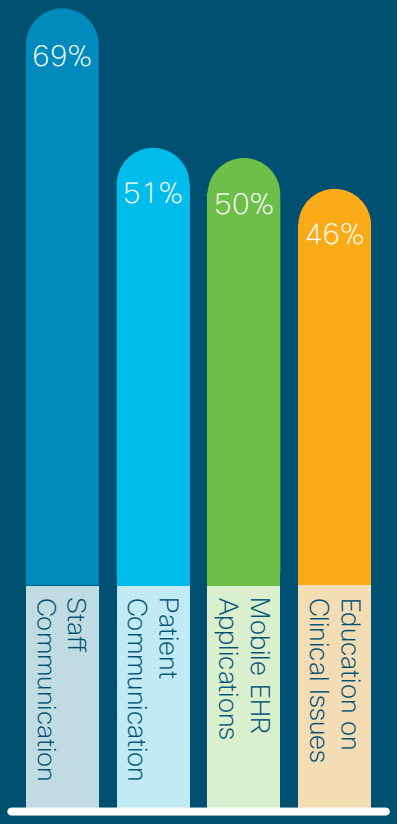
White paper

Putting Data at the Center of Care

Data center strategies for modern healthcare organizations

1. Healthcare, applications, and the data center
2. What healthcare needs to know about moving to the cloud
3. Zero-trust: Delivering the right data to the right person
4. Cybersecurity from the data center out

How are healthcare organizations using apps?[1]



Healthcare, applications, and the data center

Making IT work in a business that works fast

> "The EHR (electronic health record) is lagging again."
>
> "Why doesn't this new mobile telehealth solution work properly?"
>
> "We need to develop a custom-branded hospital app. Can we do that quickly and securely?"

Sound familiar?

Patient care moves quickly. Often unpredictable and usually time-sensitive, the business of human health demands IT solutions that are fast, efficient, and effective.

In our increasingly software-centric world, the applications running on your infrastructure are the stars of your healthcare organization. They help you collect and transfer health data, manage schedules, communicate with patients and colleagues, and so much more. And while digital solutions have brought a world of benefits, they also put significant pressure on IT teams to develop, support, and secure them. Adding even more complexity, applications are constantly evolving due to usage and traffic fluctuations, creating scalability needs.

66% of the largest 100 US hospitals have consumer-facing mobile apps[2]

All of this is happening against the backdrop of a shifting society. The digital revolution and social sharing have created "super consumers" (in this case, patients) who expect transparent interactions customized to their interests and designed to fit into their increasingly online lives. You can see these changes happening in retail, financial services, entertainment, transportation, and other industries—and now, healthcare is catching up. As competition among healthcare systems for patient loyalty intensifies, mobile experiences can be a differentiator.

59% of all health-insured patients	70% of millennials

Would pick a primary care doctor who offers a patient mobile app for routine healthcare transactions over one that does not.[3]

Top 3 features patients want from a hospital app[2]

Access to electronic health records

Tool to book, cancel, or change their appointments

Ability to make prescription refill requests

At the heart of this enterprise lies the data center. Traditionally a basement-dwelling behemoth, today's healthcare data centers are evolving to a smaller footprint—and many are making at least a partial move to the cloud.

Managing data and applications in these diverse environments can be challenging. You need to ensure application performance across any device at all locations, especially as healthcare delivery moves beyond hospital walls. You need automation built in, to account for dwindling resources and eliminate downtime caused by human error. You need security to protect against the ever-rising threats to healthcare. And you need it all to work together, simply.

Do you have an Application Centric Infrastructure?

See the solution

What healthcare should know about moving to the cloud

Can this tightly-regulated industry really make the shift?

A recent article made a bold prediction: Healthcare data centers will be "extinct in five years."[4] While some are skeptical that the industry can move this quickly, others believe that it's entirely possible. In any event, the migration has already—at least partially—begun.

Here are the top 5 reasons healthcare is beginning to embrace the cloud.

