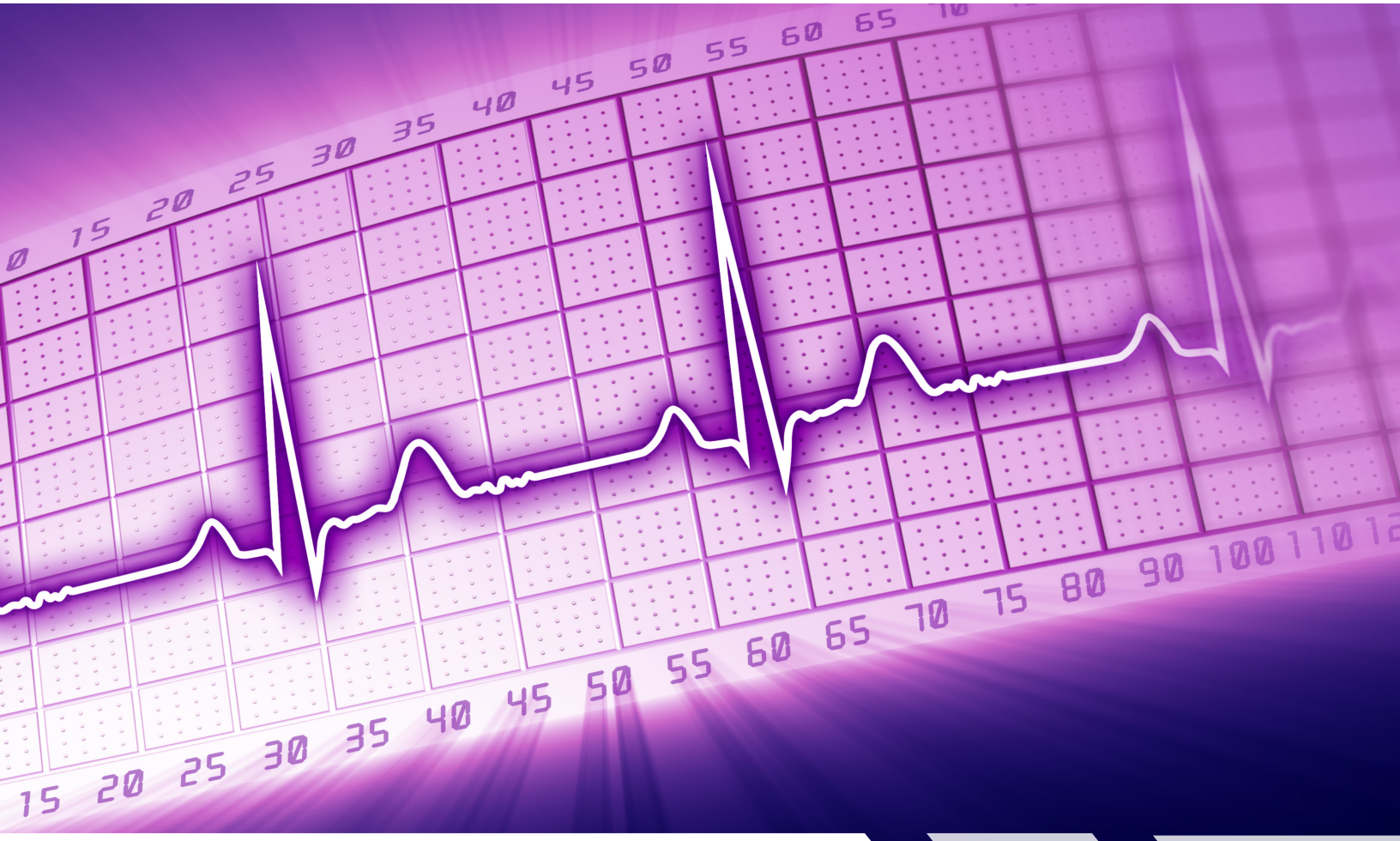
opengear



WHITE PAPER

# Healthcare Network Resilience: When failure isn't an option

Network resilience is a critical consideration for healthcare IT infrastructure. Reliable and secure network connectivity significantly impacts patient safety and clinician productivity. As healthcare organizations strive to provide better patient experiences, networks integrate new technology into their systems. Cloud services, Bring Your own Device (BYoD), IoT tools, network merges, and IT advances are continually added to these environments, causing greater strain and more points of failure which increases the likelihood of disruptions.

