FROST & SULLIVAN

The Modern LAN: Rethinking Network Design for the Modern Age

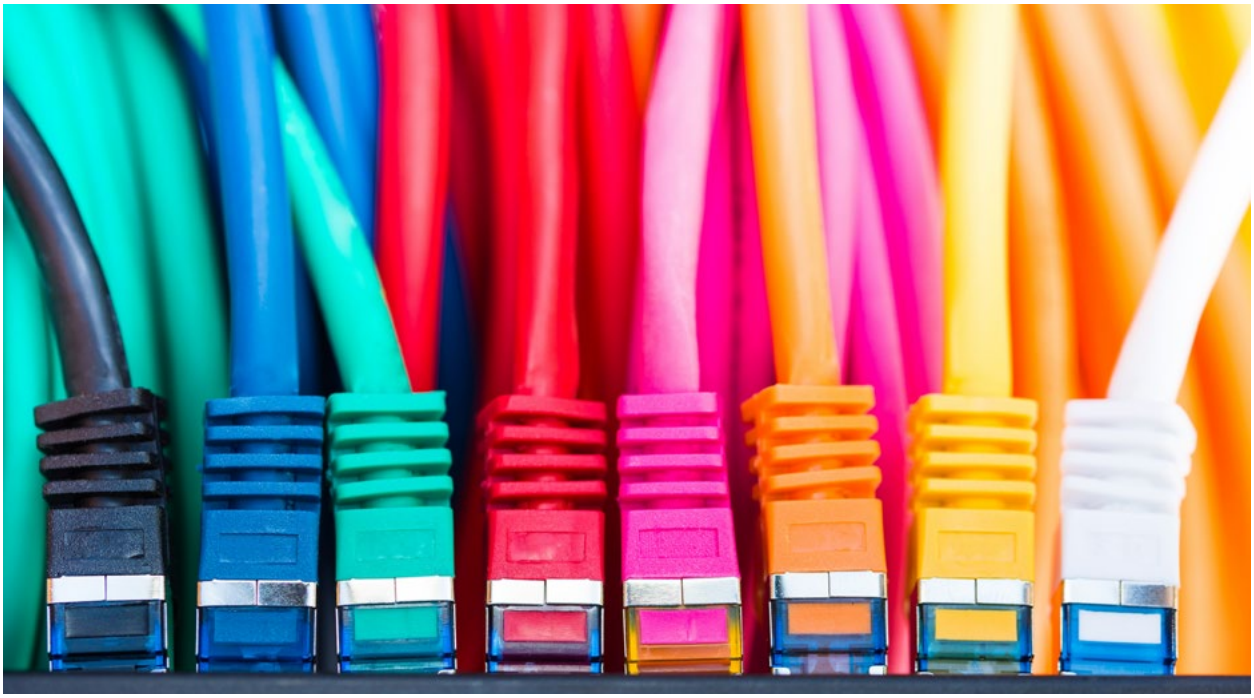
Is your LAN Ready to Securely Connect to the 'Things' of the Internet of Things?

A Frost & Sullivan White Paper

EXECUTIVE SUMMARY

Traditional network designs are trapped in a PC-centric world, putting intelligent systems at risk of significant cyber threats and poor environmental stewardship, as well as negatively impacting the company's bottom line. The local area network (LAN) is the nerve center of most businesses today, delivering mission-critical applications and communications to end users throughout the organization. Businesses rely on their data networks to operate every facet of their operations, with intelligent, connected devices replacing everything from the phones on employees' desks to the cameras and sensors that secure their facilities. However, Frost & Sullivan has identified a significant challenge to these smart organizations: the local area network.

Smart systems need a smarter network. Modern LAN design, based on a fundamentally new set of best practices reflective of these new platforms and intelligent devices, directly addresses many of the challenges that network architects and administrators are facing. Modern LAN design considers not only bandwidth and power requirements, but also environmental concerns, security threats and end-user needs. The goal is to establish a sustainable framework to make the network as smart as the devices and applications it supports.



