riverbed

White Paper

# Three Issues That Will Jeopardize Your IoT Initiatives *(and How to Overcome Them)*

## Tips for IoT Infrastructure Planning, Implementation, and Management

The Internet of Things (IoT) is ushering in a new wave of digital disruption in the enterprise. While smart homes, cars, wearables, and other consumer applications of IoT have become prominent, businesses are also deploying an array of sensors, gateways, and other connected devices. Targeted benefits include better business intelligence, stronger customer engagement, automated processes for improved efficiency, and new revenue streams.

While it is still early days for most enterprise IoT deployments, numbers from industry prognosticators suggest rapid growth is coming soon. Nearly 30% of companies have adopted IoT globally, but of those, 84% expect to increase their spending and project deployments in the next year[1]. And by 2022, worldwide IoT technology spending is expected to reach $1.2 billion, at a CAGR of 13.6%[2].

Industries experiencing strong adoption of IoT include:

### Industrial Manufacturing

Sensors and machine learning continuously improve production line efficiency and throughput, and using predictive maintenance prevents equipment failures to improve the longevity of costly assets.

### Transportation and Logistics

IoT-enabled devices and apps are transforming supply chains with real-time inventory visibility and smart control systems that ensure suitable environmental conditions, reducing shipping bottlenecks and costs.

### Healthcare

Biometric devices allow doctors to remotely monitor patients' vitals on mobile devices—improving staff efficiency, accelerating diagnoses, and improving treatment plans by identifying long-term trends.

### Energy

Oil and gas companies are using sensors at remote sites like offshore rigs to improve oil well recovery rates and raise worldwide production by consistently measuring pressure, temperature, and other metrics.

What is making IoT possible? For starters, it's the proliferation of devices and machines that now have built-in connectivity and the ability to capture and exchange data. In addition, communication protocols such as ZigBee, Z-Wave, 5G, NFC, and Beacon provide greater flexibility when selecting between range, power consumption, and cost requirements for device-to-device communication. Lastly, advances to mobile, cloud, and edge computing, coupled with IoT platforms from technology providers like Amazon Web Services (AWS), Microsoft, and IBM, continue to make strong inroads in the enterprise, powering IoT services and making information universally available.

But while IoT offers unquestionable benefits, a troubling trend is shaping. According to Gartner, nearly 60% of IoT initiatives are being planned without IT's direct involvement, or that IT is only engaged after crucial decisions have been made[3]. Getting off the sidelines when it comes to planning and implementing IoT projects is a pressing matter for senior IT leaders. That's because a number of technical challenges will jeopardize IoT initiatives, including:

1. Legacy networks that are inflexible, error-prone, and not designed to support IoT.
2. Traditional IT infrastructure that is equally cumbersome, and the cloud also introduces trade-offs.
3. An influx of other security risks due to the volume and diversification of connected devices.

To be successful, IT must anticipate these issues. It starts with a firm understanding of what each challenge entails, and then identifying and adopting the right platform that addresses them while augmenting the broader IoT ecosystem.

## Challenge: Legacy Networks Won't Support IoT Deployments

A common theme involving failed IoT projects is a lack of foresight into networking needs. Legacy, router-based networks don't have the intelligence to move IoT data across the enterprise in the most effective manner possible. Moreover, IT leaders often fail to account for the increased management complexity that will overtax traditional architectures.

More specifically, IoT deployments may congest existing networks, due to the sharp increase in the number of connected devices and associated traffic. In fact, 77% of IT teams expect IoT ecosystems to add "significant" to "very significant" traffic to the network by next year[4]. When this happens, IoT services will likely crowd out other critical apps, leading to poorer performance and unsatisfied users. This is particularly true in far-flung locations, where connectivity is unreliable and bandwidth is at a premium.

To offset the capacity and cost constraints of sending IoT traffic over long distances, networking leaders are using broadband Internet, cellular LTE, and other modes of transport. However, ensuring the right application traffic—including IoT—uses the right path to adhere to performance or security requirements using device-centric networks and command-line interface (CLI) code is nearly impossible. Such approaches are error-prone, tedious, and can't keep pace with evolving needs when quick updates need to be made. This is especially true of multi-vendor networks, where dissimilar equipment compounds the complexity of managing these hybrid networks.

