Raritan®
A brand of legrand®

The New Digital Outpost

Why We Must Rethink Remote Infrastructure

A White Paper from Raritan

Introduction

IT has always supported computing at remote sites. But business-critical digital activity at remote sites is rapidly intensifying due to multiple factors that include pervasive mobility, Internet of Things (IoT), and real-time analytics. IT must therefore proactively rethink its approach to remote infrastructure in order to enable critical digital activity and to ensure that it continues uninterrupted — while at the same time driving cost out of remote site ownership.

The New Digital Outpost

Remote computing is changing dramatically. Mobility, IoT, wireless connectivity, small-footprint software, and other technologies continue to drive digital activity everywhere. As a result, remote computing environments keep getting denser, more sophisticated, and more critical to the business.

Retailers, for example, now worry about more than just POS (point of sale) systems. They're also delivering rich mobile experience to shoppers as they walk the aisles and maintaining smarter inventory management systems. Some are achieving high sell-through by doing real-time analytics on-site.

Healthcare providers are experiencing similarly intensifying remote compute activities as their clinical systems become increasingly digital; and, as they deliver care across larger, more dispersed networks of hospitals, clinics, and specialty practices.

Added to these vertical-specific issues is the fact that buildings themselves are getting smarter and more connected. So every business depends on an increasingly intense remote computing environment to minimize its facilities costs while maintaining a safe, comfortable workplace.

So no matter what business you're in, remote computing no longer serves merely as a utility that supports your geographically dispersed facilities. Those facilities are now as digital as they are physical. They have become your company's New Digital Outposts (NDO). This requires significant rethinking and reengineering by IT. Remote computing is no longer about just sticking a server and a router in a supply closet. The New Digital Outpost requires an entirely new approach to provisioning that fulfills more demanding requirements for performance, availability, and total cost of ownership for remote computing.

55

The average number of branches served by enterprise data centers.

Source: IDC

IT must respond appropriately to this remote computing inflection point. Failure to do so will undermine digital performance — and, by extension, the financial performance — of the business.

Provisioning the New Digital Outpost

The changes taking place in remote computing require IT to rethink NDO provisioning in six specific ways:

IMPERATIVE #1:
High-Performance, High-Density Compute/Storage/Networking

As more data is processed in more ways at remote sites, remote infrastructure will have to evolve accordingly. And, because most remote sites don't have an abundance of spare square footage, the form factor for this high-performance infrastructure will have to be diligently minimized.

The cloud will not ameliorate these local/on-site IT requirements. Data still has to be staged — and, in some cases, analyzed — locally. Video streams and motion tracking, in particular, will drive intensified requirements for on-site infrastructure for applications such as distribution/fulfillment, retail, facilities security and VR/entertainment.

In fact, the cloud can actually increase on-site infrastructure requirements by increasing the number of applications, services, and data sources remote employees, customers, and others will want and need to access at any given time.

IMPERATIVE #2:
Protection from Environmental Variables

Businesses make significant investments in the physical infrastructure of their central data center environments to ensure that their primary IT facilities are kept at the right temperature and humidity, receive a consistent flow of power regardless of fluctuation in the local grid, and are shielded from potentially harmful forces like vibration and electromagnetic interference.

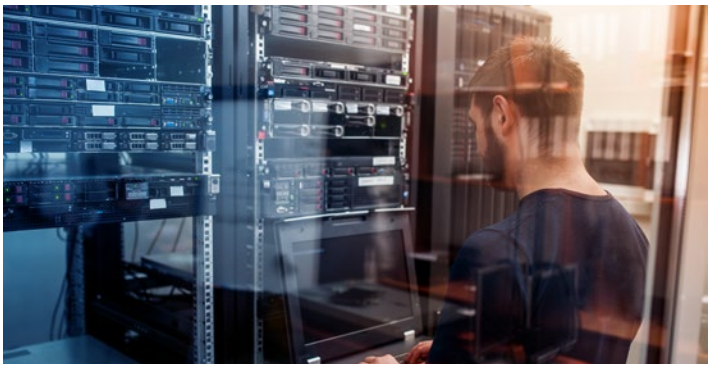
75%

Three-quarters of companies will still run their critical applications locally on remote office IT infrastructure in 2020, rather than SaaS/cloud.

