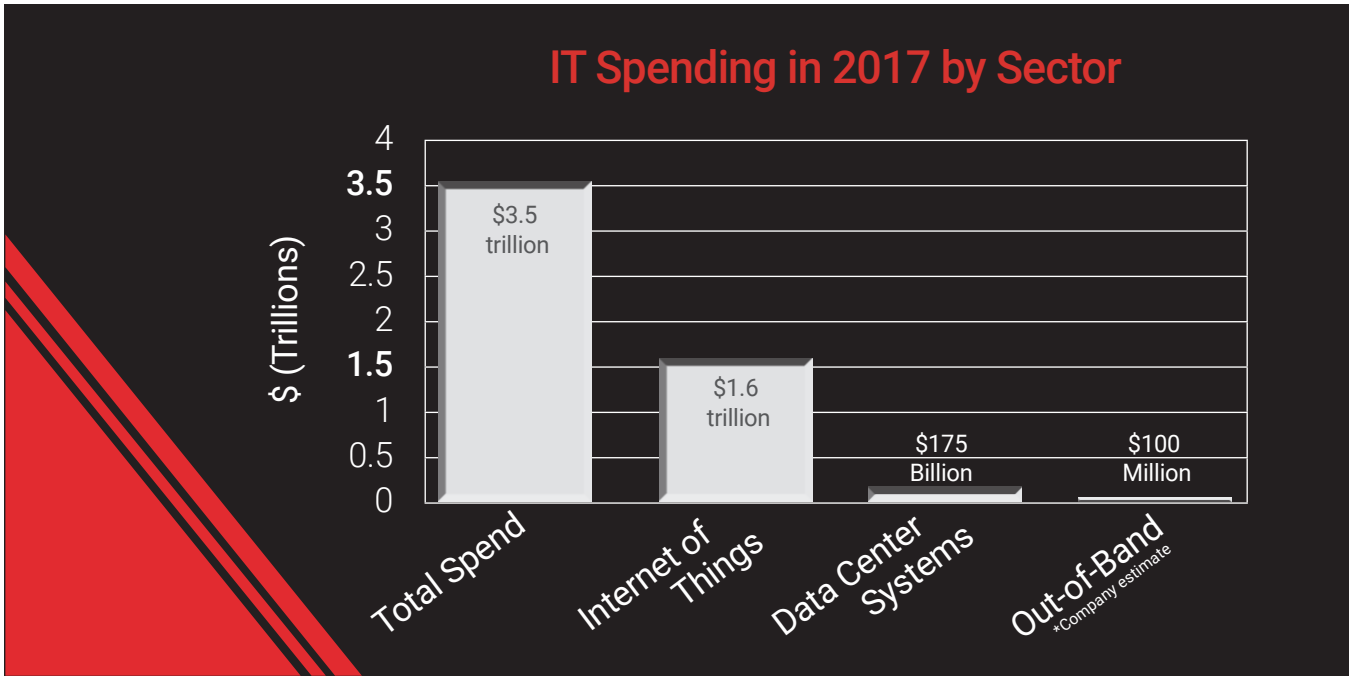
opengear

HOW RESILIENT IS YOUR DATA CENTER?

Considering Out-of-Band Management for 24/7 Access

Does 24/7 Really Mean 24/7?

The reliability of the data center is critical for a business to function. As companies become more dynamic and intelligent they rely on critical software to increase productivity, make better decisions and have accurate reporting. Thus, companies are expected to spend $3.5 trillion dollars in 2017[1] to maintain and upgrade their IT infrastructure and systems.