Healthcare organizations often run on restricted budgets and legacy systems that are more expensive to run and less efficient. At the same time, cloud services, Bring Your own Device (BYoD), Internet of Things (IoT) devices, network merges, and IT advances are continually expanding these environments. Visibility, remote management, and automation are vital to keep things running smoothly.

The effects of network downtime can be catastrophic, not only to operational and financial performance, but also to the reputation of the brand. This paper takes a look at the special challenges of healthcare networks and ways to maintain these networks with shorter Mean Time to Repair, Out-of-Band [OOB] management, failover solutions, and true resilience.

## THE VALUE OF A RELIABLE NETWORK

Three of the biggest challenges facing healthcare networks are cybersecurity, the consolidation of networks, and unintentional downtime caused by things like user error, weather, or accidental line cuts. If neglected, these challenges can severely damage networks and cost a significant amount of time and money to address.

*Cybersecurity*
Healthcare is a huge target for hackers and is one of the top two industries breached[1]. And a breach is costly, with the average cost of a healthcare data breach at more than $715,000[2]. Ransomware attacks are increasing, causing a growing number of healthcare enterprises to shut down computer systems, including their Electronic Health Records (EHR). For example, Hollywood Presbyterian Medical Center's EHR system was down for more than a week. With ransomware attacks on hospitals increasing, and hackers increasingly targeting hospitals, network resilience is essential.

*Consolidating networks*
Another issue that healthcare organizations have to deal with is the acquisition of smaller organizations and their integration into the parent networks. Even within an existing network there is likely to be a wide variety of hardware and software. For example, 40% of healthcare deployments use over 20 different operating systems[3].

*Unexpected outages*
There is no way to predict when a random outage might happen. The best option is to anticipate the possibility, but many healthcare networks neglect to adequately plan ahead. In fact, one third of hospitals don't have a HIPPA compliant EHR contingency plan in place[4]. When a single healthcare network outage costs $8900 per minute in lost revenue and productivity[5], it's vital that health organizations plan for outages.

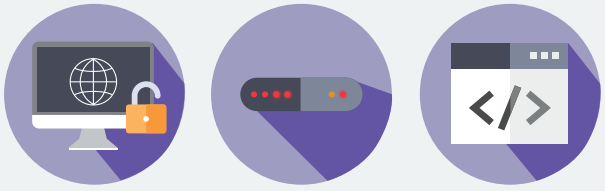
## WHAT IS OUT-OF-BAND AND *SMART* OUT-OF-BAND?

The term Out-of-Band or OOB refers to a network strategy that provides an alternative path to devices located at remote sites when the primary network is down. OOB management gives network administrators a way to securely monitor, access and manage devices without impacting normal operations. OOB solutions can integrate seamlessly with existing IT network and management systems. They minimize network disruptions with an always-on connection.

*Smart* Out-of-Band (*Smart* OOB™) builds on traditional OOB and adds automated intelligence. Architected to exceed the demands of IT and IoT resilience, highly scalable *Smart* OOB can manage the infrastructure of hundreds of sites and thousands of devices. It protects business continuity at the hardware layer. This approach enables advanced capabilities for automatic responses and repair allowing organizations to detect faults before they become failures. Advanced troubleshooting and remediation at the network's edge allows organizations to reduce operating costs and minimize downtime, all from one centralized console.

***Smart* OOB can:**
- Detect and remediate issues automatically
- Operate independently from in-band network
- Send automated alerts via email or SMS to notify of any network issues
- Identify any inconsistencies or unusual activity with temperature conditions, cage door positions and network availability

## WHAT CAUSES OUTAGES?




System outages can result from cyberattacks, hardware failure, natural disasters, construction or vehicle accidents, human error, or any number of environmental conditions.