Another networking issue deals with wireless options. Due to its lower cost and relatively efficient power use, Wi-Fi is a common source of IoT connectivity, particularly for in-building services. However, most wireless access points will buckle under the pressure of IoT deployments because they can only support a limited number of sensors. As the number of sensors at some locations grows into the thousands, IT and business leaders will be forced to boost capacity by buying more access points—adding more points of failure and increasing management complexity.

According to Gartner, 59% of IoT initiatives are being planned without IT's direct involvement, or that IT is only involved after crucial I&O decisions have already been made.

And speaking of additional devices—the sheer number of endpoints IT teams will need to account for offers one final layer of complexity in terms of network visibility. Networking managers must re-map their networks and ensure they stay in compliance as IoT devices are continually added to the enterprise. In fact, Gartner reports that 63 million new IoT devices will connect to enterprise networks every second by 2020. Many of these will be considered an extension of the shadow IT phenomenon, as devices such as smart watches and digital personal assistants will connect to the corporate network without IT's knowledge. Alarmingly, 35% of businesses report they have at least 5,000 such devices on the network at any given time that are non-IT-issued[6].

Regardless of whether or not these IoT devices are IT-approved, discovering and documenting how they talk to one another and across other systems remains a challenge, in part because there is an inherent lack of visibility unless IoT vendors expose their APIs. Such visibility challenges expand when the back-end of an organization's IoT deployment is the public cloud, due to the loss of control over the hosting infrastructure.

## Challenge: Traditional IT Infrastructure Is Equally Cumbersome, but the Cloud Isn't a Panacea

Enterprises traditionally deployed server, storage, and backup infrastructure at each business location to support the performance needs of employees and customers using locally hosted applications. IoT would force businesses to provision even more infrastructure to accommodate an explosive growth in corporate data, but this is massively inefficient from both a cost and operational perspective.

Cloud computing resolved some of the inefficiencies of these islands of infrastructure at the edge, promising simplicity, scale, and cost-savings. But, like the datacenter-hosting model that preceded it, collapsing applications and infrastructure into the cloud can create performance and visibility problems for IT when certain apps are served over long distances; namely, application chattiness and high latency, which lead to poor user experiences.

The effects of latency intensify with data-rich IoT applications. Here, any performance hiccup or slow response time associated with sending data to and from a data center or cloud would interfere with an organization's ability to act on information as it's created. However, traditional approaches to storing and protecting data locally suffer from the same aforementioned challenges of high costs and operational complexity. And, more generally speaking, keeping volumes of data outside of the robust security mechanisms of a data center or cloud puts the business at risk. If left under-protected, an unintended consequence of keeping data at the edge will be increased risk of exfiltration or loss, damaging company reputations and leading to lost business.

Moreover, some employees who need fast access to IoT data are located elsewhere in the enterprise. In fact, 76% of organizations will be analyzing data collected as part of IoT initiatives from a more centralized location, such as a regional headquarters[7]. So the ability to quickly and securely transmit and store data in other locations where it is closer for other employees to access is critical.

Accessibility aside, most data will still need to be backed up to a data center or cloud as part of business continuity/disaster recovery practices. However, it's often cost- and time-prohibitive to send massive amounts of data to a central location—again, due to high latency and bandwidth-constrained links.

## Challenge: IoT Buyer Beware, Additional Security Risks Are Ahead

Breaches involving IoT are prominently featured in the headlines, underscored by a 600% increase in attacks between 2016 and 2017 alone. This is partially due to the fact that there are hundreds or thousands of more devices on the network, many of which lack stringent security measures. And because these devices are connected, the resulting "Internet of Threats" gives hackers new vectors to gain unauthorized access to networks and corporate data. In fact, 46% of companies have reported a breach due to new IoT devices[9].

The sheer number of IoT devices that IT must onboard to the corporate Wi-Fi poses a similar issue. Most Wi-Fi solutions today rely on captive portals, which are web pages used to register Wi-Fi users. However, these will not work with headless IoT sensors, due to their lack of user interfaces, thereby making it difficult to securely connect IoT devices.