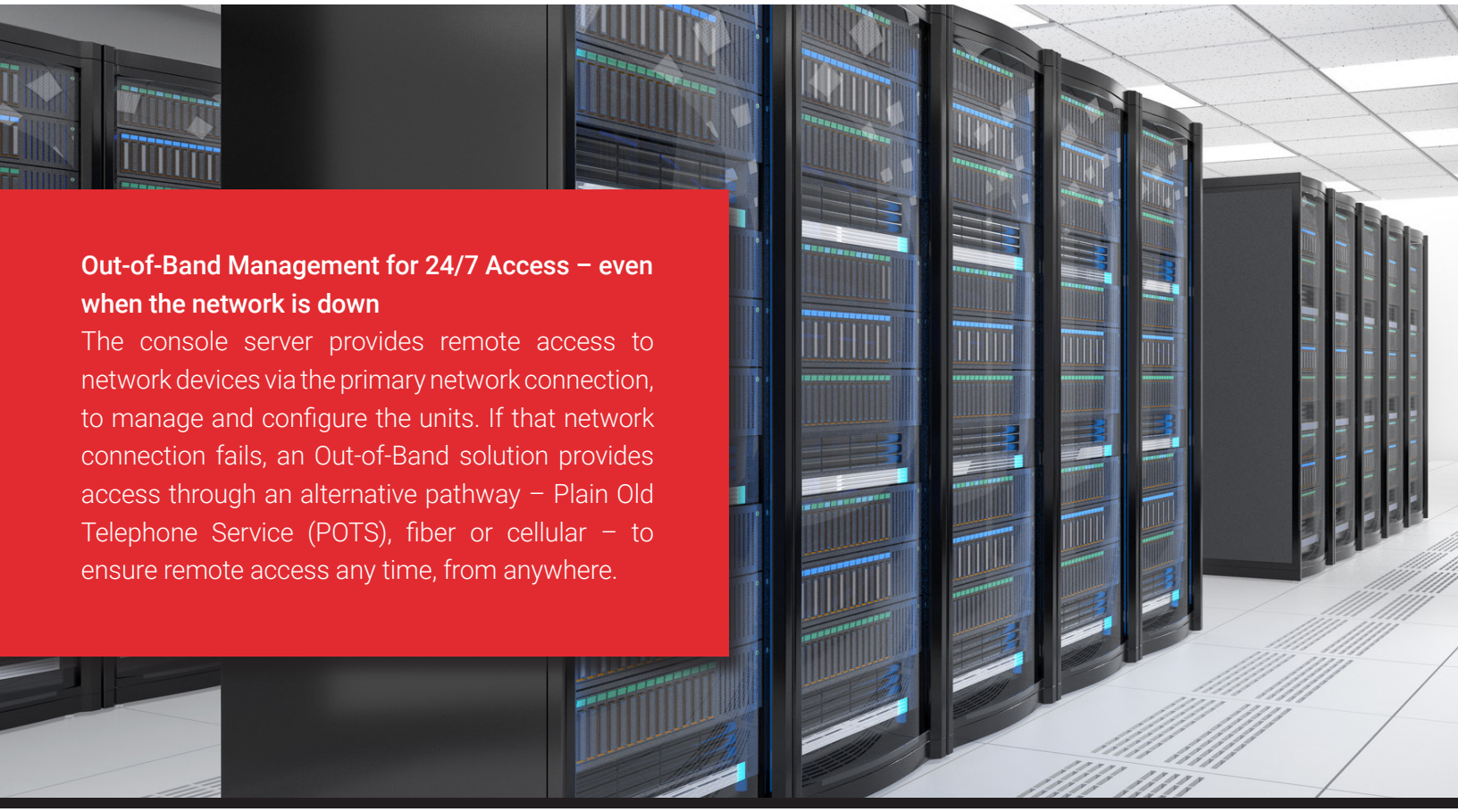
Gartner[1]

Networks are also becoming more complex, as previously all data was hosted at a corporate location but now it may be hosted at multiple centers and accessed via the cloud. With an estimated 3.2 billion[2] connected devices in business applications as part of the Internet of Things (IoT), remote sites are now more fully integrated into the IT infrastructure, putting additional demand on the data center and the need for 100% uptime and reliability.

New devices are being added to the infrastructure and older devices replaced with newer and faster features and technology. For example, a 1 gigabit backbone was sufficient for data centers two decades ago. The minimum standard has now become 10 gigabit with some 40/100 Gb solutions now in place. Even most homes are already utilizing a 1 Gb solution. More information is being transferred through the data center, all of which is critical for business function.

