BANYAN SECURITY

SOLUTION BRIEF

Revolutionizing Healthcare Cybersecurity with Banyan Security SSE

Introduction

In the ever-evolving world of healthcare, where patient data is both a treasure and a target, cybersecurity remains a constant and pressing concern.

Healthcare organizations are entrusted with not only safeguarding sensitive patient information but also facilitating the seamless flow of data among a diverse array of users, including in-house healthcare professionals, contractors, and remote staff. As the digital landscape advances, the need for modernizing existing network infrastructures becomes increasingly evident. In this context, the convergence of two transformative technologies, Security Service Edge (SSE) and Zero Trust Network Access (ZTNA), offers a promising path forward.

Let's explore the cybersecurity challenges that healthcare organizations face, particularly those with a range of user types, and delve into how embracing SSE and ZTNA can fortify their defenses while enabling more secure and efficient healthcare access.

The Healthcare Cybersecurity Challenge:

Healthcare organizations deal with a unique set of cybersecurity concerns:

- **Patient Data Privacy:** Protecting patient health records and Personally Identifiable Information (PII) from unauthorized access is essential to comply with regulations like HIPAA.
- **Data Breaches:** Healthcare organizations are vulnerable to data breaches that can lead to financial losses and reputational damage.
- **Ransomware Threats:** The healthcare sector is frequently targeted by ransomware attacks that can disrupt critical services.
- **Vendor and Third-Party Risks:** Managing secure access for contractors and third-party service providers is a complex undertaking.
- **Remote Access Challenges:** Telemedicine and remote work require robust security measures for remote access to healthcare systems and patient data.

Why Banyan Security

Banyan Security is one of the only security vendors that provides a complete range of connection options for all stakeholders, employees and contractors that engage with the healthcare ecosystem. This includes corporate and personal-owned devices that are prevalent in healthcare, as well as managed and unmanaged systems.

- Client for mobile and desktop
- Clientless
  - Chromium Browser Extension
  - Unregistered Device Support
  - Device Manager Integration

Banyan's Chrome Extension is a lightweight browser extension that can be installed, without elevated or administrator privileges, in Chromium-based browsers (such as Google Chrome, Microsoft Edge, etc). This allows end-users to access Hosted Websites and SaaS Applications secured with Banyan.

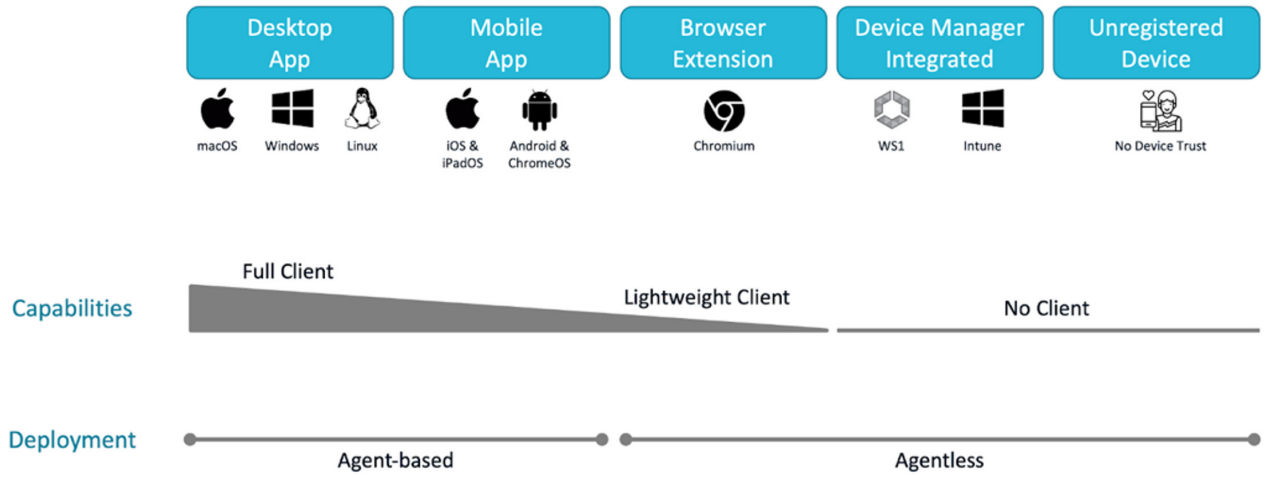
Our unregistered device functionality allows users with unmanaged and unregistered devices to have access in seconds. The authentication does not require certificates and Device Trust functionality is not supported. The functionality works by white-listing (allow-listing) a device based on IP address or CIDR. Typically, unregistered device access is used for one-time access or as a temporary solution prior to onboarding or enrolling a device.

