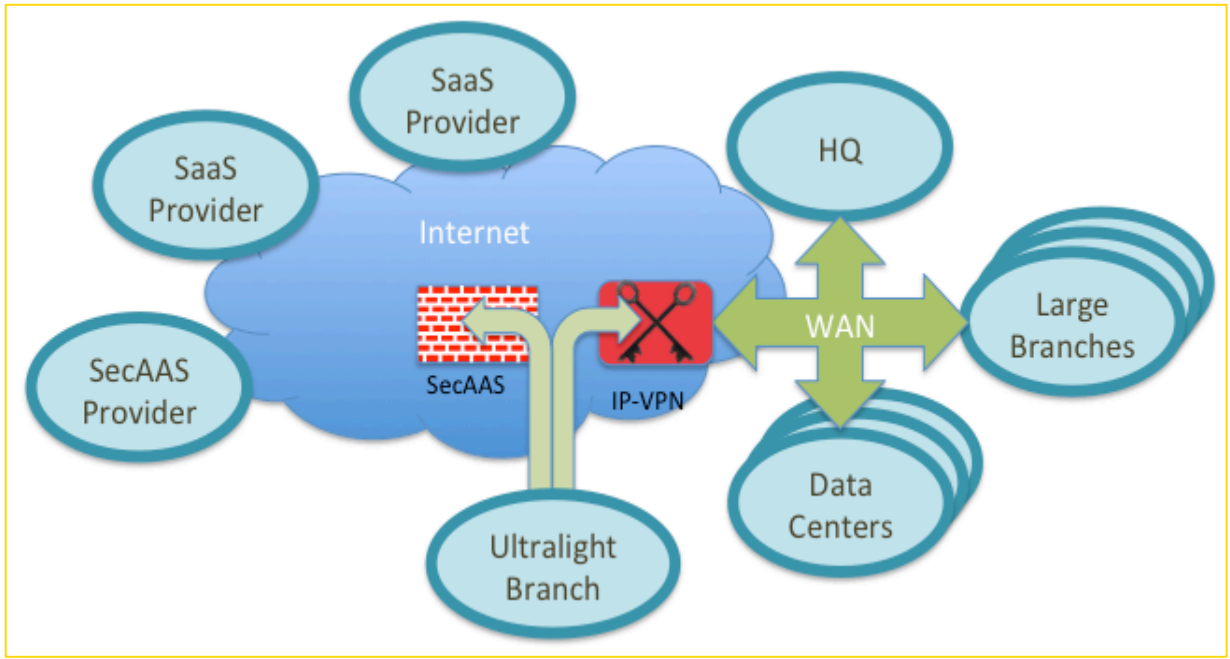


**Figure 4: Security as a Service for the Ultralight Branch**

## Simplicity: "Look, no hands!"

The cloud may be critical to the management of ultralight branches beyond just security functions. IT is still in the process of stripping staff out of branches and consolidating them in central locations. Half of all companies have IT staff on site at fewer than 25% of sites, and the overall average is only 36%—and declining. And, of course, staff will be targeted at larger sites with more users, since the primary function of on-site staff outside headquarters is hands-on user support.

IT is well versed in doing remote management of branch infrastructure, and also increasingly willing to use managed services to provide its hands-on, onsite support. The ultralight branch will favor centralized, remote support, since traditional outsourced support is often priced by the location rather than per staff member or device supported at a location. Per-location pricing isn't favorable to a many-small-branches strategy. So, IT will be looking for systems that make management as simple and robust as possible across large numbers of similarly equipped sites. Moreover, with cloud-based management options, IT can ensure continuity of management independent of IP-VPN availability or performance.

## Frugality

Having a lot of little branches implies that each branch has to be cheap to spin up. Not having IT staff on site is therefore key, as is minimizing the equipment stack that accompanies each branch. With mean annual communications spend for a branch at $62250, IT will be looking for ways to make ultralight branches cost far less. Using Internet connectivity, wireless and mobility in the ways described above, which more technologically aggressive companies already do, should help.

