HEALTHCARE

USE CASE GUIDE

Acquisition-Ready Architecture

SAFELY AND SECURELY ACCELERATE MERGER AND ACQUISITION PRIORITIES

AUGUST 2023

Spotlight

Business Benefits

Accelerate the time to value and maximize the return on their merger and acquisition investments.

Operational Benefits

Streamline integration activities and removing barriers to achieving operational excellence.

Enable a smooth and secure onboarding process for acquired sites and assets.

Ensure patient access to care applications, services, and devices.

Security Benefits

Deliver visibility, insights, and protections before, during, and after execution of M&A priorities.

Ensure continuous patient safety and data privacy while delivering cyber resilience through a Zero Trust M&A security strategy.

Enforce prevention-focused, least-privilege access while performing continuous trust verification and continuous security inspection that exceed regulatory compliance requirements.

Customer Challenges

Merger and acquisition (M&A) strategies are driving growth, consolidation, and care efficiency optimizations within the healthcare industry. These M&A priorities are creating better patient care outcomes, improving care provider efficiencies, accelerating market growth, and helping reduce the cost of patient care. Healthcare delivery organizations (HDOs) merge or acquire other healthcare providers or services for a variety of reasons which can include strategic, financial, and operational factors.

When an HDO embarks on an M&A project, they face unique challenges due to the elaborate and interconnected nature of healthcare IT systems. These challenges make IT and security teams critical to successful integrations, and addressing these challenges requires careful planning through due diligence, strong leadership, effective communication, and engagement with all stakeholders involved in the Healthcare M&A process. Some of the common M&A challenges follow.

- **IT Systems Integration**—It is difficult to overstate the significance of integrating disparate healthcare IT systems. Electronic health records (EHRs), patient management systems, billing systems, and other specialized applications require data interoperability and seamless information exchange.
- **Infrastructure and Network Integration**—To consolidate and integrate different infrastructure components, HDOs must be able to assess network capacity, address compatibility issues, and establish a unified IT infrastructure—while maintaining system performance, reliability, and security.
- **Data Consolidation and Governance**—HDOs oversee massive amounts of sensitive data, ranging from protected health information, personally identifiable information, and credit card data to intellectual property. Merging healthcare entities need to consolidate their patient data from various sources and ensure consistent data governance practices. This involves identifying duplicate records, resolving data inconsistencies, establishing data quality controls, and developing new data governance policies and procedures.

- **Interoperability and Health Information Exchange**—Healthcare M&As may involve different EHR vendors or data exchange platforms. Achieving interoperability between these systems is crucial for seamless patient care. Ensuring data can be shared securely and effectively across merged entities, as well as external stakeholders, requires careful planning and coordination.
- **Cybersecurity and Data Privacy**—Assessing the security posture of merging organizations, conducting vulnerability assessments, implementing robust security measures, and developing a comprehensive cybersecurity strategy are critical for safeguarding patient data and preventing potential breaches.
- **Regulatory and Compliance**—Because the healthcare industry is heavily regulated, merging organizations must ensure compliance with healthcare laws, privacy regulations such as HIPAA, and potential antitrust regulations.
- **Clinical and Workforce Integration**—Integrating medical staff and practitioners along with non-clinical staff between the organizations ensures a smooth transition regarding roles, responsibilities, and access to data and applications from both organizations, all to deliver continuous patient care and facilitate ongoing integrations.
- **Patient Care Continuity**—HDOs need to ensure uninterrupted patient care and a seamless transition for patients. Care coordination, patient communications, and maintaining access to essential healthcare services are especially challenging during M&A activities.

