Healthcare Network Cybersecurity in the Age of Digital Transformation

Includes special guest interview with Silvia Piai, Research Director for IDC Health Insights

IDC ANALYZE THE FUTURE

Brochure

Alcatel·Lucent Enterprise

Executive summary

Cybersecurity has long been a top priority for healthcare organisations. However, cybersecurity demands are changing due to the digital transformation taking place. Digital transformation means that healthcare organisations use more connected and mobile devices on their networks while clinicians, partners, and consulting physicians are increasingly accessing applications and data from beyond the network perimeter. As change accelerates, the old methods of network security can no longer keep up.

In this document, Silvia Piai, Research Director at International Data Corporation (IDC) shares insights on the forces changing today's healthcare cybersecurity requirements and recommends strategies healthcare organisations can adopt and technologies they can deploy to keep data and systems secure in the age of digital transformation. Alcatel-Lucent Enterprise will share how its Digital Age Networking (DAN) solution meets the demands of a digitally transformed enterprise. With a multi-faceted approach to cybersecurity, DAN maintains trust with secure, policy-based access to connected medical devices, patient data and software applications across the healthcare ecosystem.

The state of cybersecurity in healthcare today

Healthcare organisations invested **$5.5 billion globally** in cybersecurity in 2019.

In survey after survey by IDC, healthcare organisations report that cybersecurity is a top priority.[1] That's not surprising. Healthcare has long been, and remains, one of the industries targeted most by hackers. And, the problem continues to grow. In 2018, the healthcare sector saw 15 million patient records compromised in 503 breaches, three times the count in 2017, according to Protenus Breach Barometer.[2]

Breaches occur because healthcare data is extremely valuable. Individual patient records contain everything including name, current and previous addresses, work history, names and ages of an individual's relatives, and financial information such as credit cards and bank numbers.[3]

Not only do cybersecurity breaches result in stolen data, they can also lead to operational interruptions, damage to the hospital's reputation, and fines for violations of regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. An even worse situation is the potential for patient's to be harmed. For example, a pump may provide the wrong amount of insulin. Or information may not be delivered to a physician as they are treating the patient, leaving the physician unaware of allergies or other medications the patient is taking.

IDC estimates that healthcare organisations invested $5.5 billion globally in cybersecurity in 2019 to mitigate these risks. From today until 2022, IDC projects a compound annual growth in cybersecurity spending in healthcare of 8.7 percent, which is similar to the amount spent by other industries.[4]

Despite these investments, longstanding gaps in healthcare cybersecurity remain. While many organisations say that cybersecurity is a priority, it often remains an afterthought in daily practice. After all, clinicians are in the business of healing people, not thinking about cybersecurity. Clinicians, moreover, may actively resist efforts to enforce cybersecurity if it impedes clinical workflows. For instance, if doctors, nurses and clinicians are required to spend a lot of time logging in to authenticate themselves for access to electronic medical records or health record system (EMR/EHR), they will look for shortcuts to save precious time. And, many clinicians are simply not sufficiently aware of cybersecurity threats and impacts.

[1] For example: Priorities, Strategies, and Investments: Overcoming DX Challenges in European Healthcare https://www.idc.com/getdoc.jsp?containerId=EMEA44355219

[2] https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

[3] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#2bb1f96b50cf

[4] IDC's Worldwide Semiannual Security Spending Guide https://www.idc.com/getdoc.jsp?containerId=IDC_P33461

Changing cybersecurity threats

At the same time, the nature of cybersecurity threats is changing. Hackers are using artificial intelligence (AI) and machine learning (ML) to create more sophisticated, automated attacks. New social engineering techniques enable criminals to connect crumbs of information found across social media to create very good profiles of individuals or of the data held by healthcare organisations.

Digital transformation within the healthcare industry is further changing cybersecurity requirements, resulting in greater complexity, increased use of connected devices, a perimeter that is disappearing, and all at an accelerating pace.

Greater complexity

Healthcare organisations are adopting new technologies, including cloud, mobile, IoT, Big Data, and advanced analytics. These new solutions bring a new level of complexity that requires a new way of looking at security.