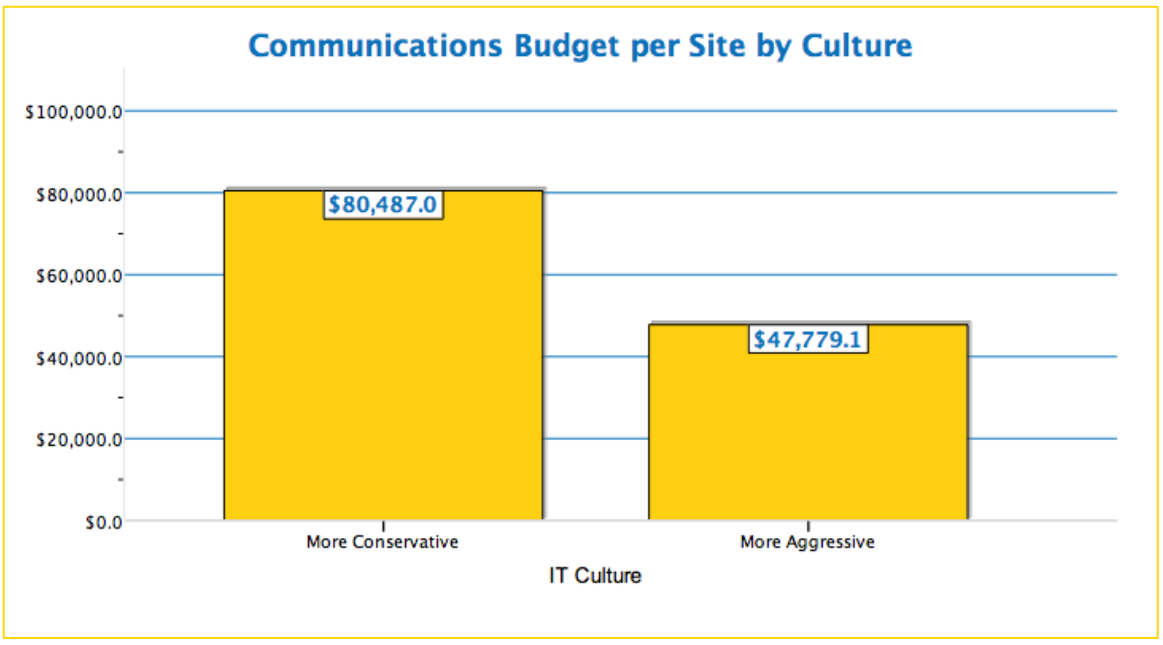


**Figure 5: Communications Budget per Branch**

Nemertes finds that IT-aggressive companies spend less per branch. (Please see Figure 5). The important thing is that paying less, on connectivity, staffing, and security, should not bring with it significant degradation of services offered. Spending less per branch shouldn't short-change users, and lower cost should flow from lower capacity and smaller device pools rather than decreased function.

## Conclusions and Recommendations

The distributed, virtualizing enterprise seeks to limit—or break—the relationship between physical location and the ability of a business to function. The ultralight branch helps enable this. By shifting from traditional mid-sized to small branches to larger numbers of very small locations, the enterprise can more agilely address its business needs and opportunities. This strategy requires that IT be able to implement a location for a small number of users with very low overhead, and that it be able to turn up services at such locations very quickly—and turn them down again just as quickly. Ultralight branches let the business drive the placement and lifespan of branches while minimizing real estate, infrastructure, operational, and service costs. Such a branch requires

- connectivity to the Internet (for cloud services and possibly for an IP VPN link into the company WAN), and/or a direct WAN connection
- a local wireless network for staff, one capable of supporting not just traditional laptops and desktops and data access but also VoIP and other real-time multimedia functionality, as well as wireless mobile devices (company owned or BYO)
- the full panoply of security services IT uses to mitigate the risks of direct-access to the Internet as well as of wireless users and BYO mobility, delivered via appliance on-site or cloud service or hybrid of both
- full function with little or no hands-on intervention by IT staff.

And, ultralight branches will have to meet all these requirements with as little equipment on site as possible, to help keep per-site costs and "weight" low. IT staff should therefore:

- Seek branch network solutions that can combine as many required functions as possible.
- Seek solutions with robust centralized management.
- Explore cloud- and web-based security solutions to replace or supplement on-site security appliances.
- Embrace at least authenticated access (802.1X compliant) on WLANs and explore access controls beyond this, including device heath checks and ongoing network behavior analysis.
- Push for unified, policy-driven security and performance management.

---