Bridging the Divide Between Physical and Digital Security

An IDC InfoBrief, Sponsored by Fortinet | **February 2019**

Lynne A. Dunbrack, Research Vice President, IDC Health Insights

IDC | ANALYZE THE FUTURE

Executive Summary

Healthcare organizations face mounting pressure to protect digital assets against cyberattack. Today's advanced physical security solutions increasingly connect to the IT network. Consequently, digital and physical security strategies are converging, with IT and facility security professionals collaborating on key initiatives.

This IDC InfoBrief presents case studies showing how two customers leverage Fortinet's Security Fabric components in their security strategies.

KEY FINDINGS

» Network-connected physical security devices are vulnerable endpoints at the edge that must be incorporated into the organization's security plan and managed by IT.

» A holistic platform approach using security fabric and greater access to data from security devices across the enterprise is key to uncovering invaluable insights on potential physical and cybersecurity vulnerabilities.

» Physical and digital security strategies must promote patient safety and not deter optimal patient care.

Digital Transformation Drives Security Transformation

As healthcare organizations embark on digital transformation and migrate to new digital processes and business models, a greater sense of urgency is created across the industry to incorporate security transformation up front.

66%

of hospitals/medical centers report that their IT security services spending will increase from 2018 to 2019.

22%

of all IT respondents (hospitals and ambulatory clinics) reported that physical security measures were a top area for increased IT services spend.

TOP FOUR REASONS

27%	Data security
21%	Cyber-security
20%	Disaster recovery
20%	Managed security services

Source: US Healthcare Provider Technology and Services Survey 2018, IDC, November-2018 / N = 100

Cyberthreats Intensify

By 2022, 40% of healthcare providers will leverage machine-learning and AI-algorithm advances to improve their cybersecurity capabilities with automated threat detection to thwart ransomware.[1]

IT Security Impact

The adoption of AI and machine learning–based cybersecurity solutions will:

- Add transparency and increased visibility into network operations
- Accelerate the identification of anomalous behavior
- Automate threat detection and response
- Act to isolate threats from spreading through the network

Guidance

Healthcare providers looking to address these cybersecurity threats should:

- Be aware of cybersecurity trends and threats as they emerge and inform staff about best practices
- Take a long-term view of cybersecurity approach and include AI-based security solutions
- Find trusted suppliers of cybersecurity technology that understand AI technology solutions

Healthcare providers are at high cybersecurity risk as they store personal and financial data, and their network systems are very sensitive to interruptions.

[1] Oct 2018 - IDC FutureScape - Doc # US43122618. IDC FutureScape: Worldwide Health Industry 2019 Predictions.

Leveraging Digital Security to Ensure Staff and Patient Safety

Workplace violence – whether physical or verbal – takes its toll on healthcare workers. In addition to physical injury that may require staff to seek their own medical treatment and miss work, caregivers experience higher levels of stress, burnout, and fatigue when exposed to workplace violence. This in turn leads to a higher risk of medication errors and patient infections.[1] OSHA and the Joint Commission have identified key steps that healthcare organizations should take to ensure staff and patient safety.

OSHA® Occupational Safety and Health Administration

According to OSHA, a comprehensive workplace violence prevention program consists of the following five key components:

1. Management commitment and worker participation
2. Worksite analysis and hazard identification
3. Hazard prevention and control
4. Safety and health training
5. Recordkeeping and program evaluation[2]

Joint Commission on Accreditation of Healthcare Organizations

The Joint Commission's Sentinel Event Alert (Issue 59, April 17, 2018) recommends making changes to the physical environment by deploying stationary and mobile panic buttons, video surveillance, and keypad door access. Healthcare organizations should evaluate their own data to determine which physical security technology should be deployed and where to ensure patient and staff safety.[3]

