everlast.

Everlast Networks Technical Whitepaper

Creating sovereign & trusted communications that can withstand the future.

Everlast Networks 2024

This page intentionally left blank.

Contents

Changes and Updates

28th September 2024: Initial document creation.
10th March 2025: Document updated for worldwide publication.

Executive Summary

Everlast Networks, since late 2022, has been researching and developing a new methodology to connect systems over existing computer network standards that is hands-off, low-to-zero latency, compatible with multiple infrastructures, and future proof.

This R&D venture was successful in mid-2024 upon testing and completion of our new networking methodology, which is now in refinement and market implementation stages.

Executive technical specifications

Client

Application language	Memory safe (Compiled Python + Go, sys calls)
Application signing	Everlast Networks or Customer.
System processes	DNS, Conn Manager, IPSec Driver, front-end [optional component].
IPSec	System/Kernel default, non-modified.
CPU load	< 1% load with established stream anticipated.
Architectures	Amd64, Arm64, RISC-V
Handshake	Conventional - single-use + pinned certs.
Routing	Kernel-based + installed in-memory

Server

Registration	Server register/validate + client pass-through.
OS	Linux
Environments	Cloud, Edge, DC, offline point to point.
Handshake	Conventional single-use to verify connecting client.

Connection

Rekeys (tunnel uplink)	5 minutes
Rekeys (comms stream)	60-120 seconds
Tunnel	NIST ML-KEM 1024 (FIPS 203 standard).
Stream	Conventional for rapid rekeys & failover. PQC stream optional.
Tested uplinks	Ethernet, Wi-Fi, Fiber Optic, Cellular (4/5G), Satellite (incl. StarLink, LEO, HEO, GEO), and RF (IP over microwave/millimetre link & line of sight)

Foreword

The world of cyber-security is becoming increasingly complicated and sophisticated, as the rapid development of artificial intelligence and increased modern-warfare doctrine by hostile foreign state-actors pose a threat to critical infrastructure, public and private sector data security, national security, defence capability, and our security capacity.

Through our extensive stakeholder consultation (particularly with those in the spheres of critical infrastructure, digital service, and defence contractors), we have come to understand the constant readiness and security threats to which they find themselves subjected to. These factors pose significant financial, operational, technical, and data sovereignty challenges.

As is the case for a bank vault for its analogue counterparts, it is often simpler to secure digital property at its point of storage, and indeed there are *many* service providers which specialise in providing secure storage solutions for **data at rest**. Yet - it is the case that both physical goods and digital information are inherently more at risk of being compromised when being transported or communicated.

Existing market offerings (such as VPN's and retail zero-trust providers) are fundamentally insufficient for our stakeholders, as "off-the-shelf" options such as these all involve sacrificing data sovereignty through third-party processing of some capacity, and involve rendering the parties as susceptible to potential interception through network exposure. They are also often impractical to implement into existing systems without tolerating vulnerabilities and operational compromise.

It is here, in securing **data in transit**, that we have found a significant niche in market capability; further, we have developed what we feel is an elegant solution. EverGuard™, our attack-resistant zero-trust communications protocol, comprehensively secures data throughout the transmission process through single-use connections that utilise next-generation post-quantum algorithms.

Our technology facilitates data communication by way of proxy, meaning the actual parties themselves are shrouded from exposure. Furthermore, our leading-edge encryption almost-constantly tests and re-verifies the legitimacy of the connection to avoid third-party penetration.

This patented technology has wide-spread applications in IoT environments, remote fleet management, critical infrastructure, government sectors, and defence contexts, accessible, cost-effective, and capable of being integrated within existing networks as already deployed, and available right now.

We are excited to bring this product to market, to revolutionise this space and to restore trust for the world of advanced cyber-security.

The Everlast Team.

Chapter 1: Increasing Importance

The importance of robust security and privacy practices cannot be overstated.

As the number of connected devices grows exponentially, vast amounts of data are generated, transmitted, and stored globally every second. This surge has driven unprecedented innovation and growth across various sectors, but has also exposed significant vulnerabilities that can be exploited by malicious actors. These risks extend to individuals, businesses, governments, and even national security.