Source: ESG

Remote IT infrastructure requires this same level of protection. In fact, because businesses often lease or rent their remote locations, NDOs may need to be even more aggressively protected from the dangers that occur due to the negligence of and/or the accidents that befall property owners and neighboring tenants. No one, after all, wants to lose revenue or jeopardize their regulatory compliance because a sink upstairs is overflowing or someone forgot to service an AC unit.

IT must, therefore, devise a new, more rigorous approach to the housing and physical protection of NDO infrastructure.



IMPERATIVE #3:
Right-Sized Form Factors

Businesses don't have an unlimited amount of floor space at their remote locations. In fact, despite the ever-increasing importance of digital technology, those locations are often chosen and laid out without sufficient advance consideration of IT infrastructure requirements — including compute, storage, network, power management, cooling, etc.

One of the keys to successful NDO provisioning is a tight, efficient form factor that consumes as little space as possible. In fact, in many cases, it will make most sense to mount an equipment enclosure behind a drop ceiling or up high on a wall. This type of setup serves the dual purpose of not consuming limited floor space and in keeping NDO equipment out of harm's way.

IMPERATIVE #4:
Remote Serviceability

Because remote locations typically lack on-site technical staff — and because sending technical staff out to those locations is so costly and disruptive — businesses must obviously be able to service their NDOs from a central location as much as possible. Historically, most IT organizations have only thought about remote serviceability in terms of basic management capabilities such as system status alerts, soft reboots, and software/OS patching. But as NDO infrastructure increases in density, sophistication, and criticality to the business, remote management capabilities must increase as well. These capabilities may include full remote KVM

sessions, hard reboot, temperature threshold alerting, and more. NDO enclosures should also make it as easy as possible for non-technical personnel on-site to perform basic tasks such as swapping out server blades and power supplies.

IMPERATIVE #5:
Security and Compliance

Businesses are going to great lengths to mitigate their vulnerability from all kinds of cyberattacks — from sophisticated penetration of perimeter defenses to simple, yet clever, spear-phishing exploits. Yet, these same businesses often fail to take the most rudimentary measures to protect the physical security of their IT infrastructure. As a result, those with malicious intent — including insiders with a grievance — can steal data or disable systems via direct access to servers or storage media.

This is especially true in remote offices, where IT equipment often sits in spaces that don't require a special pass or lock code. NDO provisioning, therefore, requires a much higher level of physical security.

This security may be a compliance issue as well. Regulatory auditors rightfully expect businesses to demonstrate that appropriate precautions have been taken to keep unauthorized persons from accessing PII, medical data, and the like. Businesses that don't diligently lockdown NDO infrastructure may thus expose themselves to a cybersecurity audit failure.

IMPERATIVE #6:
Streamlined Provisioning

Some businesses have a very large number of NDOs. Some have a smaller number, but they are dispersed across a very large geographic area. Others have very tight timelines for getting their new NDOs up and running. And all businesses need to keep the cost of NDO provisioning under control.

For these reasons and others, the NDO provisioning process is as important as the end result. A consistent, streamlined process for specifying the appropriate provisioning for each NDO, procuring the right NDO equipment, deploying that NDO equipment, and then validating the end result is essential. Without an efficient, repeatable process, NDO provisioning will be too slow, too costly, and too prone to error.

The above six imperatives are just that: imperatives. Whether you're running a county-wide school system, a multi-national casual dining chain or a multimedia enterprise with local hubs, operational excellence depends on reliable remote IT. So you must fulfill the six foundational requirements of a best-practices NDO provisioning.