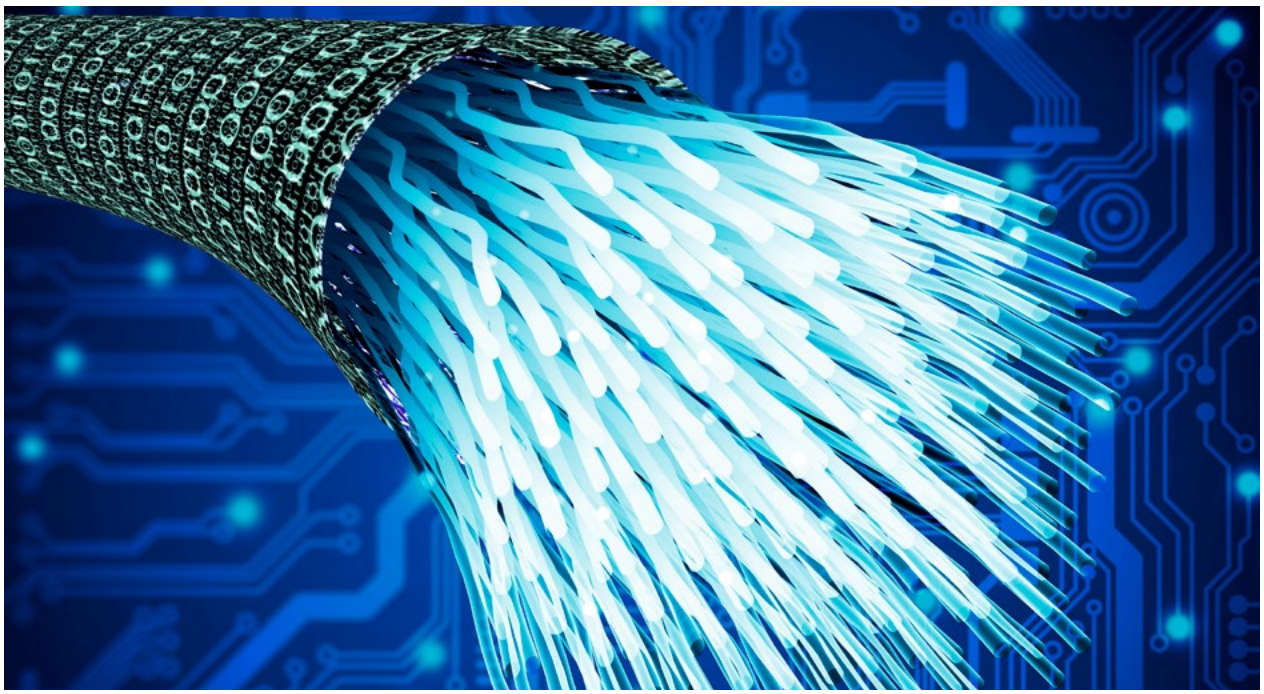
The key principles of the Modern LAN not only offer the opportunity to rethink how best to architect a local area network but also how to most effectively adapt the network to technology disruptions and digital transformation efforts; deliver cost-effective security; and incorporate environmental responsibility and sustainability into network design. This white paper will highlight the challenges that many businesses face under traditional LAN design precepts, identify a new approach to local area network design, and offer a new set of networking best practices to deliver a Modern LAN that will support business needs today and well into the future.

UNDERSTANDING THE CHALLENGES OF TRADITIONAL LAN DESIGN

Seasoned network administrators are well-versed in the best practices associated with traditional local area network design, which have their roots in the era of client-server applications and the early role that the personal computer played in business applications. In a PC-centric network architecture, making an ever-increasing amount of bandwidth available to end-user desktops was critical to ensuring the proper performance of core business applications. In addition, real-time communications, such as Voice over IP and video conferencing, migrated from their own dedicated infrastructure to Internet Protocol (IP) and local area networks for transport, both as standalone hardware endpoints and as desktop applications.

> **To stay competitive, network architects must reassess their traditional best practices and adopt a new set of design principles reflective of the evolving network landscape.**

Today, however, these traditional LAN design practices, based on homogenous network infrastructure and assumptions of high-bandwidth requirements, are creating a number of challenges as businesses incorporate a diverse set of endpoints across their networks. The proliferation of network endpoints, the advent of cloud-based services, mobile-centric applications and the Internet of Things (IoT) are all disrupting traditional LAN design. In its place is the Modern LAN, a new set of design principles and a new deployment methodology for local area networks that must support a wide array of devices.