Increasing use of connected devices

By 2022, 97 percent of bedside nurses, 98 percent of physicians, 96 percent of pharmacists and 94 percent of emergency room nurses will be utilising mobile devices.[5] As healthcare organisations and patients increasingly use mobile, IoT, and home health devices such as Fitbits, new vulnerabilities have emerged.

For example, the first generation of connected medical devices did not require passwords. Because these devices connected to the network, hackers could use them as a gateway onto the network. Today, the FDA and European equivalents mandate security features such as

By 2022, 97 percent of bedside nurses, 98 percent of physicians, 96 percent of pharmacists and 94 percent of emergency room nurses will be utilising mobile devices.

[5] https://www.aiin.healthcare/topics/connected-care/over-90-nurses-physicians-will-use-mobile-devices-2022

hardcoded passwords. Yet breaches remain inevitable and when they occur, hackers can still gain access to the entire network. IDC research shows that only 6 percent of European healthcare providers have a connected medical device security strategy integrated into their enterprise security architecture, and worryingly 16 percent have not begun to assess the potential threats to networked medical devices.[6] Indeed, presenters at the Fifth eHealth Security conference of the European Network and Information Security Agency (ENISA) estimated that there has been a 600 percent increase in attacks on IoT devices, specifically medical devices.[7]

Only 6 percent of European healthcare providers have a connected medical device security strategy.

The perimeter is disappearing

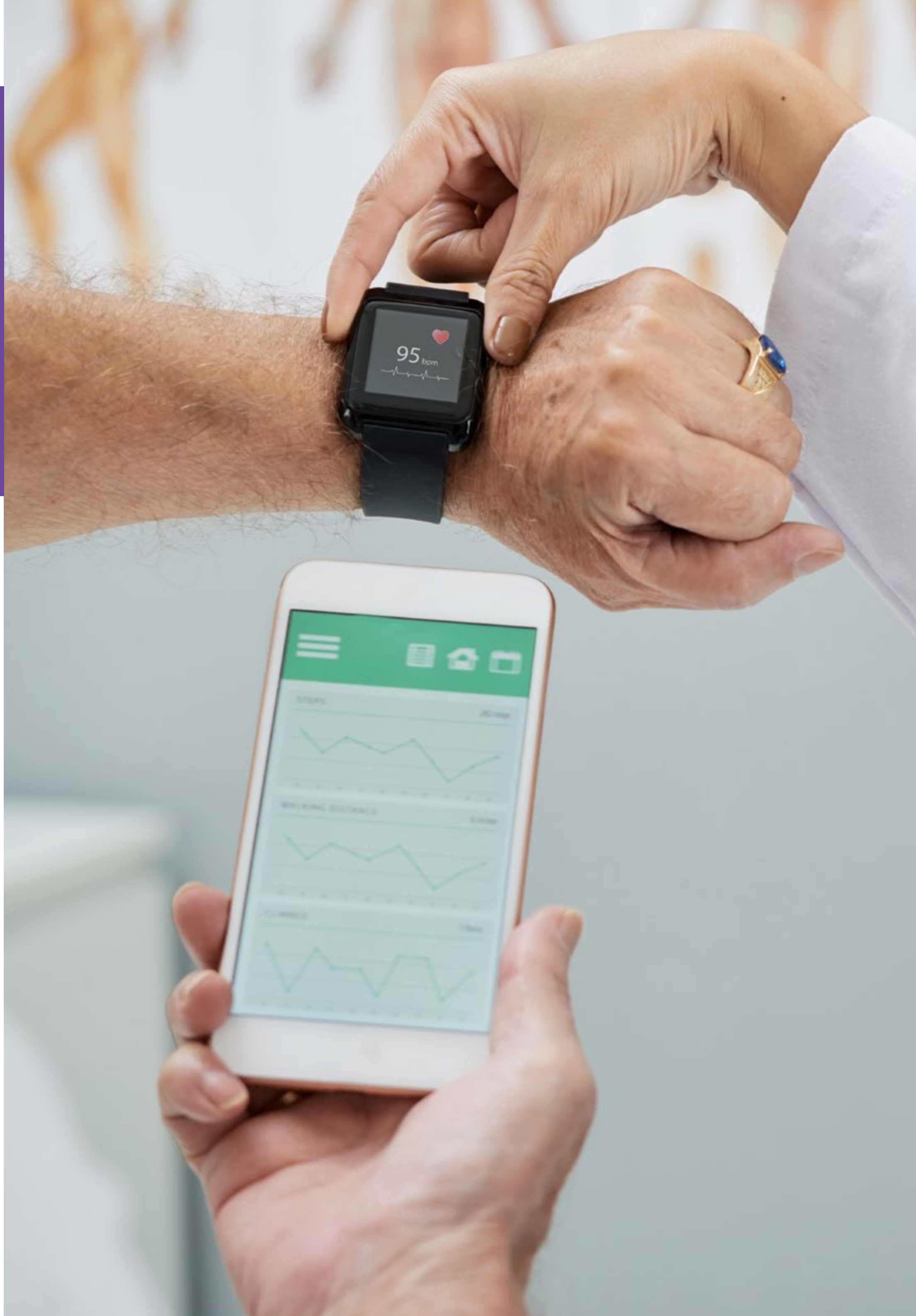
Most organisations have, for a long time, clearly demarcated between users and resources inside and outside the network.