COMMON PRE-M&A ARCHITECTURE

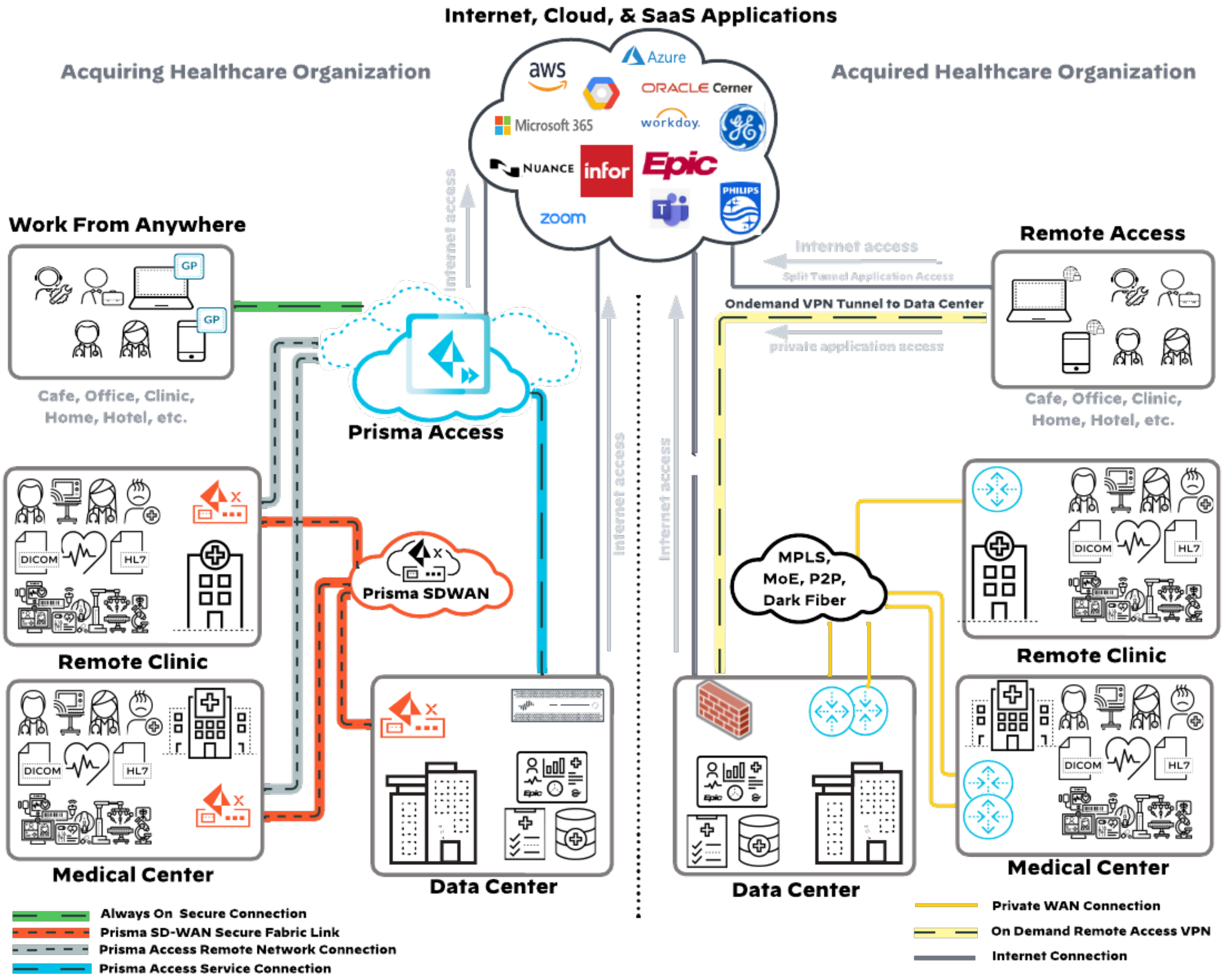
On the following page, Figure 1 shows the network architecture of two pre-merger HDOs. The right side of the diagram, under "Acquired Healthcare Organization," shows an architecture typical of an HDO that has not adopted a secure access service edge (SASE) strategy. SASE is a complete shift in network security philosophy that converges network and security functions into a single, cloud-delivered platform.

This network still uses a security stack that is entirely based in a data center. All traffic, for any type of access, must traverse this stack. This network design forces the following limitations on HDOs:

- Remote workers connect with a client-based VPN solution on-demand when they need to access applications and services, leaving them vulnerable when not connected.
- Remote clinics and medical centers rely on dedicated WAN circuits or site-to-site VPN connectivity for access to their application and services. When a singular connectivity path is impacted, care operations are disrupted until routing re-convergence or service restoration occurs.
- Most or all applications are hosted within their data centers.

All these limitations exacerbate the challenges described earlier.