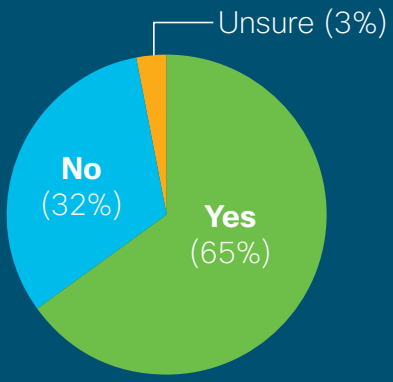
1 It saves space – and potentially, capital

Replacing hardware and software can be expensive—especially if you're considering investments that might be out-of-date in just a few years. Using the the cloud frees up those resources and allows organizations to pay only for what they use. It also opens up valuable real estate in hospital buildings that may already be tight on space.

2 It doesn't depend on physical location

For facilities located in areas prone to disasters (hurricanes, floods, earthquakes), the cloud can prevent loss of critical health data in the event of property or infrastructure damage.

Does your healthcare organization use the cloud?[5]



The two largest uses of cloud in healthcare today[6]

- ✓ Common applications such as email
- ✓ Clinical applications (i.e. EHR) delivered as SaaS

Epic as a service?

Watch the video

3 It makes IT teams more agile

As the volume of health data and usage of applications grow, a healthcare IT team using the cloud can rapidly expand services without needing to acquire new hardware—and then scale back if necessary.

4 It's secure

A quick internet search turns up dozens of articles proclaiming cloud to be even more secure than on premise. It's true: Trusted, hosted cloud companies often have more resources/technology, expertise, and time to focus on security than organizations with competing priorities, a shortage of staff, and tight budgets. Of course, it's still important to oversee security closely—just as you would with an on-premise data center.

5 It offers diversification

In healthcare, today's most popular strategy is to use a mix of on-premise, private, and third-party public cloud services.[7] This hybrid model allows IT leaders to control certain data and applications more tightly than others. Take for instance, image data like X-rays and MRIs. They're considered protected health information under HIPAA, need to be accessed frequently, and use up a lot of bandwidth, so they might be better managed in-house.

Considering a multi-cloud environment?

Take a look at Cisco HyperFlex

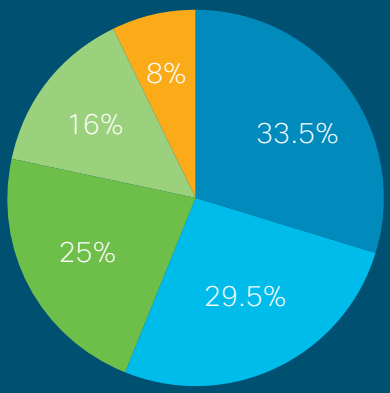
Zero-trust: Delivering the right data to the right person

The 5R's of healthcare data flow

There's a well-known safety adage clinicians use in regards to medication management: The right patient, right drug, right dose, and right route, at the right time. This same principle could also apply to data management. You need to make sure the right personnel have the right access to the right healthcare data—to the exclusion of everyone else.

Most organizations have policies and procedures in place to assure privacy, security, and access—but human error, both intentional and unintentional, can still occur. Alarmingly, a recent analysis named healthcare as the only industry in which insider threats (58%) posed the greatest risk to sensitive data.[8]

Healthcare data breach causes[8]



The solution: Zero-trust networks?

Traditional networks operate on the idea that a user inside the network is "safe" and can be trusted. But such "flat" networks, as they're known, have been the target of hackers, who can easily pose as insiders. Zero-trust assumes that no part of a network is safer than any other.

In this model, you create "whitelists" that allow you to identify specific characteristics of users and devices allowed to access applications and data. For example, in your organization, financial and business associates will likely need different types of access than clinicians.