[1] Rogers, A.E., Hwang, W.T., and Scott, L.D. 2004. The effects of work breaks on staff nurse performance. Journal of Nursing Administration. 34(11): 512–519.
[2] Source: https://www.osha.gov/Publications/OSHA3826.pdf.
[3] Source: https://www.jointcommission.org/assets/1/18/SEA_59_Workplace_violence_4_13_18_FINAL.pdf

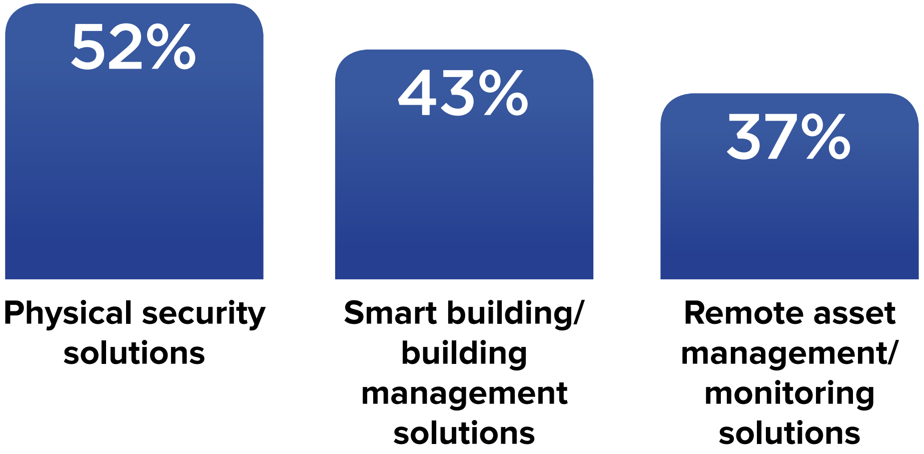
A Growing Convergence of Digital and Physical Security

Cyber and physical security are becoming intertwined as more physical security devices such as video surveillance, employee badges, and door locks are connected to the network and stream data to be aggregated, analyzed, and monitored as part of a greater Internet of Things (IoT) initiative.

Historically, physical security and cybersecurity were separate functions. However, with the growing convergence between digital and physical security, the ownership and responsibility for networked physical devices is shifting from the facility security team to IT.

Ultimately, there will be a blending of the physical and cybersecurity teams with the chief security officer responsible for ensuring physical safety and digital security.

Has your organization deployed any of the following solutions as part of your IoT initiatives?



N = 313 U.S. providers
Source: Global IoT Decision Maker Survey, IDC, October, 2018

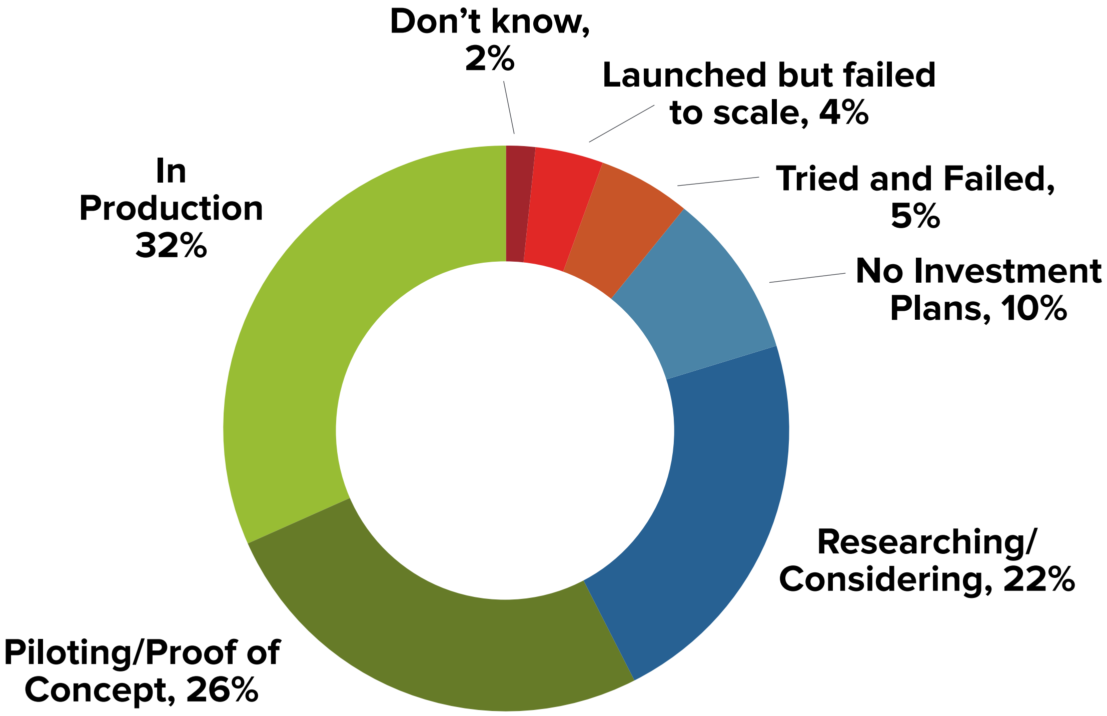
Adoption of Converged Physical and Digital Solutions is Growing