Six Imperatives Around the New Digital Outpost

1. **High Performance, High Density Compute/ Storage/Networking**
2. **Protection from Environmental Variables**
3. **Right-Sized Form Factors**
4. **Remote Serviceability**
5. **Security and Compliance**
6. **Streamlined Provisioning**

Meeting the New Digital Outpost Challenge

Given the above NDO imperatives, how can IT best provision remote IT infrastructure? What new steps should IT take in response to new requirements for reliable, cost-efficient digital business activity across multiple geographically dispersed locations?

Businesses are meeting the NDO challenge with proven remote management solutions — such as KVM switches, intelligent power and sensor monitoring solutions, and DCIM (data center infrastructure management) software. These solutions provide visibility to distributed infrastructures from anywhere, early alerts to potential issues with suggestions on how to remedy, and secure remote access to IT equipment and the supporting infrastructure.

Many of these popular remote infrastructure management capabilities are now being integrated into prefabricated micro data centers — which are gaining interest because they address the NDO challenge in three important ways:

Data center-like environments for remote locations. A well-engineered prefab unit provides a ready-made environment for remote IT equipment that closely mimics what exists in the main enterprise data center: cooling, conditioned power, protection from external damage, restricted physical access, etc.

Features and form factor tailor made for the NDO. At the same time as they mimic the data center in multiple important ways, prefab units also address the distinctive requirements of remote locations with limited space and little or no on-site tech staff. So they can be readily mounted where they're safe and out of the way — and managed remotely with minimal hands-on skills required.

Standardization/repeatability. Some businesses standardize their remote locations to the point that they can use one identical prefab design everywhere. Others need a small number of different standard designs to accommodate multiple types of remote location (regional distribution, local outlet, etc.). Either way, prefab units eliminate the need for IT to "re-invent the wheel" for every remote location.

The use of prefab units has been somewhat limited in the past because remote computing requirements were not sufficiently intense to warrant them. The selection of prefab units available to enterprise IT was fairly limited for much the same reason: inadequate market demand.

But as remote computing passes its present inflection point in terms of intensifying technical requirements and growing business value, the benefits of remote management solutions — and micro data centers — have become extremely compelling. These benefits include:

- Uninterrupted revenue
- Better, more consistent customer experiences
- Faster, easier launch of new locations
- Lower IT costs
- Reduced strain on and better allocation of limited IT staff
- Mitigated operational, security, and compliance risk
- Improved uptime and MTTR (mean time to repair)
- Preparedness for an even more digitally intense future

No business should keep provisioning its remote locations in 2017 like it did in 2007. NDOs demand a smarter strategy. Micro data centers and intelligent remote management solutions can play a central role in that strategy — significantly enhancing the performance of any business that must support more digital activity across more locations.

Intelligent Cabinet Prototype

Together with Legrand's Data Communications Division, Raritan created an Intelligent Cabinet prototype that leverages the company's data center expertise in cabinet housing of all sizes, intelligent power distribution, power and environmental monitoring, DCIM software, cabling, networking, and remote "lights-out" data center management.

A patent-pending embedded controller provides intelligence to the Raritan/Legrand Intelligent Cabinet. The cabinet has its own IP address, and both a remote and cabinet-door touchscreen interface for managing all tasks — including security authentication and door-lock release, tracking IT and infrastructure assets in the cabinet, and providing updates on the environment's health, energy usage, and potential issues. The cabinet's open architecture supports many more features and capabilities to support the needs of remote sites.

The cabinet's capabilities are ideally suited for NDO scenarios. For example, if there is a hot spot near the cabinet, the cabinet's environmental sensors alert IT staff and trigger the LED outside the cabinet to turn red. And if there is a security breach, the cabinet's cameras capture images of the intruder and send them to IT security staff.

About Raritan

Raritan began developing KVM switches for IT professionals to manage servers remotely in 1985. Today, as a brand of Legrand, we are a leading provider of intelligent rack PDUs. Our solutions increase the reliability and intelligence of data centers in 9 of the top 10 Fortune 500 technology companies. Learn more at Raritan.com