A wide range of network elements can also cause outages. Cable interconnects, power supplies, switches, dense compute chassis, storage arrays, and even air conditioning are potential sources of problems. And network devices are only increasing in complexity, with software stacks that are frequently updated and susceptible to bugs, exploits, and cyberattacks.

As health systems are increasingly tied together digitally, greater strain on the network increases the chance of a disruption. To meet demands, they must be prepared for current connectivity requirements and have the ability to scale as new applications come online.

*IoT devices*
The Internet of Things is rapidly emerging and bringing many new connected endpoints into healthcare networks. In addition to PCs, smartphones, and tablets, networks may include wearable gadgets and sensors that generate new types of data. The International Telecommunication Union has defined IoT as the "global infrastructure for the information society," and organizations are deploying the equipment and data centers needed to support these IoT initiatives. As IT projects scale and evolve with IoT, the IT infrastructure must be able to support an increasing variety of endpoints, applications, and services.

*Connectivity at the edge*
Hospitals have multipoint connectivity requirements. The epicenter of a variety of facilities such as labs, clinics, telemedicine hubs, and pharmacies may require a high capacity SD-WAN with multipoint connections in geographically distributed areas. And EHR and Picture Archiving and Communications Systems (PACS) are bandwidth-intensive applications that add additional strain to the network.

This new flexibility brings with it a heightened need for remote hands to manage the on-site devices. With the increased sophistication of the SD-WAN hardware – specifically the advanced routers located at each site – the need for "always-on" access to that hardware is more critical than ever. In many locations, the level of technical ability will be limited, so when an issue occurs the network team must be able to manage the equipment remotely.

When leveraging an SD-WAN network, healthcare organizations are more likely to experience a disruption because of a single point of failure at the router. Cloud services and SD-WAN are becoming core parts of many healthcare networks. And while connectivity has improved over the past few years, one weakness these technologies don't overcome is the last mile problem. The last mile is the final segment of the WAN network that connects a branch, data centers, telemedicine hubs, and IoT data to SD-WAN and cloud services. These last miles are the weakest links in a network's connectivity.

All of the network traffic for a single data center or branch may be funneled through single links. The bandwidth of these links effectively limits the amount of data that can be transmitted to an ISP. This bottleneck can leave the network exposed to DoS attacks or basic human error leading to outages. And this last mile can even be vulnerable to physical threats. An accidental fiber cut can knock out the entire network and leave it in the dark for a significant period of time.

## TELEHEALTH WITH IOT NEEDS OOB

A relatively new tool in health care, telehealth uses telecommunications technologies to deliver virtual health care and health education.

With the telehealth industry continuing to grow, it's only a matter of time before every major health care company incorporates telehealth. Telehealth revenue is predicted to reach $3.5 billion by 2022[6] and 86% of organizations that have not yet adopted telehealth say that it's of medium or high priority.

**Three big tech trends are involved with telehealth:**

**Reliance on mobile devices**
Telehealth needs a robust digital infrastructure and leverages Bring Your Own Device opportunities. Providers and patients use their own digital device to access telemedicine apps that offer virtual doctors' visits and remote patient monitoring.

**IoT tools**
Healthcare networks are beginning to use IoT devices connected to the internet, including wearable technology used to monitor and treat patients and collect valuable data.

**Cybersecurity**
With so many connected digital devices, healthcare organizations have to be concerned with cybersecurity. It's vital to monitor telehealth systems for unusual activity, back up sensitive information, encrypt confidential records, and establish protocols for retrieving lost data and restarting systems in an outage.

## SOLUTIONS TO HEALTHCARE NETWORK CHALLENGES

Opengear offers a new generation of remote management solutions to meet the growing necessities of always-on connectivity and resilience. These tools can help address each of the primary healthcare network challenges, by offering a seperate secure management network to access, monitor and remediate all IT locations from a single point.