Health facility infrastructure and security solutions are widely deployed to provide physical security enhanced with IoT-based technology.

These findings suggest that the convergence of technical and physical security is well underway. That said, healthcare organizations need to work with the right technology partner to mitigate the risk of failed deployments.

57%

of respondents report active use of health facility infrastructure and security solutions.



22%

of respondents are in the researching or considering phases.

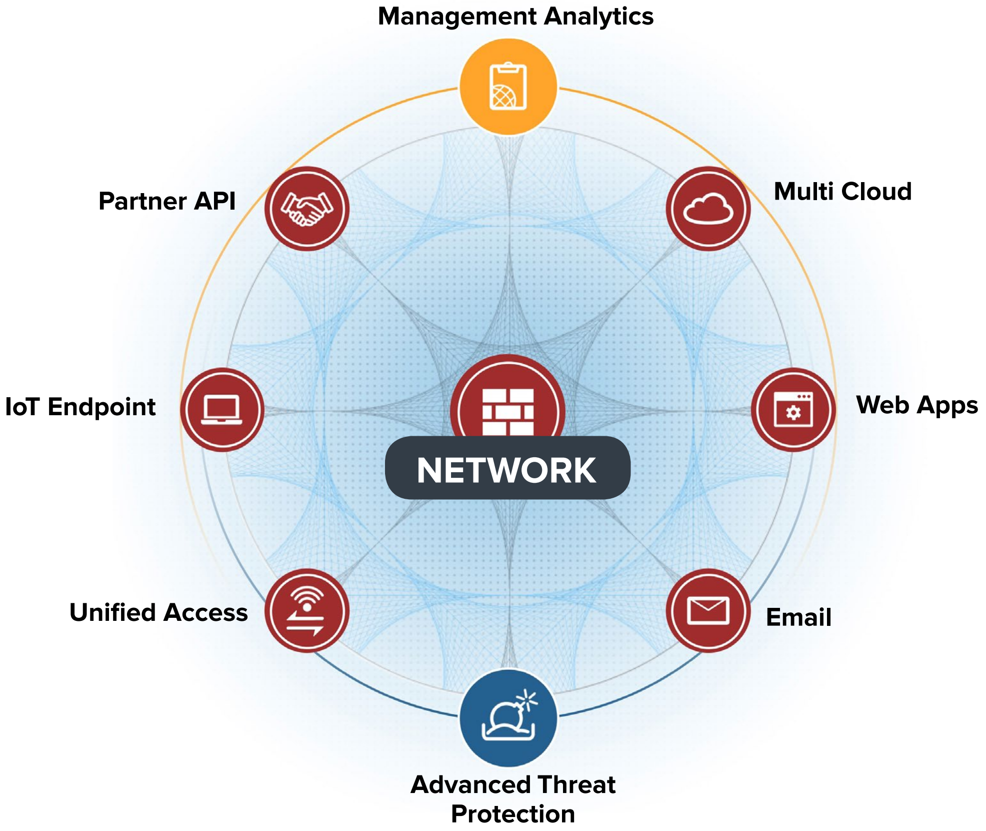
N = 54 U.S. providers
Source: Global IoT Decision Maker Survey, IDC, October, 2018