However, as healthcare organisations embrace digital transformation, they become more open to exchanges with the broader ecosystem, including patients, partners, payers, government healthcare authorities, and other providers in an integrated care/collaborative care environment. Users no longer simply access resources from inside the network perimeter—they can be anywhere. Surgeons might exchange information with primary care physicians in a different network. Hospitals might monitor patients remotely after discharge from the hospital. Physicians may use data from patients' personal healthcare devices to aid in diagnosis and care.

IT resources are also no longer confined to inside the perimeter. They're on-premises and in the cloud and connected via APIs. Healthcare organisations need modern ways to protect resources when the perimeter no longer exists.

Accelerating rate of change

In a digitally transformed world, everything moves faster. Security tools must handle this speed.



[6] IoT Security in European Healthcare https://www.idc.com/getdoc.jsp?containerId=EUR145549919

[7] https://www.enisa.europa.eu/events/5th-ehealth-security-conference

Interview with Silvia Piai, Research Director for IDC Health Insight

Alcatel-Lucent Enterprise recently had the opportunity to speak with Silvia Piai, Research Director for IDC Health Insights, to get IDC's views and recommendations regarding cybersecurity in the healthcare industry.

IDC recommendations for enhancing cybersecurity in healthcare

Despite the emerging challenges, the healthcare industry's approach to security remains traditional. Healthcare organisations often implement security simply to tick the compliance boxes and don't consider changes due to digital transformation that impact security requirements.

IDC recommends that healthcare organisations adopt a holistic approach to network security that includes strategy, technology, people (for example, training), and processes (for example, how security is embedded in workflows). In this paper, we will look at strategy and technology.

Strategy

Instead of implementing the minimum cybersecurity to achieve compliance, healthcare organisations should take the opportunity to develop a strategic security plan that manages risk in a manner that meets the demands of today's digital transformation context.

They should:

- **Think of regulatory compliance as a starting point.** While many organisations start by doing the minimum necessary to comply with GDPR, or other equivalent regulations outside of Europe, healthcare organisations should think of regulatory compliance as a starting point for rethinking the way they're managing and governing data within their organisations and with their partners.
- **Understand that security drives business value** by ensuring business continuity. Healthcare organisations must avoid lost revenue (and reduce patient safety

concerns) that result from cyberattacks that take down IT systems. Align security with your broader enterprise objectives and make it a part of your everyday business.

- **Follow a security-by-design approach:** Risk goes hand-in-hand with business workflows, which are constantly evolving along with technologies. Healthcare organisations must incorporate security into workflows from the start. Security needs to be a core business value and complement every business decision healthcare organisations make.
- **Work with the ecosystem.** Healthcare organisations no longer have a clear perimeter to defend as they integrate care from other organisations for their patients and partners. They need to work with the ecosystem to maintain cybersecurity.

Technology

Creating a secure connected ecosystem becomes paramount as healthcare organisations digitally transform their operations. This ecosystem requires a layered approach that places the four core disciplines of security–identity management, vulnerability management, threat management and trust management–into a new dimension enabling scalability, velocity, intelligence and automation. This approach should align with the broader enterprise digital environment and the outcomes the organisation wants to achieve.