The healthcare industry accounts for 20% of all publicly reported data breaches, making it the most vulnerable to cyberattacks, ahead of the public sector (16%), technology (11%), education (9%), and professional services (6%).

(Source: Persona)

Another option leverages a Device Manager. This is ideal for users that don't want to bother with manual enrollment. This allows a certificate to be pushed out to the device. Since passwordless access feeds a frictionless user experience, this certificate can imbed device and identity information to enable Passwordless authentication and Device Trust.

Client and Clientless Deployment Options



Along with inbound connectivity, Banyan Security provides outbound controls to enable Acceptable Use Policy (AUP), malware and phishing protection. With Internet Threat Protection (ITP), administrators can easily create policies for different users and groups. Executives and medical staff may be able to go to any site while the operators updating appointments may only visit web applications needed to fulfill their role.

ITP allows broad category filtering along with allow-list creation. Categories are continuously uploaded and new domains are added as soon as they are live, without needing to make configuration changes.

In 2022, there were 707 publicly disclosed data breaches among healthcare firms.

(Source: Persona)

Key Benefits

- **Enhanced Security:** Banyan Security's ZTNA ensures that only authorized users access healthcare systems, significantly reducing the risk of insider threats and unauthorized access.
- **Regulatory Compliance:** Banyan Security helps healthcare organizations maintain compliance with regulations like HIPAA, GDPR, and more.
- **Resilience Against Ransomware:** By implementing a Zero Trust model, healthcare organizations can fortify their defenses against ransomware attacks
- **Streamlined Remote Access:** With SSE, remote healthcare professionals enjoy secure and efficient access to resources, facilitating telemedicine and remote work.

Customers may want to work with Banyan Security for several compelling reasons:

1. **Enhanced Security:** Banyan Security specializes in Zero Trust Network Access (ZTNA) and Security Service Edge (SSE) technologies, which provide robust and granular access controls. By working with Banyan Security, customers can significantly enhance the security of their networks, systems, and data.

2. **Zero Trust Expertise:** Banyan Security is a recognized leader in the implementation of the Zero Trust security model, which is increasingly crucial in today's threat landscape. Customers can benefit from Banyan's expertise in designing and deploying Zero Trust architectures to protect against insider threats and external attacks.

3. **Compliance and Regulatory Alignment:** For customers in regulated industries like healthcare, finance, and government, Banyan Security can help ensure compliance with industry-specific regulations such as HIPAA, GDPR, and more. Their solutions are designed to align with these stringent requirements.

4. **Improved User Experience:** Banyan Security's solutions are not just about security; they also focus on delivering a seamless user experience. Customers can enjoy secure, efficient access to the resources they need, whether in the office or working remotely.

5. **Flexibility and Scalability:** Banyan Security's solutions are designed to be flexible and scalable, allowing organizations to adapt to changing business needs and accommodate growth seamlessly. This adaptability is particularly valuable for businesses experiencing rapid expansion or transformation.

6. **Protection Against Ransomware:** Banyan Security's Zero Trust approach can help protect customers from ransomware attacks by ensuring that even trusted users and devices are continually verified and authenticated before gaining access to sensitive resources.

7. **Vendor and Third-Party Access Management:** Banyan Security's solutions are well-suited for managing secure access for vendors, contractors, and third-party service providers. This capability simplifies access management and reduces security risks associated with external entities.

8. **Ease of Integration:** Banyan Security's solutions can often integrate with existing network infrastructures and technologies, minimizing disruption and making the transition to a more secure access model smoother.

9. **Continuous Innovation:** Banyan Security is dedicated to staying at the forefront of cybersecurity innovation. Customers can benefit from access to the latest security technologies and strategies as the threat landscape evolves.