*Cybersecurity*
For healthcare, ransomware cyberattacks and unencrypted data are the largest threats to network security. Opengear solutions provide enterprise grade security for edge and core networks with advanced security and encryption features built-in to each device. And Lighthouse Centralized Management gives organizations full visibility into their network to detect faults before they become failures.

*Consolidating networks*
The Secure NetOps Provisioning module from Opengear enables healthcare providers to ship equipment to a new, remote site and provision it without the need of highly skilled engineers. Remote deployment can help smooth the way for these transitions and limit the time and expense of needing technicians on hand for deployment and maintenance.

Once networks are connected, a centralized management system such as Lighthouse allows healthcare providers to manage hundreds of devices at various locations and have full visibility through a single pane of glass.

*Unexpected outages*
When an outage occurs, a network can failover automatically to an alternative cellular interface to connect to the main site during an outage and manage the equipment for troubleshooting. And with Failover to Cellular™ (F2C), critical applications can still run using the router bandwidth while network problems are remotely remediated, resulting in vital business operations remaining uninterupted when the primary internet connection is down.

*IoT devices and edge networks*
Smart network management solutions give IT admins the ability to use robust and always-available LTE connections to remotely manage and oversee switches, routers and other endpoints. Even a small group of IT admins can ensure that any number of mission-critical endpoints, no matter where they're located, are working well at all times. By pairing IoT with *Smart* OOB management, organizations can rest assured that the network at the heart of their operations will function properly and that problems can be quickly identified and easily resolved.

## CASE STUDY

One of the largest voluntary healthcare non-profits in the United States needed a solution to replace POTS lines and modems. Dedicated to funding research, finding cures, and enabling access to treatments for patients, the organization had 75 offices across the country that required network connectivity. POTS lines were an expensive and inconsistent solution and they continually experienced challenges. Issues with multiple local carriers and moving to new locations led to billing issues and resulted in lines being shut off or unplugged.

**The solution had to meet several criteria:**
- Enable the easy setup of new network connections
- Provide a replacement to POTS lines
- Ensure compatibility with current equipment and providers

The healthcare organization chose Opengear for each remote site. With the Resilience Gateway, they are now able to use Smart Out-of-Band (Smart OOB™) and Failover to Cellular™ to ensure networks are online, even during primary connection failures. Having many locations, technicians are able to save time during set up and to remotely access all network equipment if an issue does occur. The equipment is able to be used with their current cellular provider, Verizon, and with current network equipment from Cisco.

**The healthcare organization has:**
- Reduced costs by eliminating $50 fee per line, per month without POTS lines
- Enabled easy set up by pairing with previous vendors Cisco and Verizon
- Ensured resilient connectivity for new network connections remotely

## CONCLUSION

Healthcare networks need Out-of-Band for true resilience. Whether it's a network at a large hospital or smaller medical group, using remote, out-of-band (OOB) management products from Opengear allows administrators new freedom and flexibility. They can monitor and manage IT infrastructure, spread across multiple locations, from anywhere via a cellular network connection so all locations—hospitals, clinics, labs, data centers, telehealth hub, and other facilities—are covered. And this scalable solution grows as they are added to the healthcare network.

Failover to Cellular™ is dramatically less expensive and more reliable than POTS for remote dial-up access. And with Opengear *Smart* OOB™, IT support staff can monitor, manage and remediate IT issues across locations via a single interface – keeping critical systems functional even during a network outage. Opengear console servers at each medical facility provide powerful remote OOB capabilities that help proactively address issues to improve uptime and reduce the duration of downtime during failures.

1. https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/
2. https://netdiligence.com/portfolio/cyber-claims-study/
3. https://healthitsecurity.com/news/majority-of-medical-devices-are-running-on-legacy-systems
4. https://www.hipaajournal.com/third-of-hospitals-lack-hipaa-compliant-ehr-contingency-plans-3522/
5. https://www.ponemon.org/blog/2016-cost-of-data-center-outages
6. https://intouchhealth.com/what-to-expect-from-telehealth-in-2019/