Key aspects of layered network security technology should include:

- **Endpoint security**–to manage vulnerabilities for individual devices.
- **Identity management**–to authenticate users and control access. The solution should provide user authentication capabilities and fine-grained security policies that grant users just the right level of access to only the information they need.

- **Secure data exchange**–the use of encryption and secure file exchange protocols should safeguard data in motion.
- **Containerisation**–to prevent threats from jumping from one system to the next once a threat has gained access to the network, the solution should use containerisation and network segmentation to isolate individual systems.
- **Trust management**–healthcare organisations need a risk management approach that addresses the fact that users and resources can reside outside the network perimeter. One way to establish trust in such an environment is by understanding what constitutes normal and abnormal behavior on the network. Artificial intelligence (AI) enabled tools for identity and authorisation management enable you to establish a normal baseline for behavior on the network. These tools can evaluate each user and device and their application, security, and quality of service requirements to establish a normal baseline behavior. Thereafter, AI can quickly identify any unusual events or actions, such as a surveillance system tapping into an EMR or EHR, and analytics that help determine why something has changed.
- **A software-defined architecture**–an automated network management solution can provide the speed required to keep up with digital transformation.

The Alcatel-Lucent Enterprise solution

Alcatel-Lucent Enterprise Digital Age Networking in Healthcare is a multi-faceted approach to healthcare network cybersecurity that provides security in depth for connected medical devices and applications through multiple layers of security.

Flexible connectivity through a service defined network

Our approach starts with a flexible, service defined network that makes it fast and easy to configure network and cybersecurity policies for the vast number of connected users, devices and applications that fuel digital transformation.

In the past, IT has been a break-it/fix-it operation. IT would install new equipment, get it up and running, and manage the network using tedious manual processes. DAN is a smart, automated network that makes it easy to connect users and devices to their specific applications in a secure manner. Built using Alcatel-Lucent Enterprise Intelligent Fabric (iFab) technology, DAN includes our homegrown Intelligent Fabric combined with industry-standard Shortest Path Bridging (SPB). Together, these technologies simplify the creation and configuration of networks while enabling multipath routing and link aggregation to combine multiple network connections in parallel and thereby increase throughput and provide redundancy.

With the ALE approach, IT defines network services, architecture, access policies and containers and the network builds itself out automatically. Once the network is architected, if anything is moved, changed or added, the network makes the necessary adjustments automatically and undetectably. For example, if a switch goes out of service, the network will automatically reroute around that switch.

Using a service defined network, healthcare organisations benefit from automation that reduces manual configuration errors and helps them keep up with the accelerating rate of change within their organisations. Because automation eliminates manual work, IT becomes more of a business engine driver.

Comprehensive access control through intelligent, automated policies

Healthcare organisations can use ALE DAN to define user access rules and policies that govern which applications and devices users can access and use—and follow users wherever they go. For example, they can set up policies that give:

- Physicians access to all systems except financial systems
- Patients access to internet services
- Lifesciences companies or other partners a contractor-based policy