Figure 1 Common HDO architectures for a SASE and non-SASE environment preparing for M&A


Internet, Cloud, & SaaS Applications
Acquiring Healthcare Organization
Acquired Healthcare Organization
aws
Azure
ORACLE Cerner
Microsoft 365
workday.
NUANCE
infor
Epic
PHILIPS
zoom
Work From Anywhere
GP
GP
Cafe, Office, Clinic, Home, Hotel, etc.
Internet access
Prisma Access
Remote Access
Internet access
Split Tunnel Application Access
Ondemand VPN Tunnel to Data Center
private application access
Cafe, Office, Clinic, Home, Hotel, etc.
DICOM
HL7
Remote Clinic
Prisma SDWAN
Internet access
Internet access
MPLS, MoE, P2P, Dark Fiber
DICOM
HL7
Remote Clinic
DICOM
HL7
Medical Center
Data Center
Data Center
DICOM
HL7
Medical Center
Always On Secure Connection
Prisma SD-WAN Secure Fabric Link
Prisma Access Remote Network Connection
Prisma Access Service Connection
Private WAN Connection
On Demand Remote Access VPN
Internet Connection

Palo Alto Networks Approach

On the left side of Figure 1, under "Acquiring Healthcare Organization," is the network of an HDO that has adopted a SASE architecture powered by Palo Alto Networks®. This architecture delivers an acquisition-ready architecture, enabling the acquiring HDO to be in an acquisition-ready state.

A SASE architecture enables the delivery of patient care from any location via an application fabric, enabling the healthcare workforce to access care delivery insights and data from anywhere, and provides the agility to host needed applications and services in data centers, in the public cloud environments, or consume them as a service safely and securely at all times and from all places.

SASE lowers administrative overhead, reduces security risk, enables agility for continuous digital innovation, and ensures availability of application, services, and medical devices so that healthcare providers can focus on what is truly important—patient care.

Palo Alto Networks delivers a comprehensive SASE solution that, along with our attack surface management (ASM) solution, helps healthcare IT organizations navigate M&A challenges, accelerate the time to value for the M&A, and streamline integration efforts required for operational success and patient care. The Palo Alto Networks solution allows your IT teams to prioritize the following:

- Data migration and system integration efforts.
- Smooth, disruption-free transition of care capabilities and services.
- Consistent enforcement of effective security standards.
- Continuous compliance with regulatory and other legal requirements.
- Management of the migration and integration timelines.
- Shifting access transparently to new applications services and datasets without any impact to clinical experience or patient care.

As the acquiring organization works through their M&A plan, they must decide which computing systems, applications, and services will be included in the post-merger IT environment. Additionally, they must determine the locations for devices and data across their data centers, cloud service providers and application hosting providers, and SaaS application providers.

With these decisions made, the IT team accelerates the integration of the acquired workforce, remote clinics, medical centers, and data center. Leveraging the acquisition-ready architecture enables safe, secure, and controllable interconnectivity unlocking many integration efficiencies.

Data centers, cloud providers, application hosting locations, and SaaS applications no longer needed can be decommissioned and transitioned out of service post-migration.

Duplicative SaaS applications can be migrated into a single tenant, and the other tenant can be decommissioned.

For remote clinics and medical centers of the acquired organization, the IT team can transition their use of Prisma® Access from connecting only to resources from the acquiring organization to either of the following:

- Relying on Prisma Access for all of their communications and connectivity to the internet, cloud service providers, SaaS applications, and new data center resources.
- Provided with a Prisma SD-WAN Ion appliance, to deliver site reliability and availability as well as control of applications and services. These on-premises appliances connect sites to the application fabric, enabling private healthcare applications to be routed over private secure paths to the data center. Patient guest and SaaS applications can be directed to Prisma Access for the most effective and secure path for these applications—without transporting to a data center security stack.

Finally, with the Palo Alto Networks solution in place, supporting the remote workforce of the acquired organization requires no further changes aside from security policy changes enabling access to the finalized, post-merger IT environment.

KEY SOLUTION ELEMENTS

The acquisition-ready Palo Alto Networks SASE architecture for HDOs is composed of several components, complemented by Cortex® Xpanse™ for attack surface management.