As your business becomes increasingly dependent on these systems, you also need a reliable network to ensure maximum uptime. For example, your accounting team needs access to ERP (Enterprise Resource Planning) to know which vendor bills are coming due. If the network at the data center fails, they will not be able to perform their duties, leading to a backlog of work and failing to pay vendors on time which could damage relationships. Similarly, your sales team needs data from the CRM (Customer Relationship Management) to reach out to their next prospect. Without access to this key contact information, your sales people cannot sell and revenues could be impacted.

Every division and every process in your company demands 24/7 access to their data and computational power, so it's critical that the uptime of the data center is close to 100%. Any downtime can impact the company financially and in some instances hurt customer perception or damage vendor relationships. In addition to building and maintaining a reliable data center, your IT infrastructure is constantly expanding with new site deployments or through acquisitions. That means more devices, more users and more data packets moving.



Out-of-Band Management for 24/7 Access – even when the network is down

The console server provides remote access to network devices via the primary network connection, to manage and configure the units. If that network connection fails, an Out-of-Band solution provides access through an alternative pathway – Plain Old Telephone Service (POTS), fiber or cellular – to ensure remote access any time, from anywhere.

Keeping the Network Running

Network administrators strive to build redundant networks with failovers to minimize outages. While redundancy is important, no network is 100% reliable and failure can and will occur. Out-of-Band management (OOB) is the data center's insurance policy to minimize the impact of these failures and provide access at those moments. Yet in many instances, the primary focus is on the actual infrastructure, while very little is done on the out-of-band solution.

As a result, network administrators need better tools to access infrastructure. The evolution from simple console servers (providing local access) to units providing out-of-band management (access everywhere and anywhere) is critical during those failures. Using OOB, they have a dedicated network pathway even when the rest of the network is down. The types of out-of-band connections could range from fiber connectivity, to built-in POTS or cellular modems, and as the solution has evolved, network administrators have better accessibility when they are remote. Even if the network administrator is away on vacation, the ability of "Remote hands" is invaluable and eliminates the need of having someone on site 24/7.

In addition, to offering different pathways for OOB management, the hardware has become more intelligent, faster and secure. Console connectivity provides a large amount of information and control over the end device, and because of this information, many solutions can preemptively resolve problems based on certain conditions. Newer platforms also house faster processors and larger memory which are critical to obtain new enhancements to security and encryption. Without updating the security, an out-of-band device could be exploited by hackers.

OUT-OF-BAND ACCESS IS CRITICAL DURING FAILURES

While the importance of out-of-band is clear, it is only a tiny percentage of the overall spend, as it accounts for around $100 million out of the $3.5 trillion total IT budget. Instead network administrators continue using existing solutions in place that may utilize legacy technology. These legacy solutions can be close to end of life and be a security risk with lack of vendor support, bugs or unaddressed security loopholes. By not reevaluating their OOB solution, network administrators are failing to take advantage of new technologies and features that can minimize downtime, increase security, simplify management and save costs.

VIDEO: Smart Out-of-Band Management Explained

Why Implement a New Out-of-Band Solution?

1. Improved network MTBF and MTTR
2. Stronger network security and compliance
3. Reduction in costly operational downtime
4. Increased standardization and efficiency through automation tools

What to Look for in an Out-of-Band Solution

An out-of-band solution needs to be simple and reliable. When the network goes down, the device needs to be ready to provide an alternate pathway via a console server, to reach the IT infrastructure and determine what is wrong and resolve the issue. While this still holds true today, new features are available to reduce costs, simplify management and reduce downtime.

Secure OOB solutions are feature-rich, and incorporate many functions that save companies time and money. In earlier iterations, a failure would occur and the network administrators would login and try to determine the issue. We can call this *manual* out-of-band. Today's solutions are more intelligent, with condition based functions that can automate the recovery before a network admin needs to step in.