Cyber-attacks are increasingly recognised as a critical global risk, surpassing even natural disasters in some areas, according to the World Economic Forum. The growing frequency and sophistication of these attacks highlight the inadequacies of our current systems, where outdated encryption methods and poor security practices are all too common (*World Economic Forum, 2023*).

The digital transformation of critical infrastructure, including utilities, telecommunications, and government sectors, has raised the stakes even further. As these systems become more interconnected, the potential for catastrophic failures due to security breaches grows significantly. A stark example of this was the 2021 Colonial Pipeline ransomware attack in the United States, which disrupted fuel supplies across the East Coast, showing the devastating consequences of compromised critical infrastructure (*Colonial Pipeline: What We Know and How to Protect Against Future Attacks, 2021*).

At the same time, consumer privacy awareness has reached unprecedented levels, with the public becoming increasingly concerned about how their data is being protected. The proliferation of personal data collection, coupled with high-profile data breaches, has sparked a growing demand for stronger privacy protections.

Legislative measures such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) reflect this shift towards prioritising user privacy and holding organisations accountable for safeguarding personal information, however despite these regulatory advancements, the implementation of effective privacy protections remains inconsistent, leaving many individuals vulnerable to data misuse (*The GDPR and CCPA: The Impact on Data Privacy, 2022*).

The urgency for advanced security and privacy measures is greater than ever. Traditional methods, while essential, are no longer sufficient to meet the evolving threat landscape. There is a clear need for innovative solutions that can adapt to the complexities of modern digital environments and provide comprehensive protection against a broad spectrum of threats going forwards. As our reliance on digital technologies deepens, ensuring the security and privacy of our data and infrastructure will be crucial to maintaining trust and enabling continued progress.

Chapter 2: Consequences of Insufficient Security

The consequences of insufficient encryption in modern digital and physical infrastructures are potentially catastrophic, with significant implications for privacy, financial stability, and national security. Inadequate encryption leaves systems vulnerable to unauthorised access, resulting in data breaches, operational disruptions, and in some cases, physical damage to critical infrastructure – and that's before we get to operational risk to government and defence sectors.

Damages to infrastructure

In Australia, significant infrastructure attacks in recent years highlight the critical need for robust encryption. The 2023 DP World hack disrupted port operations nationwide, bringing essential shipping and logistics activities to a standstill. The attack on DP World's IT systems halted operations at four major Australian ports, severely impacting supply chains and underscoring the vulnerability of critical infrastructure to cyber threats. The breach illustrated the risks associated with insufficient encryption and cybersecurity measures in protecting national supply chains and essential services (*Clark, 2023*).

Another notable example is the 2021 Colonial Pipeline cyberattack in the United States, where the DarkSide ransomware group targeted the pipeline's IT infrastructure, leading to a shutdown that disrupted nearly half of the East Coast's fuel supply. The company paid a $4.4 million ransom, underscoring the severe impact that cyberattacks on poorly secured systems can have on critical infrastructure (*CISA, 2021*).

Damages to personal data

In terms of data breaches, the 2017 Equifax incident remains one of the most severe, with attackers exploiting inadequate encryption and security measures to access the personal data of 147 million individuals. The breach compromised social security numbers, birth dates, and addresses, resulting in significant financial penalties for Equifax, including a $700 million settlement with the Federal Trade Commission (*FTC, 2019*).

The healthcare sector has also faced severe consequences due to inadequate encryption. The 2015 Anthem breach exposed the personal data of nearly 80 million people, including names, birth dates, and medical identification numbers. This breach, resulting from a poorly secured database, demonstrated the vulnerability of sensitive health information to cyberattacks, leading to widespread identity theft and fraud (*Office for Civil Rights, 2016*).

These examples demonstrate the severe consequences of insufficient encryption, not only in terms of financial losses and privacy violations but also in the potential for physical harm and environmental damage – and typically have one dangerous mixture in common – an exposed endpoint or system, and human error.

Thus, one can see that as cyber threats continue to evolve, the demand for robust, scalable, and adaptive encryption solutions has never been more critical. Failing to adequately protect sensitive data and critical systems can lead to devastating outcomes, reinforcing the urgent need for innovation in encryption technologies.

