vmware

Forrester Consulting Study Reveals Cyber Risk of Healthcare's Distributed Workforce

As across all industries, an unprecedented number of healthcare employees began working remotely in the spring of 2020. And like their counterparts, healthcare organizations—which by their very nature require an onsite workforce—were unprepared to handle the security challenges associated with remote work.

As health systems coped with treating patients, supporting clinicians, acquiring PPE and remaining operational, they were also frantically working behind the scenes to drive back escalating cyber threats, based on a commissioned study conducted by Forrester Consulting on behalf of VMware in January 2021 of more than 526 leaders responsible for strategy and security, with 53 of them in healthcare.[1] The survey revealed that security vulnerabilities were exacerbated as a distributed healthcare workforce relied on their own home networks, devices and online services to get their jobs done.

Although healthcare organizations intend to have employees return to onsite work as soon as possible, the success of emerging care models, such as telehealth, will depend on healthcare leaders strengthening defenses against cyber attackers to prevent operational losses, brand damage and patient harm.

> **Between 2019 and 2020, healthcare experienced a 9,851 percent increase in attacks as well as 239.4 million attempted cyberattacks targeting patients, an average of 816 attempted attacks per endpoint.**
>
> — VMware Carbon Black. "Healthcare in Crisis: A Look Back at 2020," February 2021.

1. Forrester Consulting. "Hindsight Is 2020 – The Pandemic Provides A Wake-Up Call: Integrated Solutions Future-Proof Organizations." February 2021. (A Forrester Consulting Thought Leadership paper commissioned by VMware.)

Key Finding #1

Attackers are exploiting healthcare's highly vulnerable, distributed workforce, and healthcare decision-makers are feeling the impact.

As administrative workers—and in some cases, healthcare clinicians, too—quickly dispersed to home offices during COVID-19, healthcare decision-makers have experienced major security concerns.

Those surveyed by Forrester cited these top issues as a result of an increased remote workforce:

- Increased need for endpoint security (47%)
- Acceleration of cloud adoption due to pandemic (45%)
- Loss of network visibility with remote workforce (45%)
- Loss of user activity monitoring with remote workforce (42%)
- Connectivity or bandwidth challenges through corporate VPN (40%)

A consistent theme was lack of visibility, which makes it harder to keep up with new and frequent threats. Here's why.

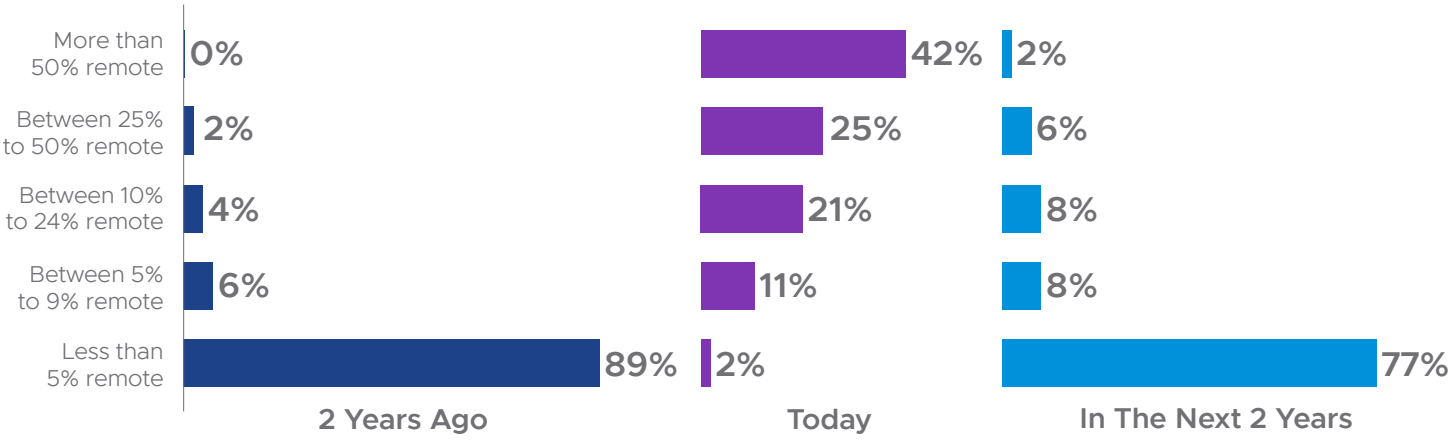
Until recently, patient information was perceived to be physically secure, confined to systems housed within offices and facilities. Healthcare sites typically avoided going all-in with cloud computing for the same reason—ensuring that information not leave the physical facility. With the increased remote workforce, the ability to secure newly remote end-user devices and environments has become the leading concern. Because healthcare information is highly confidential and protected by compliance mandates to assure patient privacy, it requires greater attention to network visibility and the ability to monitor user activity.

As healthcare workplaces moved offsite, IT lost the visibility and control needed to stay ahead of attacks. Endpoint and network security is of utmost priority so that security teams can regain visibility as well as address connectivity and bandwidth challenges through the corporate VPN.

Key Finding #2

Healthcare was less prepared for the security impact of remote workers compared to other industries.