10. **Peace of Mind:** By partnering with Banyan Security, customers can have peace of mind knowing that they have a trusted partner working alongside them to proactively address cybersecurity challenges and protect their digital assets.

What About HIPAA?

Banyan Security can assist healthcare organizations in complying with the Health Insurance Portability and Accountability Act (HIPAA) through its Zero Trust Network Access (ZTNA) and Security Service Edge (SSE) solutions. Here's how Banyan Security helps with HIPAA compliance:

The average cost of a healthcare data breach is $7.13 million.

(Source: Ponemon Institute)

1. **Data Encryption:** Banyan Security ensures that all data in transit is encrypted. HIPAA requires the encryption of patient data to protect it from unauthorized access during transmission. By encrypting data, Banyan Security helps healthcare organizations meet this HIPAA requirement.

2. **Access Control:** HIPAA mandates that only authorized personnel should have access to patient health records and sensitive data. Banyan Security's ZTNA solutions enforce granular access controls, ensuring that only authorized users, devices, and applications can access sensitive healthcare data.

3. **Continuous Authentication:** HIPAA requires organizations to implement mechanisms for verifying the identity of users accessing patient data. Banyan Security's Zero Trust model verifies user identities continuously, even after initial authentication, providing a higher level of security and meeting HIPAA's authentication requirements.

4. **Auditing and Monitoring:** HIPAA requires healthcare organizations to maintain logs and audit trails of system activity. Banyan Security's solutions provide detailed logs of access attempts and activities, helping organizations monitor and audit access to patient data effectively.

5. **Vendor and Third-Party Access Control:** HIPAA extends its requirements to third-party vendors and contractors who have access to patient data. Banyan Security enables healthcare organizations to manage and secure the access of third-party entities, ensuring that they also comply with HIPAA regulations.

6. **Zero Trust Principles:** Banyan Security's Zero Trust approach aligns with the principles of least privilege access, where users are only granted the access they need to perform their job functions. This helps healthcare organizations adhere to the "Minimum Necessary Standard" requirement under HIPAA.

7. **Secure Remote Access:** With the increasing need for remote work and telemedicine, Banyan Security's solutions provide secure remote access to healthcare systems, allowing healthcare professionals to access patient data securely from anywhere while meeting HIPAA security standards.

8. **Incident Response and Breach Detection:** HIPAA mandates that healthcare organizations have a robust incident response plan. Banyan Security's solutions can aid in the early detection of security incidents, helping organizations respond swiftly to potential breaches and minimize their impact.
9. **Compliance Reporting:** Banyan Security offers reporting and auditing capabilities that can assist healthcare organizations in demonstrating HIPAA compliance to auditors and regulatory bodies.

By implementing Banyan Security's ZTNA and SSE solutions, healthcare organizations can strengthen their cybersecurity posture, meet HIPAA requirements, protect patient data, and minimize the risk of data breaches and associated penalties. This proactive approach to security aligns with the overarching goal of safeguarding patient privacy and ensuring the integrity and availability of healthcare systems and data.

Conclusion

Banyan Security's innovative ZTNA and SSE technologies provide healthcare organizations with the tools they need to revolutionize their cybersecurity infrastructure. By embracing a Zero Trust model and ensuring secure access to cloud services, healthcare organizations can protect patient data, maintain compliance, and adapt to the evolving digital healthcare landscape confidently. With Banyan Security, healthcare cybersecurity becomes a strategic asset, enabling secure, agile, and compliant healthcare operations.

Contact Banyan Security today to embark on a transformative journey towards a more secure healthcare future.

About Banyan Security

Banyan Security provides secure, zero trust "work from anywhere" access to applications and resources for employees and third parties while protecting them from being phished, straying onto malicious web sites, or being exposed to ransomware. A Flexible Edge architecture enables rapid, incremental deployment on-premises or in the cloud without compromising privacy or data sovereignty. A unique device-centric approach intelligently routes traffic for optimal performance and security delivering a great end user experience. Banyan Security protects workers across multiple industries, including finance, healthcare, manufacturing, and technology. To learn more, visit www.banyansecurity.io or follow us on Twitter at @BanyanSecurity.

BANYAN SECURITY

info@banyansecurity.io | +1 415-289-9414 | www.banyansecurity.io