Chapter 3: Current Methods and Challenges

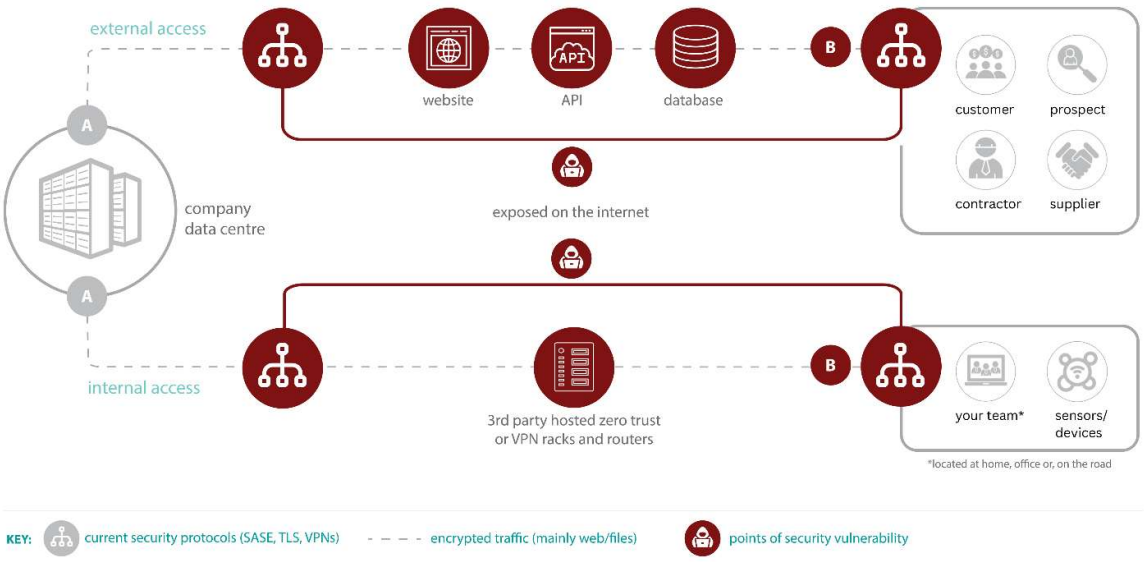
Current organisational security predominantly relies on SSL/TLS protocols, VPNs, and third-party-hosted Zero Trust Network Access (ZTNA) solutions, which form the backbone of secure communication across networks and the internet. SSL/TLS is widely adopted for securing web traffic, while self-hosted VPNs like OpenVPN and WireGuard are commonly used for secure remote access by organisations of all sizes. Zero Trust has emerged as the pinnacle of secure network and remote access; however, it is noteworthy that approximately 98% of Zero Trust traffic is hosted by third-party providers, raising concerns about data sovereignty and control (*Brooks, 2023*).

Adoption rates of these encryption strategies vary significantly across industries, too. For example, the Internet of Things (IoT) sector, known for its low-power devices, is often criticised for poor encryption practices, with less than 15% of IoT devices utilising any form of encryption (*Zscaler, 2023*). In Critical Infrastructure (CI) sectors, vital to national security, the adoption of robust encryption remains insufficient, with only around 30% of systems employing adequate encryption methods (*IoT For All, 2023*).

Interviews and surveys we conducted with companies in the IoT space (including Operational Technology (OT), Critical Infrastructure (CI), Smart Cities, and Utilities) revealed common challenges: lack of computational power, scalability issues with existing technology, and the high cost per device were prevalent obstacles in securing their networks. However, many companies indicated that when IoT devices were networked, a single point, such as a router or server, could effectively handle encryption as a local concentrator for connected low-power devices.

Further discussions with Internet Service Providers (ISPs), Managed Service Providers (MSPs), and technology companies, including those serving government and defence sectors, highlighted similar concerns with existing solutions. VPNs, for example, require manual configuration on each device, becoming increasingly cumbersome as the number of devices grows within enterprise and IoT environments. Although WireGuard was suggested as more scalable due to the option to automate config file creation, there is significant risk associated with these credentials being stolen or hijacked from devices (*Wired, 2023*), allowing instant unauthorised access to other devices and resources on the internal network.

Ultimately in culmination, these issues could be outlined in a simple diagram showing internet connected devices, devices, and networks are the root of compromise:



The complexity of onboarding large fleets of devices and maintaining their connections also emerged as a significant challenge. IoT vendors reported rising costs associated with sending staff out daily to reset VPN connections on critical infrastructure that had gone offline.