Even if IT accounts for device-based vulnerabilities, other risks exist. For instance, IT needs to isolate IoT traffic from other parts of the network. For example, sensors on manufacturing equipment should not be able to talk to financial or HR systems that contain sensitive customer or employee data. And while network segmentation is not a new concept, quickly and reliably doing so using traditional networking tools is taxing and subject to human error.

Similar issues will crop up as organizations seek to set and enforce network or security policies around IoT. Using outdated, fragmented management tools to enforce policies governing access and usage across a hybrid network consisting of numerous modes of transport and equipment from multiple vendors will lead to increased errors, more security events, and higher risk for the business.

## Solution

While many powerful IoT platforms are emerging on the market, organizations still need to ensure reliable connectivity and accessibility to IoT-related data while offloading some of the management complexity associated with legacy infrastructure. But this should not be done with a piecemeal approach with point solutions that address these requirements in a discrete manner.

Instead, companies should seek a platform that augments their IoT initiatives—enabling them to move with greater agility and less risk—while also supporting other strategic initiatives.

Such a platform should consist of the following two components:

1. Cloud networking, which simplifies the process of building, deploying, and managing IoT networks.

2. Extensible edge computing platform, which gives IT the agility to instantly deploy and centrally manage IoT services at the edge.

## Cloud Networking

IT leaders need to displace traditional, device-centric networks to keep pace with business needs while ensuring consistent, reliable connectivity across IoT deployments. Newer technologies such as a software-defined WAN (SD-WAN) are meeting the challenge by making networks more intelligent, while mirroring the elasticity and efficiency of the cloud.

SD-WAN brings a programmatic, centralized approach to managing distributed networks. This means network configurations are made in one location through a graphical user interface, not router-by-router, which significantly boosts IT agility. It's also transport agnostic, meaning it can support virtually any connectivity type, minus the inherent complexity of setting and managing rules that dictate which network path an application should take. In essence, SD-WAN helps network managers leverage hybrid networks more effectively by automatically determining the most efficient way to route different types of traffic from location to location.

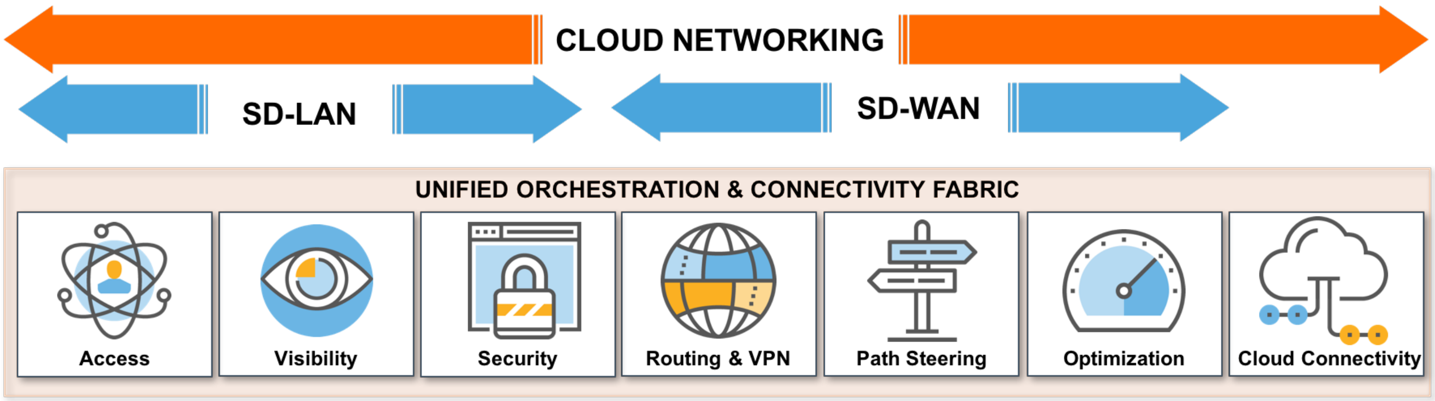
This routing intelligence helps ensure the levels of resiliency and performance IoT services require.