- **Prisma Access**—Prisma Access is a cloud-based security service that provides a full suite of security and inspection of traffic—without backhauling to an existing security perimeter or choke point.
    - **For Remote Networks**—Prisma Access connects medical centers and remote clinics to SaaS applications, cloud providers, and internet, including safe guest access.
    - **For Mobile Users**—Whether remote workers are at home, on the road, or on premises, Prisma Access secures and inspects connections to applications, services, devices, and data hosted by SaaS providers, cloud providers, data centers, business associates, and the internet.
- **Prisma SD-WAN**—This easily and rapidly deployed application-driven, next-generation software-defined WAN (SD-WAN) solution, ensures optimal access to devices, applications, and services within the healthcare infrastructure.
- **GlobalProtect®**—GlobalProtect is a lightweight, intelligent security connection agent that can be deployed to all workforce devices running Windows, Linux, MacOS, iOS, or Android operating systems. The GlobalProtect agent manages where and how to connect, ensuring optimal access to applications, services, devices, and data within the healthcare infrastructure, enabling a seamless remote access experience for the workforce.
- **ADEM**—Autonomous Digital Experience Management (ADEM) is an embedded monitoring platform that provides performance visibility from the viewpoint of your workforce. Whether from the perspective of a clinical or a non-clinical user, ADEM helps your IT team understand the user experience of accessing the applications and services needed—no matter where users are connecting or how they are accessing resources.
- **Cortex Xpanse**—The Palo Alto Networks ASM platform, Cortex Xpanse, is a critical aspect of building an acquisition-ready architecture because it improves due diligence on security posture before and after M&As. Cortex Xpanse continuously scans and indexes the entire internet and actively discovers your unknown risks in all connected systems and exposed services. Using supervised machine-learning models, it maps your attack surface and prioritizes remediation efforts—without manual analyst efforts. Instead of merely raising IT tickets, Cortex Xpanse leverages built-in automated playbooks to immediately reduce your attack surface risks.

SOLUTION SUMMARY

Using Cortex Xpanse and implementing the Palo Alto Networks SASE architecture within an HDO looking to drive M&A priorities (Acquiring Healthcare Organization) will greatly enhance an IT organization's ability to efficiently integrate in a safe and secure manner while reducing unnecessary risk exposure. It aims to ensure exceptional experience for the workforce, expanding care provider locations and potential care services and delivering an accelerated return on investment.

Benefits

BUSINESS VALUE

- **Accelerate Time-to-Value for M&A Investments**—Eliminate time consuming integration hurdles and accelerate the recognition of the anticipated M&A value gains.
- **Empower Clinical Care**—During the execution of M&A priorities, maximize connectivity, reliability, and security of delivering patient care.
- **Risk Insights**—Identify and understand the associated risk of your M&A priorities. Identify technical debt that you could be taking on, along with security risk exposure that you are not aware of or has not been disclosed.

OPERATIONAL VALUE

- **Simplify Integration and Operation**—Quickly establish secure and controlled connectivity enabling integrated care between both the acquiring and the acquired organization, accelerating patient care outcomes.
- **Seamless Workforce Integration**—Connect and ensure the experience of the acquired workforce to all applications, services, and data needed without placing the burden on the workforce to know where and how to access what they need.
- **Safe Infrastructure Interconnection**—Onboard M&A remote clinical and medical center locations and their data center and hosting locations quickly and securely, without increasing the risk or sacrificing compliance requirements.