When exploring the option of outsourcing these functions using "Zero Trust Network Access" (ZTNA) products, we discovered substantial risks - these solutions often require integration with third-party providers to handle data, which introduces vulnerabilities and trust issues. Third-party providers typically have access to decrypted data internally, posing a major security risk if the provider's security is compromised, and account compromise risks are high, potentially allowing malicious users or the third party itself to modify devices, including the ability to shut down accounts (*Brooks, 2023*). Further, companies and organisations that have a requirement to use their own infrastructure, which is common in CI Gov and Defence industries, **cannot** route extremely sensitive data over a third party.

Recent high-profile domestic breaches, such as the Optus and Medibank hacks, have starkly highlighted the vulnerabilities associated with the handling of encrypted data by third-party providers (*Australian Financial Review, 2023)*. These incidents serve as compelling case studies illustrating why third-party encryption is far from ideal, especially for organisations operating within critical infrastructure sectors. The security risks are amplified when encryption and data management are outsourced, leaving sensitive information exposed to potential breaches.

Moreover, contemporary attack vectors (including insecure applications, databases, APIs, MFA spamming, credential theft, and social engineering) often exploit weaknesses that existing encryption methods are intended to protect against. Despite the theoretical robustness of these methods, their real-world effectiveness is frequently compromised due to improper implementation or human error, rendering them ineffective in practice (*Verizon, 2023*).

The challenges of scalability, reliance on third parties, costs in licensing and ongoing maintenance, and the continuously evolving tactics of cybercriminals underscore the pressing need for more robust and adaptable cybersecurity solutions – and without so, we are going to see more regular, and impactful, breaches.

Chapter 4: Creating better security.

The evaluation of existing encryption methodologies and the associated challenges underscores the pressing need for a more effective and adaptable cybersecurity solution. Through extensive consultations with industry experts across various sectors, including IoT, critical infrastructure, telecommunications, and government services, it has become increasingly clear that the existing solutions are inadequate to address the growing complexities and threats posed by contemporary cyberattacks.

The IoT and critical infrastructure sectors are confronted with unique challenges due to their reliance on legacy systems and often outdated security protocols. These sectors have been identified as having some of the lowest adoption rates of advanced encryption technologies, largely due to the perceived difficulty and costs associated with implementing these solutions (*Gartner, 2023*). The rise of state-sponsored attacks and sophisticated hacking groups has further exposed the vulnerabilities in current security frameworks, highlighting the urgent need for a novel approach to cybersecurity (*Mandiant, 2023*).

Our findings

In response to these findings, our discussions with industry leaders have reinforced the need for a solution that is not only robust and secure but also scalable, cost-effective, and easily integrated into existing infrastructure. The feedback from these engagements consistently points to several key requirements for an effective solution:

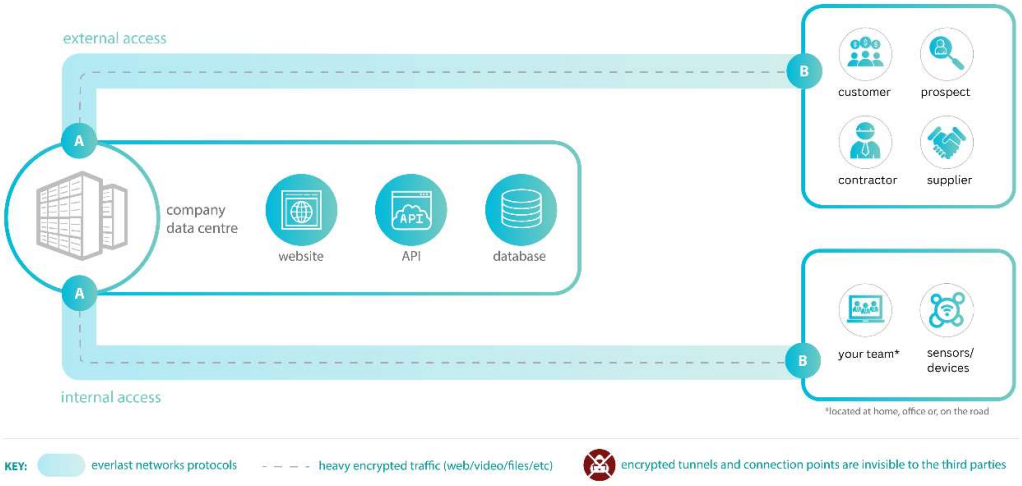
1. **Affordability:** The high costs associated with traditional cybersecurity solutions, particularly those involving third-party zero-trust networks, have been a significant barrier to widespread adoption, especially among small to medium enterprises (SMEs). An affordable solution is crucial for broader adoption, ensuring that even smaller entities can protect their systems against sophisticated threats (*IDC, 2023*).