Bridging the Divide Between Digital and Physical Security Requires Security Fabric

IDC defines security fabric architecture as an integrated and automated security framework that provides network, multicloud, and IoT endpoint security and advanced threat protection along with advanced security management and analytics.

Benefits of Security Fabric Architecture

- Combines the many elements of security into a common security framework
- Enables incremental buildout of the overall security strategy
- Provides greater levels of integration and intelligence sharing between security products
- Reduces operational costs and staffing requirements through automation, single pane of glass visibility into the network, self-optimization and self-healing capabilities
- Accelerates response and remediation time in the event of a suspected or known attack



CASE STUDY 1

Solution Snapshot

Organization: Riverside Healthcare is a fully integrated system serving patients in four Illinois counties.

Operational challenge: Understanding what devices are connected to the network.

Solution: 14 Fortinet products and solutions, including FortiSwitch, FortiAP, FortiNAC, and FortiVoice.

Benefits: Platform solution provided true integration across security products and enabled vendor consolidation that also helped to reduce operational costs.

Lessons learned: Do your own homework up front. Identify what capabilities you need in the next three to four years so you don't outgrow your initial investments.

Riverside Healthcare Takes a Holistic View of Security

"You need to think holistically. What is the end goal for deploying the technology? Then think like a hacker to identify how they might exploit that technology. This perspective has opened the eyes of the facility security and cybersecurity teams to issues that they haven't thought of before." —Erik Devine, CISO, Riverside Healthcare

Riverside Healthcare is a longstanding Fortinet customer. The Illinois-based integrated delivery network installed its first Fortinet firewall seven years ago after evaluating six other vendors' products. Selection factors for the initial security technology acquisition included: Fortinet firewalls were a proven product; the software was the same between devices for wired and wireless networks; and lower operational costs were "CFO-friendly."

As Riverside grew in size and complexity, it was clear that a truly integrated platform was needed to address the enterprise's expanding physical and cybersecurity requirements. Since deploying Fortinet's firewall technology in 2011, Riverside has taken advantage of Fortinet's Security Fabric and expanded its security portfolio to 14 Fortinet products and solutions including FortiSwitch, FortiAP, FortiNAC, and FortiVoice.

The physical security director and CISO work closely together and jointly manage the video surveillance and door systems. Consequently, Riverside has achieved operational efficiencies by taking a holistic view of security. This close working relationship has also helped the facility security director to think differently about how physical security devices are deployed. For example, before working with the IT security team, the facility security team might not have contemplated what would happen if a video surveillance device was attacked by cybercriminals, taken offline while a physical crime was committed, and then turned back on to reduce detection of the intrusion. Now, physical security is applying cybersecurity best practices as the two disciplines are more closely aligned. The combined expertise of physical security and law enforcement, along with digital and cybersecurity, greatly enhances the overall security of patients, staff, visitors, and IT assets.

CASE STUDY 2

Solution Snapshot

Organization: Bridgeway Senior Healthcare is a family-owned provider of senior care ranging from subacute / rehab care and long-term care to assisted living.

Operational challenge: Replacing a legacy system on the brink of failure, with limited resources to do so.

Solution: FortiVoice

Benefits: Greater staff efficiencies, visibility into communication practices, and ability to hold staff accountable improved communication overall and led to a better staff and patient experience.

Lessons learned: Glean best practices and potential use cases from customer references. Focus on solutions that make staff or processes more efficient.