SECURITY VALUE

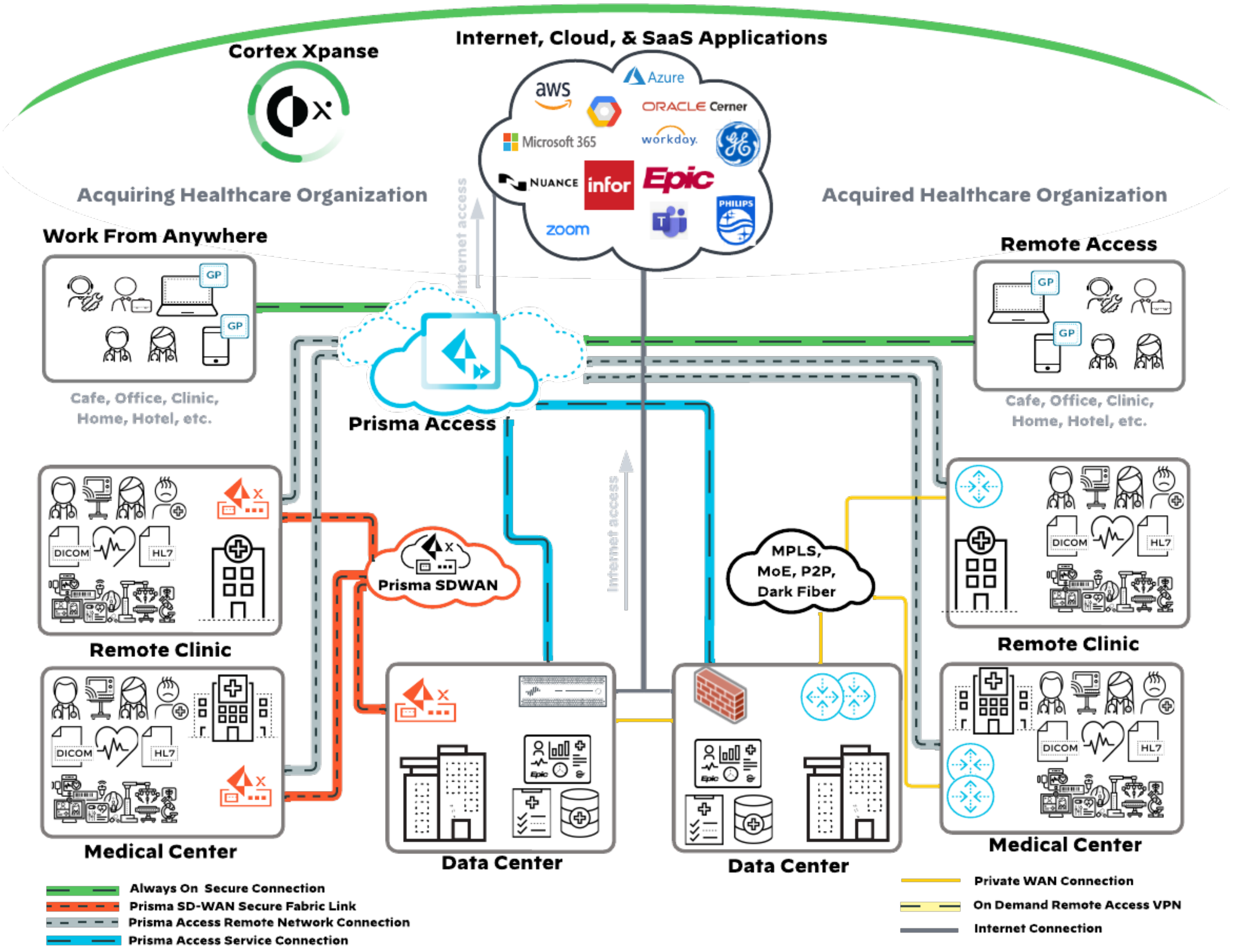
- **Increase Visibility and Insights**—Gain outside in and operational visibility, insights, and context, to be able to protect all connected medical devices, clinical applications, and services impacting patient safety, and improve data security while minimizing disruptions to the care operations.
- **Consistent and Comprehensive Protections**—Maintain a zero-trust security prevention strategy during the entire M&A process at scale and protect all applications, services, data, users, and connected devices regardless of which organization they belong to, while eliminating accidental exposure of systems and services to the internet and bad actors.
- **Continued Regulatory Compliance**—Help ensure continuous compliance requirements such as HIPAA and PCI-DSS are met or exceeded during the M&A process, while enforcing consistent security everywhere and automating prevention, detection, and response workflows.

Actual Customer Implementation

HDOs that have adopted a Palo Alto Networks SASE architecture and Cortex Xpanse have an acquisition-ready architecture. This enables their IT and security teams to become an enabler of quick, efficient, and successful M&A priorities, unlocking the value of the post-M&A entity. This acquisition-ready architecture provides IT teams with the infrastructure visibility, insights, and controls needed to accelerate the integration process.

The following interconnectivity implementation steps are typical of HDOs IT teams facing M&A activities. Figure 2 highlights the connections within the combined architecture of the acquiring and acquired organization.