Let's look at a few key considerations:

Network Consolidation Introduces Security Risks Prior to the modernization to IP-based transport, security solutions (cameras, motion sensors, keycard readers and access control devices) and communications solutions (desktop phones, conference room phones and video conferencing endpoints) operated on their own physical

network islands. While this approach limited integration, it provided a measure of security and reliability for each network. IP-based LANs, on the other hand, offer new capabilities for security and communications platforms, including a deeper level of integration with business applications and an economy of scale that comes with shared infrastructure. But those advantages come at a cost. With a shared infrastructure, inadequately vetted and quickly deployed IoT devices and services can negatively impact mission-critical security, communications and PC-based systems. Conversely, bandwidth-hungry applications and services could inadvertently starve other devices. Desegregation puts all devices at risk of denial-of-service attacks, malware or even a rogue endpoint consuming more network bandwidth than it should.

Infrastructure and Physical Plant Requirements: High-bandwidth network connectivity is often hampered by distance limitations. The reach of Ethernet over industry standard CAT5 or CAT6 structured cabling is limited to 100 meters between networked devices. For small offices, 100 meters might be reasonable, but larger facilities will require a network infrastructure to be specifically architected around this limitation. As a result, intermediate distribution frames (IDF), commonly referred to as secondary wiring closets, are required to deliver Ethernet connectivity throughout a facility. IDFs serve as a junction point for Ethernet cabling, with network switches installed to address Ethernet's distance limitation and connect nearby networked devices. In a traditional or PC-centric network architecture, structured cabling can be planned for and incorporated into office or cubicle layouts. But that becomes a significant barrier when a business factors in additional endpoints, such as IP-based phones, overhead paging, security cameras or IoT/smart building sensors. These types of devices are often deployed out of reach to avoid tampering or, as in the case of sensors, installed in locations throughout a facility. In either case, such network elements often push the bounds of Ethernet distance limits; in traditional LAN designs, they will likely require additional IDFs to run smoothly.

Perpetual Buying Cycles and Sunk Costs Each major advance in Ethernet speeds requires new hardware. To achieve performance upgrades for fixed-configuration or non-expandable network switches, businesses must replace the entire switch and invest in new gear. For businesses that have invested in modular network switches, Ethernet speed upgrades require replacement line cards, although port density (the number of Ethernet ports available per line card) is often compromised for the sake of port speed. Regardless of the type of Ethernet switchgear, a PC-centric LAN architecture, and its continuous need for additional bandwidth, results in a steady cadence of "rip-and-replace" upgrade cycles to keep pace with the advances in speeds and feeds. The cycle can happen even more frequently when endpoints equipped with power over Ethernet (PoE), such as VoIP desk phones, IP cameras, and Wi-Fi access points, are deployed, since PoE-enabled network switches are necessary to deliver power to these endpoints (at additional cost). Finally, as Ethernet speeds increase, the physical cable plant may have to be recertified or even replaced to handle the additional capabilities, extending the sunk costs assumed by businesses.

CONVERGENCE ON THE MODERN LAN

Local area networks, once the domain of desktop computers, servers and printers, now play host to multiple, previously disparate networks:

The **business communications** network, including communications platforms, desktop phones, overhead speakers, and paging and intercom systems.