2. **Enhanced Features for Service Providers:** Service providers, including managed service providers (MSPs), have expressed the need for additional features that would allow them to offer more comprehensive security services to their clients. This includes capabilities for monitoring and managing security across multiple client environments without compromising the security of the underlying infrastructure (*Frost & Sullivan, 2023*).

3. **Device Agnosticism and Scalability:** A recurring theme from our discussions was the necessity for a device-agnostic and scalable solution. Companies emphasised the importance of a system that could be deployed across a diverse range of devices, from IoT sensors to enterprise servers, without requiring significant modifications to existing hardware or software. Scalability is equally critical, facilitating the seamless onboarding of devices, whether a single unit or tens of thousands (*Forrester, 2023*).

4. **Customisability and API Integration:** Enterprises have highlighted the importance of a solution that can be integrated into their existing infrastructure via APIs, allowing for customisation and the development of middleware tailored to their specific needs. This flexibility enables organisations to maintain control over their data and security protocols, ensuring compliance with internal policies and regulatory requirements (*Gartner, 2023*).
5. **Licensing and UUID Generation:** To address concerns around scalability and management, our proposed solution incorporates features such as UUID generation for each device, ensuring unique identification and secure management. Additionally, a flexible licensing model that scales with the size of the deployment has been identified as crucial to meeting the diverse needs of different industries (*IDC, 2023*).
6. **Futureproofing**: While it's certainly hard to predict the capabilities and capacities of state-based attackers and agents, we can take steps to ensure that:
    1. **Our connections are hard to detect and identify** by installing the routes using existing standards but entirely in memory and not as a virtual network device;
    2. **Data in transit is hard to capture** by means of rapidly rekeying on the fly with no discernible transaction to the end user or device;
    3. **Captured data is hard to decrypt** by means of making it exponentially expensive and harder to decrypt a stream of data.

With these identified needs in mind, we started developing and actively validating a new communications security technology designed to comprehensively address these challenges. **EverGuard** aims to provide an affordable, scalable, and highly secure alternative to current methods for remote systems access, or point to point secure networking, with the flexibility to integrate seamlessly into a wide range of industries and applications.



Conclusion

The increasing sophistication of cyber threats, coupled with the expansion of IoT devices and the growing reliance on digital networks within critical infrastructure, demands a significant evolution in the approach to cybersecurity. Current market offerings, while effective in certain capacities, fail to address the complex and evolving challenges posed by modern cyber threats. The limitations of existing solutions, including VPNs, SSL/TLS protocols, and third-party-hosted Zero Trust Network Access (ZTNA) systems, have been exposed through various high-profile breaches, underscoring the need for a more robust, scalable, and adaptable approach to data security.

Our research and industry consultations have made it clear that there is a critical need for innovative solutions that not only meet today's security demands but also anticipate the challenges of tomorrow. **EverGuard™**, our zero-trust communications protocol, is our response to this need. By leveraging cutting-edge post-quantum encryption technologies and a zero-touch, zero-trust architecture, we'll be offering a unique solution that secures data in transit, and hides endpoints.

This approach is not only innovative but necessary. As the world becomes more connected, and as cyber threats continue to evolve, organisations must rethink their security strategies. Traditional methods are no longer sufficient, and the consequences of failing to adapt are significant, as evidenced by recent cyberattacks on critical infrastructure and data breaches affecting millions of individuals.

We invite all stakeholders, including CISOs, IT managers, and business leaders, to reflect on their current security practices and consider how our technology could be integrated into their existing strategies to provide comprehensive protection against current and future threats. By embracing a more secure, scalable, and adaptable approach to cybersecurity, organisations can better protect their assets, data, and infrastructure, ensuring they remain resilient in the face of an increasingly hostile digital landscape.