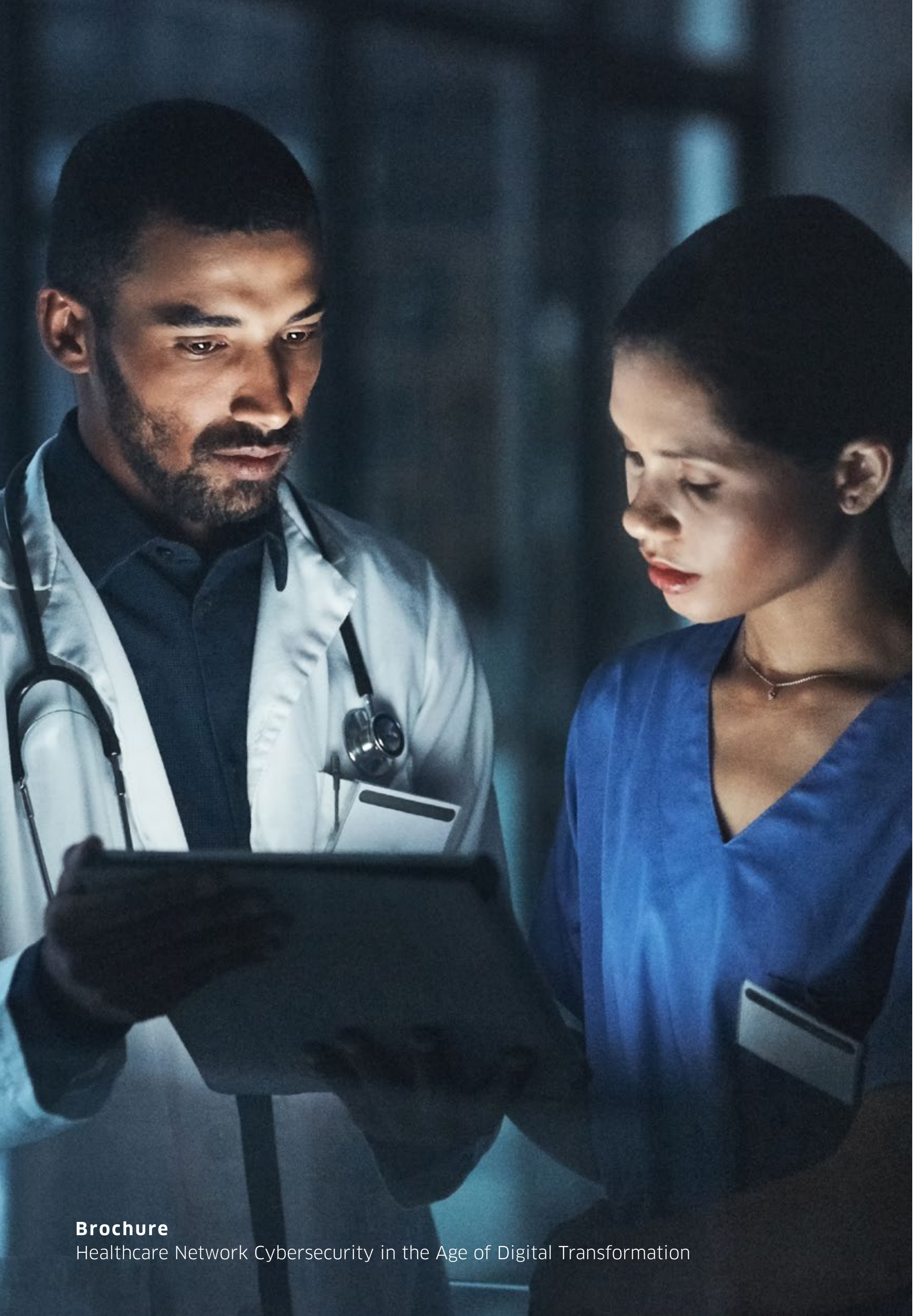
ALE also offers location-based services, such as indoor wayfinding navigation, asset and people tracking that enables healthcare organisations to set up policies that take user location into account.

Unified Policy Management capabilities enforce policies automatically every time a user connects, ensuring users have only the permitted access privileges. Once users log into the network with a PC/laptop/mobile device and their credentials are validated, they don't need to keep authenticating. They stay connected if the device is on and the system automatically enforces the policy for that user.

Policies ensure that all users, inside or outside the organisation, have access only to permitted areas and that these access controls are enforced consistently. They also simplify hospital workflows while enforcing cybersecurity. Clinicians caring for patients can quickly access the systems and information they need to care for patients without onerous security login procedures.

Reduced vulnerability with containerisation and segmentation

Healthcare organisations use many IoT devices, including MRI machines, patient monitors, infusion pumps, prescription dispensing robots, as well as video cameras, HVAC systems, sprinkler systems, intrusion detection systems, and many others. The ALE DAN solution allows healthcare organisations to containerise each device, creating a virtual network segment for it to prevent any device from becoming a vector for attack. Containerisation within DAN makes multiple virtual networks out of a single physical network, which is managed by a single management system.