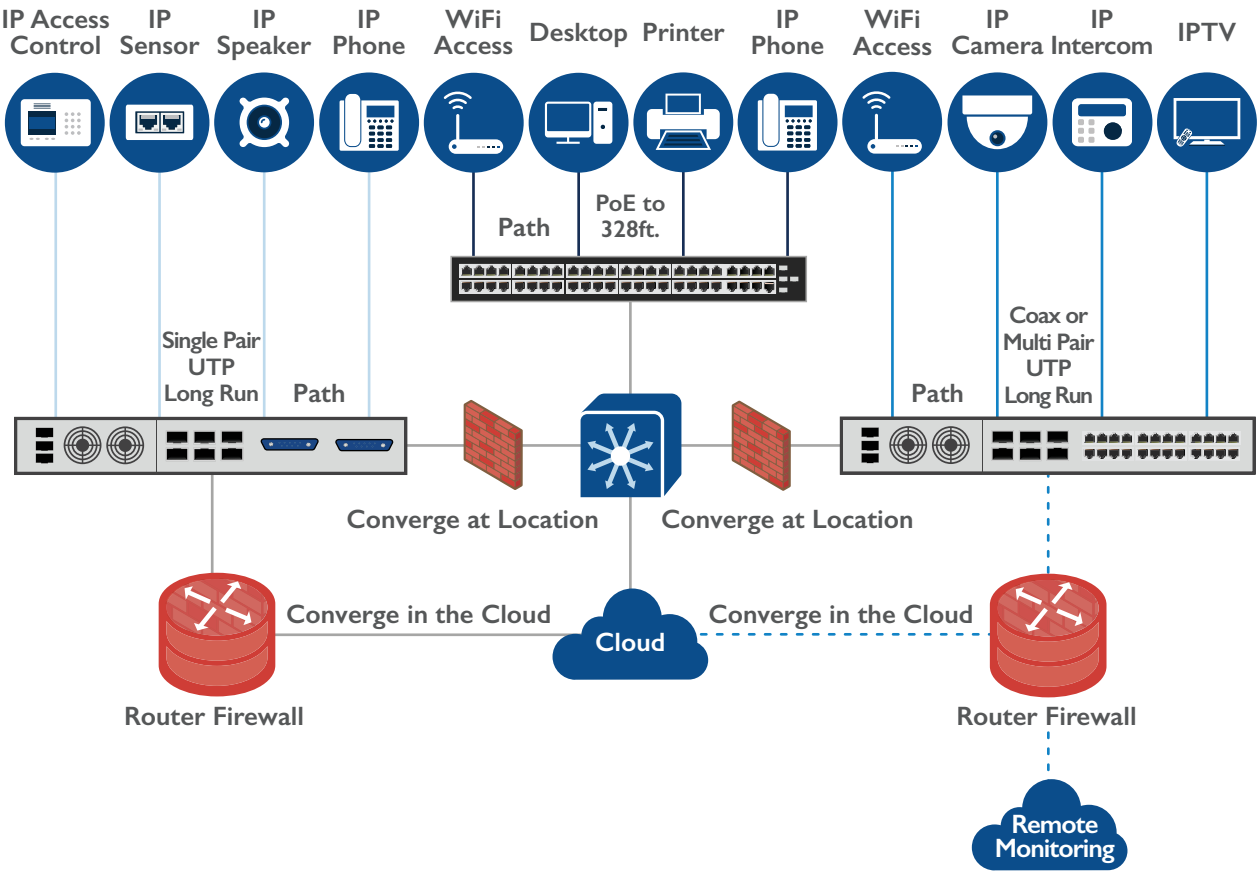
The **security and access control** network, featuring monitoring and video recording stations, motion and alarm sensors, beacons, access card readers and cameras.

The **building and facility** network, which manages HVAC and climate control systems, LED lighting, and, increasingly, IPTV, digital signage and distributed antenna systems.

Dealing with Exceptions While most network administrators strive for homogenous local area networks and centralized management, the reality is that there are always going to be exceptions to the rules when it comes to deploying network devices. For example, based on their physical location, security cameras often require a long-range power over Ethernet (LRPoE) solution. Traditional LAN design, with its PC focus, simply cannot account for these types of modern network devices, forcing the administrator to make the tough calls about how to resolve exceptions. In a traditional LAN design, this means deploying additional network switches and, in many cases, additional IDFs (with their added power and cabling demands) to deal with Ethernet range limitations. Alternatively, a network administrator may choose to leverage alternative Ethernet solutions, such as LRPoE products, but they are treated as one-off or quick fix installations. As more platforms are migrated to IP, these exceptions are becoming more prevalent, but they remain outside the core network strategy. Without a clear corporate-wide approach to dealing with exceptions, previously pristine corporate networks can degrade into a mashup of inconsistent point products impetuously purchased and deployed to address an immediate need. The result: more work to manage the network, increased exposure to potential security risks and excessive IT spending.

BREAKING THE THREAT CYCLE WITH A MODERN LAN ARCHITECTURE

To address the many challenges that businesses and network administrators are facing, Frost & Sullivan recommends a fundamental rethinking of local area network design. First and foremost, Modern LAN design requires a clean break from the PC-centric focus of the past to truly account for the myriad devices that now exist on corporate networks: unified communications endpoints, security cameras, access control units, mobile devices and the emerging use of IoT sensors, beacons and control platforms.