Prior to COVID-19, healthcare organizations had very few remote workers. When asked what their workforce looked like 2 years ago and how they expected it to look in the next 2 years, healthcare decision-makers told Forrester:

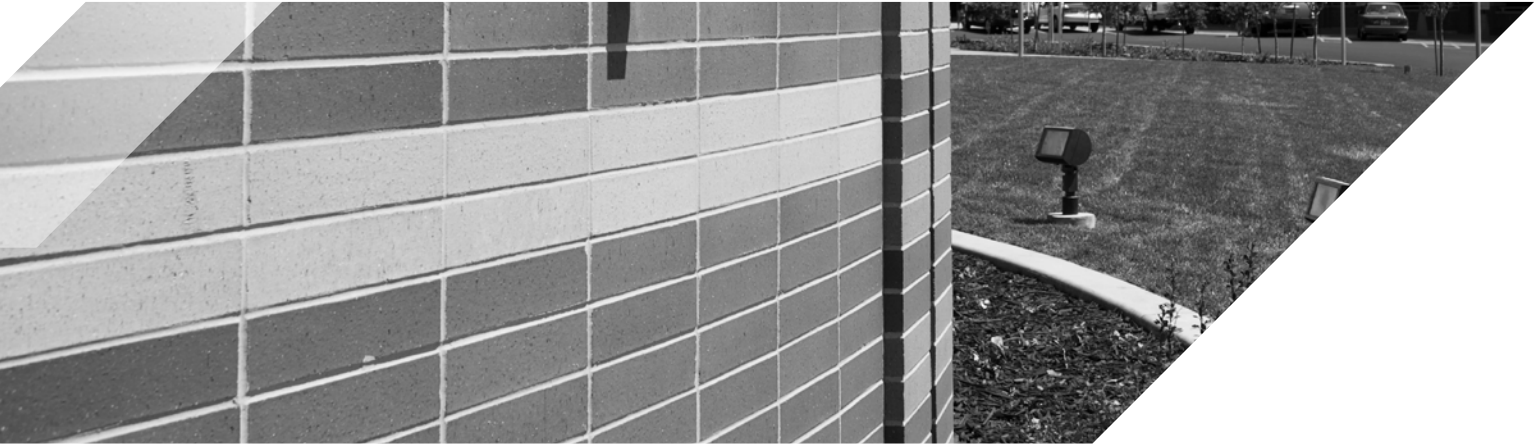


2 YEARS AGO	TODAY	2 YEARS FROM NOW
Only 11% of Healthcare organizations had more than 5% of employees remote	**98% of Healthcare organizations** have more than 5% of employees remote	**At least 23% of Healthcare organizations** will have more than 5% of employees remote

Most healthcare executives agree (85%) that their organizations had to quickly move the majority or all of their workforce remote at the start. These were among the most significant impacts to their businesses, particularly IT:

- Increased use of personal devices (80%)
- Accelerated a remote workforce strategy (75%) and had to piece one together (60%)
- Onboarding employees became more difficult (66%)
- Help desk tickets increased (64%)

Each of these factors is a recipe for a security breach. It will be important for healthcare IT to make long-term investments in remote work security to close existing vulnerabilities and stop new threats from succeeding, particularly with the rise and popularity of telehealth.



Key Finding #3

Healthcare prioritizes data protection, yet budget gaps and changing attack complexity prevent providers from improving security practices.

While other industries are highly focused on improving experience, healthcare decision-makers surveyed by Forrester are prioritizing safeguarding data. In a ranking of top use cases for the next 12 months, healthcare leaders indicated that their primary areas of focus are:

- Data protection (62%)
- Enhanced employee experience (55%)
- Protecting against endpoint and network threats (53%)
- Improved network performance (47%)
- Identity/access management (45%)

Organizational issues and dynamic environments tend to tie up healthcare providers' efforts to keep data safe and combat cyber threats. Healthcare's biggest security challenges today, according to the decision-makers whom Forrester surveyed, are:

- Lack of budget (34%)
- Changing/evolving nature of IT threats (32%)
- Day-to-day tactical activities taking up too much time (30%)
- Convincing the organization of the business value of security (28%)
- Securing the remote workforce (26%)

Through the crisis, healthcare organizations have been caught in the middle of a delicate balancing act. Caring for the influx of critically ill patients has been costly while wellness exams and elective surgeries were postponed or cancelled, affecting finances. Thus, it's no surprise that lack of budget has been an issue.

This, in turn, complicates the evolving nature of threats as corporate security is only as strong as its weakest link. Hacking, ransomware and other forms of malicious practices quickly became even more intense as employees relied on their own home networks, devices and online services to get their jobs done.

Key Finding #4

Shared adversity improved the relationship between IT and security teams, and security relationships saw significant gains.

Prior to the COVID-19 crisis, relationships between security teams and just about everyone else in the organization were predominantly negative. However, the healthcare IT teams benefitted from the pandemic's "we're all in this together" attitude, and many saw improvements in their working relationships, according to survey respondents.