Bridgeway Senior Healthcare Creates a Better User Experience and Competitive Advantage with FortiFone

"Deploy a solution that makes caregivers more efficient in caring for their patients."
—Jason Dugenio, CIO, Bridgeway Senior Healthcare

Bridgeway Senior Healthcare selected Fortinet's FortiVoice and FortiFone to replace a legacy voice and voicemail system with one using a more modern architecture. Key selection factors included company reputation, solid products, customer references, costs, and ease of management. Lower acquisition and operational costs for Fortinet's products enabled Bridgeway to also make infrastructure upgrades at the same time.

FortiVoice offers a cordless handset solution which works well in the Bridgeway environment given the inherent mobile nature of staff and caregivers. Calls from physicians or family members can be easily transferred to caregivers and nurse managers no matter where they are in the building or campus. The ability to log when a call came in, how long it took for someone to pick up the call and the length of the conversation, and whether a voicemail was left if the call went unanswered has led to improved visibility into communication practices and greater staff accountability for voice communication. Bridgeway staff, as well as patients and their family members, report that communications has improved since FortiFones were deployed, resulting in greater satisfaction levels. While ROI can often be difficult for healthcare organizations to quantify, better communications is at the core of quality patient care. The ability to respond quickly to hospital case workers looking for a SNF or rehab bed, or a family member inquiring about an assisted living option for a loved one, also has a financial impact. Senior care is a census-driven business. A missed call is a missed opportunity to admit a new patient into a Bridgeway facility.

Bridgeway is exploring adding FortiCamera and FortiRecorder. Use cases for these technologies include monitoring patients who are at risk for wandering, caregiving staff being in the right place at the right time, and monitoring physician rounding. Object recognition capabilities enable asset tracking and inventory management. Fortinet's Security Fabric enables Bridgeway to add new security capabilities, including connected physical security devices that protect patients.

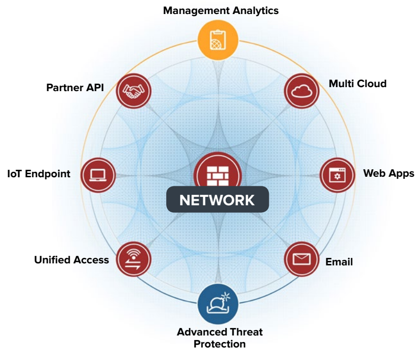
Essential Guidance

Consider your long-term plan for security/take the holistic view.

Develop an overarching security plan that combines physical and digital security.

Look to form a strategic relationship with your security technology supplier.

Share best practices between cyber and physical security.



Deploy a platform solution/fabric.

A MESSAGE FROM OUR SPONSOR

About Fortinet: Fortinet is a worldwide provider of network security appliances and a market leader in Network Security (FW/NGFW/UTM). Our products and subscription services provide broad, integrated and high-performance protection against advanced threats while simplifying the IT security infrastructure. NASDAQ: FTNT

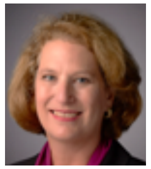
FORTINET®

Learn more about Fortinet Healthcare Solutions at
https://www.fortinet.com/solutions/industries/healthcare.html

Contact healthcare@fortinet.com for a Cyber Security Threat Assessment.

Follow us @FortinetHealth on Twitter

IDC Analyst Profile



Lynne A. Dunbrack
Research Vice President, IDC Health Insights

Lynne Dunbrack is Research Vice President for IDC Health Insights responsible for the research operations for IDC Health Insights. She manages a team of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads the IDC Health Insights' Connected Health IT Strategies program. Specific areas of Lynne's in-depth coverage include mobile, constituency engagement, interoperability, health information exchange, privacy, and security. Technology coverage areas include clinical mobility (physician facing) and mobile health (consumer facing), health information exchange, end-to-end remote patient health monitoring for health, wellness and chronic conditions, Internet of Things (IoT), personal health records and member, patient, provider portals, kiosks, videoconferencing and online care, unified communications, aging in place, and social.

IDC Corporate USA
5 Speen Street
Framingham, MA
01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.