To that end, Modern LAN design prescribes an outside-in approach. Whereas traditional LAN design principles focus on the core, aggregation and edge networks with little consideration for the endpoints themselves, the outside-in approach starts with a deep assessment of the endpoint devices on the network. By understanding the needs and purpose of each network device on the edge, including bandwidth, power and physical-placement requirements, companies can leverage the most appropriate network deployment. For example, while PCs, servers and video conferencing units are bandwidth-intensive devices with little to no PoE requirements, IP phones, security cameras and IoT sensors are the opposite, with strict power needs (often at long range) but relatively small bandwidth requirements. Modern LAN design accommodates each of these devices, ensuring their unique needs are met in the most efficient and cost-effective way possible.

Modern LAN design principles also address the desegregated network created by traditional designs. With an outside-in approach, network administrators are empowered to incorporate a level of physical segregation among solutions, while still maintaining the advantages of IP network integration. For example, on a Modern LAN, security devices are consolidated on their own switches, creating a dedicated path, rather than being spread across the same edge switches as PCs or wireless access points. In the event of a network issue on the primary application network, the security network remains unaffected and operational, and vice versa.

Modern LAN design also aligns closely with the environmental responsibility and sustainability initiatives many organizations are currently undertaking. First, modern LAN practices cater to the exact bandwidth and power requirements of the deployed network endpoints and apply the best network switching gear to meet those needs, rather than traditional network designs that applied a "one-size-fits-all" approach to network architecture. This means that the lifecycle of Modern LAN architecture components will vary by the endpoint they are serving. For example, while the network gear for PC and servers may continue to need continuous upgrades, the switches connecting IP phones, security cameras or other low-bandwidth devices will need to be upgraded far less frequently. By focusing on the endpoints, rather than the network itself, an organization can drastically reduce the "rip-and-replace" cadence as well as lower their e-waste output over time.

Modern LAN design also encourages the reuse of existing cabling infrastructure, including reliable twisted-pair wiring and coaxial cabling. Many organizations, guided by traditional LAN design and conventional wisdom, have abandoned this established cabling infrastructure as part of previous IP modernization efforts. Paired with the right network solutions, such as long-range power over Ethernet (LRPoE), network architects can reclaim the value of the abandoned infrastructure still installed in the walls of their facilities. In fact, leveraging existing cabling can accelerate smart-building, digital transformation and

THINKING MORE ABOUT POWER

Considering the power requirements for local area networks means more than just finding the nearest outlet. Mission-critical applications, including security cameras, access control panels and emergency response systems, demand uninterruptible power supplies (UPS), also known as battery backups, to keep going, even if the power goes out.

Consolidated networks, based on traditional LAN design, require a wide array of UPS units spread throughout the facility, which are expensive, hard to maintain and unfriendly to the environment. The Modern LAN, with its network segregation, optimizes UPS deployment to devices that need it and offers a sustainable approach to battery usage.

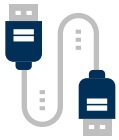
"At NMSU we are an example of Frost & Sullivan's Modern LAN principles in action," said Ray Cadena, Manager, Telecommunication Systems. "When we upgraded our telecom system from TDM to IP phones, our first action was to analyze the endpoint (IP phone) requirements. We then began a search for technology that could help us to deliver those requirements and found the PoLRE™ long reach switch. This enabled us to send PoE through our existing copper plant, re-use our point-to-point TDM topology, and safeguard the IP phone convergence to our core network. Plus, we accelerated our transformation, saved money, and the environment—pretty modern thinking if you ask me."

smart-enterprise initiatives, all while lowering costs, deployment complexity, disruption and risk. Modern LAN principles actively encourage establishing a reuse strategy in cases where the bandwidth and power requirements can be met with alternative Ethernet solutions, rather than a recycle or discard approach. Ultimately, by including sustainability and environmental impact into their network design choices, network architects can not only lower ongoing cabling and IDF closet costs but also minimize an organization's waste footprint and resource consumption.

BEST PRACTICE RECOMMENDATIONS

Adopt an "outside-in" approach to local area network design and planning. Before new endpoints are deployed, identify the power, bandwidth and application requirements of each unique physical device to determine the best topology and infrastructure to support it.

Consider the impact of all additional endpoints and applications on the network to ensure overall reliability, security and ease of management today and into the future. This must include BYOT devices (i.e., the technology employees bring into the enterprise).