TODAY'S SOLUTIONS ARE MORE INTELLIGENT AND AUTOMATED

Upgraded Hardware

By implementing newer hardware, it extends the life cycle of the device. Security implementations are very resource dependent so choosing a solution with the maximum amount of processing power and memory is critical in futureproofing the infrastructure. This also enables the device to work faster and eliminates delays in reporting issues to the network administrators.

Embedded Solutions vs Add-ons

Selecting a complete solution with embedded features means that the device is tested as one unit. One such feature that exists now is using cellular communication for OOB.

Does Java Keep You Up At Night?

If the current solution is running some type of web interface that utilizes Java, the network could be exposed to potential security risks. A plethora of articles by security experts[3] have all pointed out that Java is one of the biggest vulnerabilities of computer systems today. While Java has been pushing ahead with security releases and patches, many of these implementations could break functionality in the remote terminal servers if the manufacturer does not continuously keep up with updates. Even if an update is available, the firmware may need validation before being deployed into production. During this period, the company is at risk of someone exploiting the issue or deploying untested firmware that could bring down the system. For devices that are end of life, that update or fix may never come.

Companies are looking to move away from POTS due to its limited availability and high cost. Many vendors now offer a cellular solution instead, using add-on modems in partnership with cellular vendors to be sold as a "complete solution". This can result in a complex implementation with additional risk of failures beyond just the basic box. If an issue were to occur, it can also be difficult to find a resolution between the two vendors.

Automation

Automated provisioning is a critical feature for enterprise customers looking to quickly and efficiently deploy many devices, and this should also extend to the OOB devices being put in to production. By using automation, it reduces time to deployment and minimizes errors that could cause problems later, but unfortunately, these tools have not reached a level of standardization. Companies need to find solutions that are adaptable and can be reconfigured depending on requirements. This same flexibility is necessary in the provisioning of OOB devices so they can either fit into existing deployments or be adapted at a time when deployment processes are changed.

Unified power management of UPS and PDU

Implementations in the data center will also need to manage the power systems in place. The out-of-band solution should have a wide range of support from various vendors. Authorized users have secure outlet control to power on, power off, and power cycle at the managed device level. Power metering and temperature monitoring are coupled with logging and alerts. And with auto-response, power issues can be automatically detected and remediated — before they become problems. Consolidating this management into OOB makes sense as adding another system/device complicates the network administrator's job.

CASE STUDY: Learn how IPSec protects their customers' infrastructure with Opengear console servers.

50% of Mission-critical service outages[4] are caused by issues related to process complexity:

- Complex network environments
- Administration of individual devices
- Changes and release of new configurations
- Handoff between administrators

Making 24/7 Access A Reality

As networks grow larger and more complex, the data center infrastructure needs to be more resilient and adaptable to these environments. The out-of-band solution that connects to this network infrastructure also needs to evolve. Legacy solutions no longer provide enough functionality in today's environment and could cause unnecessary network downtime.

The out-of-band management system supporting your data center needs to be just as advanced as the infrastructure it's connected with. These advanced features include multiple pathways for out-of-band access, fewer embedded elements that pose a security risk, easier deployment methods offering more control over your end devices, and the ability to proactively detect faults to minimize downtime. While out-of-band is only a small piece of the IT budget, it provides an invaluable return on investment during infrastructure failures.

Don't let out-of-date out-of-band be the weak link in your network resilience.

CLICK HERE
and contact Opengear for a free demo today

opengear

www.opengear.com

Further Reading

» **CASE STUDY:** Learn how Secura Hosting achieved ROI on their out-of-band investment.

» **VIDEO:** See our IM7200 Infrastructure Manager product overview.

» **PRODUCT:** Find the right Opengear product for your needs with the online Selector tool.

REFERENCES
(1) Gartner Worldwide IT Spending Forecast, (2) Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017,
(3) Krebs on Security, "Good Riddance to Oracle's Java Plugin", (4) Gartner RAS Core Research Note, Ronni J. Colville, George Spafford, 2015