To be truly effective, the software-defined principles of SD-WAN must extend to the local area network (LAN)—including corporate Wi-Fi—and offer other integrated services such as network optimization and visibility. The resulting set of capabilities is defined as a cloud networking solution, and should deliver:

- **A unified network fabric:** IT should be able to manage the entire enterprise network from a single pane of glass—spanning wireless and wired LANs, WANs, and data centers—for improved efficiency. Automating connectivity to leading cloud providers such as Microsoft Azure and Amazon Web Services is also a must, given that cloud will still be strategically important to IoT deployments.

- **Centralized policy orchestration and management:** Ongoing network management should be further simplified with the ability to push out changes to policies, traffic rules, and other parameters in a few clicks, not router by router. And as IoT deployments expand to other use cases or business locations, IT teams need to be able to add sites, uplinks, and the appropriate network devices seamlessly using zero-touch provisioning, not with tedious CLI, complex scripts, or a need to dispatch skilled network engineers from site to site.

**Figure 1:** A cloud networking solution combines many capabilities that help simplify the management of IoT deployments.



- **Policy-based network segmentation:** The simplicity of setting and enforcing policies must extend to network segmentation. Dynamic, device-based policies should control access to IoT-related assets and be seamlessly applied across the network. Network zoning should also be used to securely segment IoT traffic from other apps, devices, and systems, limiting exposure and blast radiuses in the event of an attack. Establishing these policies via a graphical user interface that is characteristic of SD-WAN—instead of having to manually key them in—reduces security events that stem from operator error.

- **Scalable, high-performing Wi-Fi:** To keep up with growing IoT traffic demands, enterprise Wi-Fi networks should be architected on software-defined access points with high-density support to deliver greater bandwidth with less equipment. In this manner, when more capacity is needed on a wireless LAN, it can be deployed from the cloud to the edge with a single click.

- **Easy device onboarding and management:** A Wi-Fi onboarding workflow that eliminates the need for captive portals or web browsers is necessary to accommodate headless sensors and other IoT devices. And to ensure security, such devices need to be auto-classified by type as they connect to the network, where traffic is tagged and policies governing access are then applied at the point of connection for tighter oversight.

## Extensible Edge Computing Platform

Organizations need the flexibility to host IoT apps and data based on business objectives—not technical limitations. To that end, they need a solution that enables real-time processing of data at the edge. This need has given rise to a new computing paradigm—edge computing—which allows data to be triaged locally so it can be analyzed closer to where it is generated, reducing the backhauling of traffic to a central data center or cloud.

> Edge computing allows data to be processed and analyzed closer to where it is generated, eliminating the wait time associated with backhauling traffic through a data center or cloud.

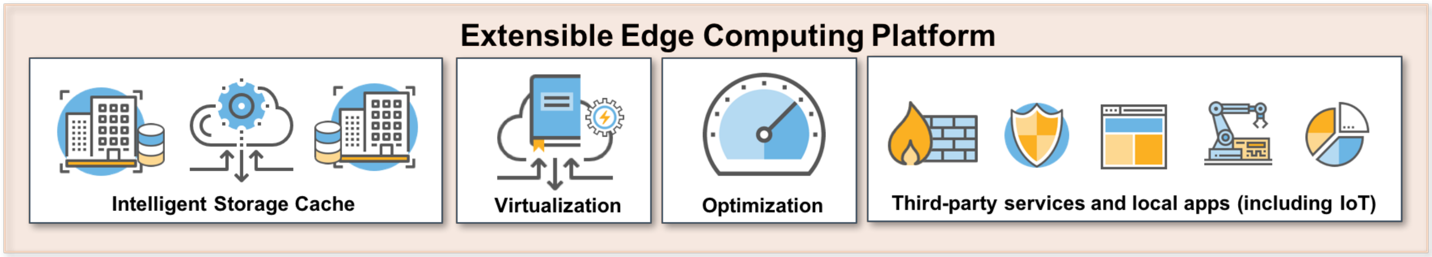
But what remains is the need to ensure data is continuously backed up and secured, while still making it available throughout other locations across the enterprise. Moreover, the edge computing solution needs to have a lean footprint to avoid excessive CapEx and OpEx, yet still be powerful enough to scale for future needs.