These were among the most significant relationship changes:

- Security and IT practitioners relationships – 38% positive pre-pandemic to 60% positive today
- IT leadership and IT practitioners relationships – 26% positive pre-pandemic to 47% positive today
- IT audit and both security and IT teams – Improved +3% and +8%, respectively, since the start of the pandemic

As healthcare organizations sent key parts of their workforces' home to work, internal teams have seen the advantages in collaborating, communicating and aligning to support their remote workforces. As a result, many relationships have been improved, and this improvement extends to HR, workplace resources, and office and facilities teams as well.

Key Finding #5

Healthcare organizations are pivoting to address key use cases and future-proof their organizations.

It's notable that 43 percent of healthcare executives surveyed report that their delivery of employee experience has worsened in the wake of the pandemic, compared to only 23 percent reporting improvements. These numbers are more negative than all industries overall. Yet healthcare leaders are committed to moving forward and making the new normal work for them.

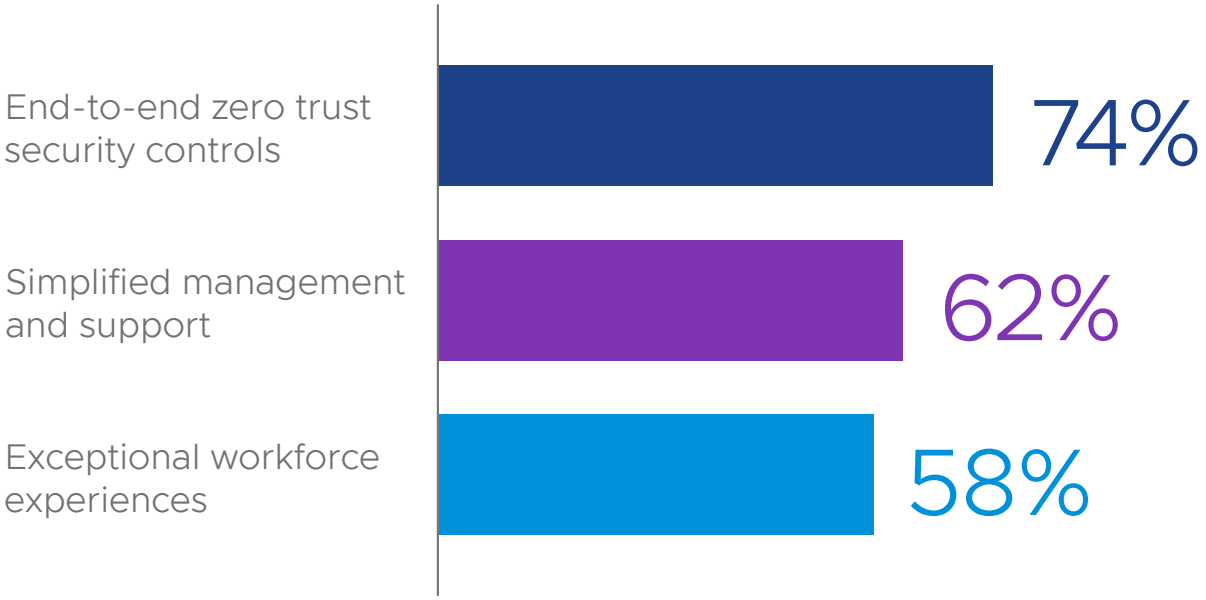
According to the healthcare respondents, this means prioritizing these use cases:

- Those helping future-proof our organization (51%)
- Those most important to business stakeholders (47%)
- Those that improve security or the security posture (47%)
- Those that reduce networking challenges (42%)
- Those that reduce remote workforce challenges (38%)

The good news for healthcare organizations is that there is a solution today that can jump-start all these efforts.

Next Steps:
Future-Proofing Healthcare IT

Boosting security and improving clinician and employee experience have become key priorities for healthcare organizations as they look to the future. These are not mutually exclusive needs. More than 70 percent of the healthcare decision-makers surveyed feel an integrated workforce solution is a high or critical priority, citing these benefits:



Delivering and handling data has moved front and center as a concern for healthcare executives managing in a forever-changed environment. A majority also see a need to provide employees better experiences. The proper handling of sensitive data requires a well-trained and supported workforce, regardless of whether they work from home or onsite. A key piece of this support, of course, is superior network performance, which enables consistent access while supporting strong security protocols.

All of this—superior application and information performance and usability, data protection, and robust networking—is integrated in the VMware Anywhere Workspace.

There is a great deal to learn from the pandemic's positive and negative impacts. While many healthcare executives see the work-from-home scenarios as temporary for much of their workforce, the rise in cyber threats and need to protect data are not changing.

Healthcare enterprises can and should take advantage of the improved relationships between IT and security teams to adopt integrated solutions that support stronger cybersecurity initiatives as well as bolster the day-to-day user experiences of remote workers. Positive relationships between teams can break down silos and create cross-function buy-in for stronger and more pervasive approaches to security—whether onsite or remote.

Learn more about VMware Healthcare Solutions by visiting *vmware.com/solutions/industry/healthcare-it-solutions.html*.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: FY21-6354-VMW-FORRESTER-HEALTHCARE-BRIEF-USLET-WEB-20210524 5/21