If you think that developing and applying whitelist policies seems resource-intensive, you're right. But a technology solution like Cisco Tetration can automate the work, giving you deep visibility into what's happening on your network, and allowing you to make informed security and operational decisions using behavior analysis. Here's how a Cisco Executive explains it:

> "Enforcing policies—also known as segmentation or micro-segmentation—is just one of the steps to get to a Zero-Trust model. First, you need to know what policies you want to enforce. With [Cisco] Tetration, we observe thousands or tens of thousands of your applications and how they behave. We do this not only through the lens of their network communication, but also through the lens of what they do locally in their operating systems: process activity, memory usage patterns, file accesses, privilege escalations, container level granularity, all of which are invisible through the network lens alone."
>
> -Roland Acra, Senior Vice President & General Manager Data Center Networking, Cisco

Find out how Cisco Tetration brings the Zero-trust security model to applications

Read the report

Cybersecurity from the data center out

Build a data center that protects you and your patients

By now, most healthcare professionals are well-aware of both the volume and severity of cyber threats facing the industry. New attacks are discovered almost daily, and the proliferation of connected devices in healthcare only adds to the complexity. The burning question remains: What can healthcare organizations do about the problem that's sustainable and cost-effective?

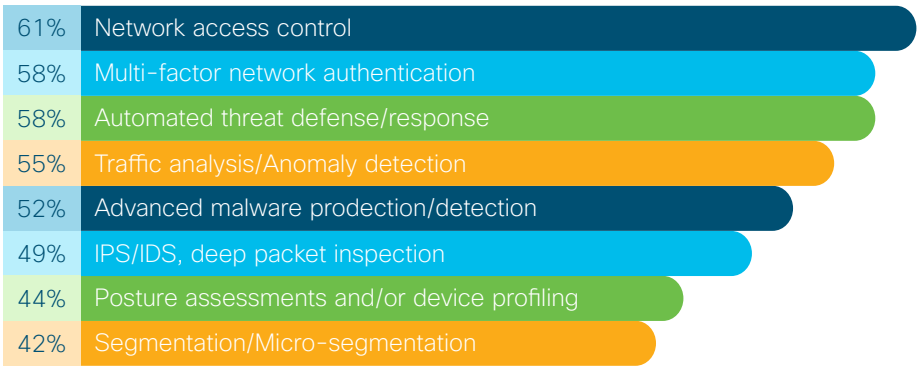
Find out more:

Read The Goldilocks Zone: Cloud Workload Protection White Paper

References

1. 2018 Mobile Health Survey results, Physicians Practice 2018
2. Hospitals struggle with mobile apps: How to fix it, Healthcare Business and Technology 2016
3. Survey: Patients Want More Digital Health Tools from Primary Care Physicians, Healthcare Informatics 2016
4. Healthcare Data Centers: Extinct in 5 Years? Healthcare IT News 2017
5. 2017 Essentials Brief: Cloud, HIMSS Analytics 2017
6. Health IT and The Cloud, 5 Must Watch Trends for 2017, HIMSS Analytics 2017
7. Healthcare Data Storage Options: On-Premise, Cloud and Hybrid Data Storage, HIT Infrastructure
8. Protected Health Information Data Breach Report, Verizon, 2018
9. 2018 Security Capabilities Benchmark Study of Healthcare, Cisco 2018

Percentage of organizations using specific security measures to secure their medical device network[9]



It comes down to efficiency, automation, and acting proactively—via both technology investments *and* an organizational culture of security—to protect your valuable workloads.

Discover cybersecurity strategies for healthcare

For IT teams working with the cloud, robust security requires specific network building blocks, including:

1. Visibility: High resolution visibility on the network, compute and storage planes inside the workload, as well as some visibility into the infrastructure layer
2. Vulnerability detection and management
3. Full lifecycle management of micro-segmentation policy
4. Application behavior analysis
5. Application whitelisting
6. File Integrity, memory monitoring, memory subsystem monitoring
7. Deception and decoys

Healthcare data centers continue to evolve and advance, much like the industry itself. And whether everything moves to the cloud in five years or 10 or 20 (or more), the steps you take now can help protect the availability of your applications and data, ensure privacy and security controls, and drive innovation across your enterprise.

Where human meets machine, exciting innovations are happening—and with the right foundation, your organization can grow, succeed, and leverage the tools of tomorrow.