An extensible edge computing platform that converges server, storage, backup, and other infrastructure into a single form factor is the answer. But with many converged systems existing in the marketplace, here are some key capabilities or characteristics to consider:

- **Purpose-built for edge/IoT locations:** Many converged systems weren't designed for the edge. While hypervisors and networks are stateless functions, data is often "statefully" stored at remote locations, making it difficult to recover if an outage occurs. Moreover, while many converged systems are easy to scale and administer in a data center, that advantage doesn't extend to the edge, as each location needs its own version of the same components, requiring distributed management. So, consider a solution that eliminates this management overhead, and scales and standardizes to support all edge location types.

- **Cloud-like infrastructure provisioning:** Deploying new IoT apps or services should be as simple as spinning up new VMs or containers in the cloud. Not only does this expedite new service deployments, but IT teams become more efficient too, as, once again, it minimizes the need to send specialists to remote sites to rack and stack the necessary equipment.

**Figure 2:** The right edge computing solution brings the requisite levels of performance, agility, and security to drive IoT.


Extensible Edge Computing Platform
Intelligent Storage Cache
Virtualization
Optimization
Third-party services and local apps (including IoT)

- **Intelligent storage delivery:** Selecting a platform with the right storage delivery intelligence can give you the best of both worlds when it comes to IoT data availability and security. Data can be secured in a data center or cloud, while still being instantly available at the edge. Such an approach minimizes data footprints at the edge by projecting only the required data needed by IoT applications. Complete copies are maintained securely in the central data store, and any modifications to IoT data sets are instantly synchronized back to it. This technique should also encrypt data sitting at rest at the edge and in-flight over the enterprise WAN. A related benefit here would be improved business continuity/disaster recovery plans, as all backups are completed centrally and continuously, giving businesses far more recovery points if an IoT service suffers an outage.

- **Seamlessly run third-party functions:** Successful IoT implementations require an ecosystem of technologies. Selecting a platform that can run virtualized third-party functions—such as other networking or security services—minimizes infrastructure footprints, promoting easier management and operational simplicity.

## Conclusion

Organizations continue to embark on their digital transformation journeys, and IoT is quickly becoming the backbone. But before IoT deployments can fully mature, CIOs and other technical leaders need to do away with legacy, hardware-bound approaches to managing the underlying infrastructure that lead to poor connectivity, subpar performance, and gaps in visibility and security. This means adopting newer technologies such as SD-WAN and edge computing, where the most successful architectures will be based on consolidated platforms that tightly integrate with other parts of an IoT ecosystem. Doing so will allow IT leaders to properly address networking, data, and security vulnerabilities, helping ensure smoother IoT roll-outs and easier management of the infrastructure moving forward.

**Footnotes:**

1. Columbus, Louis, “The Era of Integrated IoT Has Arrived in the Enterprise,” Forbes, Sept. 29, 2017
2. IDC, “Worldwide Semiannual Internet of Things Spending Guide,” June 2018
3. Ganguli, Sanjit; Naegle, Robert, “I&O Leaders Must Get Involved with Current or Planned IoT Initiatives,” Gartner, March 20, 2018
4. McGillicuddy, Shamus, “Ease IoT Complexity at the Branch with SD-WAN,” EMA, Feb 18, 2018
5. Infoblox, “What Is Lurking on Your Network,” June 2018
6. ESG, “ROBO and Cloud Survey,” Prepared for Riverbed, Dec. 2017
7. Gartner, “Shift Cybersecurity Investment to Detection and Response,” Jan. 7, 2016
8. Altman Vilandrie & Company, “Are your company’s IoT devices secure?” June 2017

### About Riverbed

Riverbed®, The Digital Performance Company™, enables organizations to maximize digital performance across every aspect of their business, allowing customers to rethink possible. Riverbed’s unified and integrated Digital Performance Platform™ brings together a powerful combination of Digital Experience, Cloud Networking and Cloud Edge solutions that provides a modern IT architecture for the digital enterprise, delivering new levels of operational agility and dramatically accelerating business performance and outcomes. At more than $1 billion in annual revenue, Riverbed’s 30,000+ customers include 98% of the Fortune 100 and 100% of the Forbes Global 100. Learn more at riverbed.com.