Containerisation is simple for IT to implement. The DAN solution automatically discovers each device on the network. When a device is plugged into the network, the Alcatel-Lucent OmniVista® 2500 Network Management System, available on-premises or in the cloud, attempts to identify that device. If the management system doesn't have the device in its database, it will consult a cloud-based database of 17 million plus devices.

Once the device is identified, the system will classify it, for example, as a security camera. If that device is on the approved vendor list for security cameras, it will be connected to the network. If not, then it won't be connected. The solution is then set up in a virtual container for the device, segmenting it from the rest of the network. If someone hacks into any networked device, that attacker will be unable to use that device to access the rest of the network.

Improved trust through artificial intelligence

Once devices are connected, they must be continuously monitored to identify any threats and maintain trust. ALE analytics and application visibility allow network administrators to see what's going on in the network by device. Analytics identify patterns for normal, expected network behavior as well as any unusual patterns when they occur. We can look at the behavior of applications at the edge of the network to decide whether to connect to that application as well as unusual behavior in allowed applications, such as a video camera that's producing more data than it should.

If an anomaly or unusual behavior occurs on the device, the analytics will show that so the network security manager can intervene. Today the investigation must be performed manually, but ALE is working on automating the response using AI and ML.

AI capabilities support remote patient services as well. ALE is developing equipment that allows hospitals to remotely monitor patients in their home as they recover from an ailment or surgery. The equipment needs to securely communicate data from the device to the hospital. AI can monitor activity from remote IoT devices to ensure their behavior is consistent with expected behavior. In addition, patients are increasingly using apps to monitor their health. If a clinician can monitor an Apple Watch® or other monitoring device worn by a patient, they can improve patient engagement and make better diagnoses. With ALE AI, healthcare organisations will have visibility into whether an application or activity within it can be trusted.

Secure network equipment reduces vulnerabilities

Healthcare organisations today are aware of the need to secure IoT devices on the network. But they may fail to consider devices that form the foundation of the network, such as switches and access points.

ALE employs many technologies to reduce the threat from these devices. Our solutions:

- Harden the OS software to provide secure, diversified code.
- Send the OS software for third-party verification and validation to ensure it has no easy entry points or backdoors.
- Ensure every time a switch is booted up, the memory is compiled and brought up in a different manner. Although switches function identically, no two have the same memory configuration internally. If someone were to break into one of our switches, they would be unable to access another switch the same way.
- Provide built-in denial of service (DoS) protection. Our CPU can detect unusual amounts of network traffic and automatically shut down the CPU if necessary.
- Complete multiple security certifications such as JDIC and FIPS.
- Perform continual software upgrades.

Secure connections for incoming and outgoing traffic

For incoming traffic, our VPN capabilities provide an encrypted connection to the local network while end-to-end traffic is protected using the MACsec encryption (also known as IEEE 802.1AE) to protect information as it traverses the network, and with the ability to reload services, such as TLS and HTTPS with no reboot required, the network isn't interrupted.

Reporting

ALE reporting enables different personas to access information about the status, health and performance of the network, how applications are running, and user satisfaction. For example, IT can see data about network performance and operations. Line of business units can ensure that equipment such as imaging systems (MRI, X-rays) are transmitting data to servers and tablets seamlessly. CXOs can determine whether the network is delivering services that allow clinicians to spend more time with patients and whether they're getting the most out of the network.

Conclusion

Digital transformation has profoundly changed hospital's cybersecurity requirements as the number of connected devices increases, the network perimeter disappears, and change continues to accelerate. The Alcatel-Lucent Enterprise Digital Age Networking in Healthcare solution keeps your IT assets and patient data secure in today's age of digital transformation. Through this solution, you can closely manage user access, reduce vulnerabilities created by IoT, mobile and network devices, keep the inevitable breach from providing a vector for attack and communicate across the healthcare ecosystem from a position of trust.

We are Alcatel-Lucent Enterprise.
We are ALE. We help you Connect your patients, staff and healthcare ecosystem. Delivering technology that works across and beyond your facilities.
www.al-enterprise.com/en/industries/healthcare

www.al-enterprise.com The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2020 ALE International, ALE USA Inc. All rights reserved in all countries. DID20021001EN (March 2020)

Alcatel·Lucent
Enterprise