In conclusion, the necessity for advanced encryption and cybersecurity solutions is clear. We will be shortly offering an accessible, affordable, and powerful solution that addresses the shortcomings of current technologies.

References

Chapter 1

1. World Economic Forum (2023). Global Risks Report 2023. Retrieved from https://www.weforum.org/reports/global-risks-report-2023
2. Colonial Pipeline: What We Know and How to Protect Against Future Attacks. (2021). Cybersecurity & Infrastructure Security Agency (CISA). Retrieved from https://www.cisa.gov/news/2021/05/10/colonial-pipeline-what-we-know-and-how-protect-against-future-attacks
3. The GDPR and CCPA: The Impact on Data Privacy. (2022). International Association of Privacy Professionals (IAPP). Retrieved from https://iapp.org/resources/article/the-gdpr-and-ccpa-the-impact-on-data-privacy/

Chapter 2

1. Brooks, C. (2023). "Zero Trust Network Access Is Here: What You Need to Know" *Forbes*. Retrieved from: https://www.forbes.com/sites/chuckbrooks/2023/06/05/zero-trust-network-access-is-here-what-you-need-to-know/
2. Zscaler. (2023). "State of Zero Trust 2023" *Zscaler*. Retrieved from: https://www.zscaler.com/resources/security-research/state-of-zero-trust-2023.pdf
3. IoT For All. (2023). "Security Concerns in IoT Devices" *IoT For All*. Retrieved from: https://www.iotforall.com/security-concerns-iot-devices
4. Grand View Research. (2023). "Virtual Private Network (VPN) Market Size, Share & Trends Analysis Report" *Grand View Research*. Retrieved from: https://www.grandviewresearch.com/industry-analysis/virtual-private-network-vpn-market
5. MarketsandMarkets. (2023). "Firewall Security Market". Retrieved from: https://www.marketsandmarkets.com/Market-Reports/firewall-security-market-68569239.html
6. Market Research Future. (2023). "Zero Trust Security Market Research Report". Retrieved from: https://www.marketresearchfuture.com/reports/zero-trust-security-market-9919
7. Wired. (2023). "Why WireGuard Is the Most Secure VPN Out There". Retrieved from: https://www.wired.com/story/wireguard-vpn-security/
8. Australian Financial Review. (2023). "Optus and Medibank Breaches Expose Gaps in Cybersecurity". Retrieved from: https://www.afr.com/technology/optus-and-medibank-breaches-expose-gaps-in-cybersecurity-20221214-p5c6us
9. Verizon. (2023). "Data Breach Investigations Report". Retrieved from: https://www.verizon.com/business/resources/reports/dbir/

Chapter 3

1. Frost & Sullivan. (2023). *Cybersecurity in Managed Services: Market Trends and Challenges*. Retrieved from: https://www.frost.com/
2. Forrester. (2023). *The State of IoT Security 2023*. Retrieved from: https://www.forrester.com/
3. Gartner. (2023). *Top Security Trends and Predictions for 2023*. Retrieved from: https://www.gartner.com/en/documents/2023/top-cybersecurity-predictions
4. IDC. (2023). *Cybersecurity Market Dynamics: SMB Adoption and Challenges*. Retrieved from: https://www.idc.com/
5. Mandiant. (2023). *The Evolution of Cyber Threats: A 2023 Analysis*. Retrieved from: https://www.mandiant.com/resources/2023-threat-landscape-report

Chapter 4

1. CISA. (2021). "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks." *Cybersecurity & Infrastructure Security Agency*. Retrieved from: https://us-cert.cisa.gov/ncas/alerts/aa21-131a
2. Clark, D. (2023). "Australia's DP World Ports Hit by Cyber Attack Disrupting Operations." *Reuters*. Retrieved from: https://www.reuters.com/article/us-australia-cyber-idUSKBN2HC1BQ
3. FTC. (2019). "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach." *Federal Trade Commission*. Retrieved from: https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related
4. Office for Civil Rights. (2016). "Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History." *U.S. Department of Health and Human Services*. Retrieved from: https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach-history.html