Figure 2 Palo Alto Networks SASE and Cortex solutions safely accelerate mergers and acquisitions


Cortex Xpanse
Internet, Cloud, & SaaS Applications
aws
Azure
ORACLE Cerner
Microsoft 365
workday.
NUANCE
infor
Epic
PHILIPS
zoom
Acquiring Healthcare Organization
Acquired Healthcare Organization
Work From Anywhere
GP
Cafe, Office, Clinic, Home, Hotel, etc.
Internet access
Prisma Access
Remote Access
Cafe, Office, Clinic, Home, Hotel, etc.
Internet access
DICOM
HL7
Remote Clinic
Prisma SDWAN
MPLS, MoE, P2P, Dark Fiber
Remote Clinic
Medical Center
Data Center
Data Center
Medical Center
Always On Secure Connection
Prisma SD-WAN Secure Fabric Link
Prisma Access Remote Network Connection
Prisma Access Service Connection
Private WAN Connection
On Demand Remote Access VPN
Internet Connection

IMPLEMENTATION OVERVIEW

1. Start by expanding Cortex Xpanse beyond actively monitoring the acquiring organization to understand the connected systems and exposed services of the acquired organization (right side of Figure 2). This continuous real-time assessment helps to deliver comprehensive insights regarding the acquired organization's infrastructure and internet-connected systems and to expose potential hidden risks. Leverage these insights to accelerate your integration planning, reduce high-risk security impacts, and prioritize data migration and system integration efforts.

2. Onboard the acquired organization's applications, services, and data hosted within their data centers and cloud service providers to the Prisma Access infrastructure via service connections (blue dashed lines in Figure 2 from the data centers to Prisma Access). This is non-disruptive and provides safe and secure access for the acquiring organization (left side of Figure 2) to access and understand the systems, applications, and data hosted within the acquired organizations.

   Prisma Access provides comprehensive visibility and utilization along with security policy enforcement control access and continuous security inspection of the communications. For direct data-center-to-data-center communications, it may be necessary to build a dedicated connection between the data centers terminated on wide-area network focused Palo Alto Network Next Generation Firewalls (NGFWs), if large volumes of data transfers and synchronizations are required or expected between the data center resources.

3. Roll out GlobalProtect client to the acquired organization's remote workforce. This will enable the remote workforce of the acquired organization access to both their existing applications, services and data resources and the added resources of the acquiring organization safely and securely via Prisma Access (green dashed lines in Figure 2 from the remote access workers to Prisma Access). This makes for an easy training, transition, and experience for the acquired workforce to have connectivity to their legacy resources and added resources during the M&A transition while maintaining the acquiring organization's security posture standards with visibility, access controls, and security inspection.

4. Onboard the acquired organization's remote clinics and medical centers to Prisma Access via standard IPsec tunnels to existing networking gear (routers, firewalls, SD-WAN devices) deployed at the remote clinic and medical center locations (gray dashed lines in figure 2 from the remote clinics and medical centers to Prisma Access). This will enable the same dual access as previously mentioned above for the remote workers, but now for all medical center and remote clinic workers with the same security visibility, controls, and inspection.

With safe, secure, and controllable interconnectivity established with Prisma Access, the IT team has the visibility and control to fully understand all connectivity, communications, utilization of systems, applications, services, and data by the acquired organization.

Palo Alto Networks SASE architecture and the Cortex Xpanse platform accelerates the achievement of the acquiring HDO's M&A priorities by enabling the following:

- Supercharging discovery and insights for the acquired organization.
- Removing extraneous planning burden of how to interconnect the M&A organizations.

- Removing from the critical path the lead times for standard infrastructure equipment ordering and deployment, without sacrificing access or increasing security risk.
- Providing the acquiring organization a better assessment of and insights into the reality of the acquired organization's IT systems, applications, services, devices, and data for migration and integration planning.
- Enhancing the experience of the acquired workforce and medical practitioners through minimizing the changes and disruption to their workflows during the M&A transition.
- Helping ensure compliance with regulatory requirements.
- Maintaining zero trust cybersecurity and data privacy standards.

For More Information

To explore more about how you can be prepared for your next merger or acquisition and seamlessly integrate into your existing digital landscape safely and securely, please contact your Palo Alto Networks account team or partner.

Additional information regarding Palo Alto Networks healthcare solutions can be found on the **Palo Alto Networks Healthcare Industry** page.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com