Develop an environmentally responsible framework around LAN design and deployment. Re-use and repurpose existing endpoint cabling infrastructure, reduce IDF closet requirements, and adopt energy-efficient PoE switches and endpoints wherever possible.

Seek strategic opportunities to leverage existing physical infrastructure to accelerate IP modernization efforts. Repurposing existing cabling infrastructure, when appropriate, can reduce end-user disruption and implementation costs while speeding deployment of innovative IT solutions.

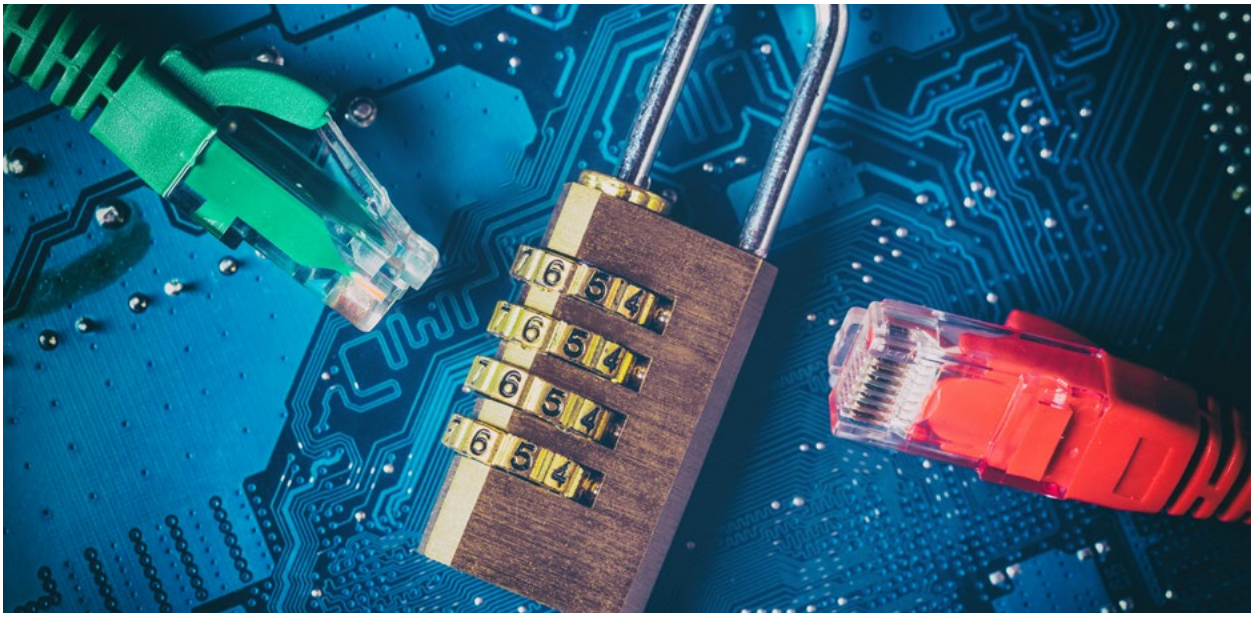
Evaluate and certify network switches and infrastructure solutions that offer LRPoE and can leverage existing physical cabling infrastructure and topologies as part of approved network standards.

When possible, construct physically separate but functionally integrated IP network paths for different and dedicated applications, ensuring mission-critical platforms are not impacted by disruptions or intrusions of the primary business network. By doing so, organizations have the option to create separate networks or connect them on site or in the cloud with a single cable.

Consider network segregation to isolate cloud-managed endpoints and minimize security or network-breach exposure. Modern LAN designs must account for multiple application and management platforms, including on-premises, server-based applications, cloud-based platforms and hybrid solutions.

CONCLUSION

Forward-thinking businesses are leveraging disruptive technology to increase productivity, enhance communications and streamline or automate many of their business processes. Unfortunately, the nerve center of these technologies, the local area network, is still being designed with an earlier generation of technologies in mind, exposing the businesses to cyber threats, cost overruns and elevated demands on an already taxed IT organization. A new set of design principles, the Modern LAN, is necessary to make today's corporate network as agile, flexible and disruptive as the technologies it is being tasked to support.



Modern LAN design directly addresses many of the challenges that network architects and administrators are facing. By taking an outside-in approach that considers environmental needs, security concerns and end-user requirements, companies can more easily take advantage of transformational technologies today and create a framework to embrace completely new solutions tomorrow.