BlackBerry
Intelligent Security. Everywhere.

White Paper

Zero Trust, the Future of Healthcare

Keep Technology Secure Without Exhausting Resources

Introduction

The healthcare industry faces a surge of new threats from the cyber chaos created by interconnected technology and an increase in remote workers. Technological advancement, increased interconnectivity, and workforce changes have created an expanding attack surface that is particularly dangerous for healthcare organizations. Unfortunately, many facets of the healthcare industry are still relying on outdated trust models and small IT security teams to protect their infrastructure.

Zero Trust architecture provides a model for keeping technology secure without exhausting resources in an effort to keep pace with exponentially increasing threats. It operates on the assumption that actors must earn and maintain trust in order to access organizational resources. Restricting access to trusted entities addresses many vulnerabilities commonly exploited by threat actors today.

Examining the origins of the new threats facing healthcare organizations is key to understanding the value of a Zero Trust approach to security. Once the nature of these emerging vulnerabilities is grasped, the necessity of transitioning to a Zero Trust security framework becomes clear.

"Zero Trust architecture provides a model for keeping technology secure without exhausting resources in an effort to keep pace with exponentially increasing threats."

What Is Cyber Chaos?

Modern healthcare organizations are a hive of interconnected devices and networks. Smartphones, tablets, medical equipment, and Internet of things (IoT) hardware are constantly connecting to both public and private organizational infrastructure. Employees carry their devices out of the workplace networks to home where they access heavily regulated patient data from consumer devices and networks. Likewise, visitors bring personal devices into hospitals and other healthcare facilities to connect with public/local infrastructure. This back-and-forth of high-volume connections from a variety of devices and networks makes keeping healthcare environments secure a Herculean task.

Unfortunately, medical equipment and other connected devices have little, if any, cybersecurity capability. This means every non-protected device connecting to healthcare infrastructure creates an expanding attack surface. Every connected smartphone with third-party apps, USB storage device, Bluetooth® headset, and embedded system brings its own vulnerabilities to the technical environment. Beyond that, healthcare organizations must also solve for remote employees accessing corporate data and PII from personal devices on non-work networks.

Adding to the problem, it is estimated that over 100 billion lines of code are written every year[1]. This means many devices capable of accessing healthcare resources are likely running untested or vulnerable code. Passwords, another popular attack vector, have grown by an estimated 300 billion in the last three years[2]. Hundreds of millions of accounts are breached every year, leading to many of these passwords

1 https://www.darkreading.com/risk/what-wont-happen-in-cybersecurity-in-2020/a/d-id/1336927
2 https://www.scmagazine.com/home/research/video-300-billion-passwords-by-2020-report-predicts/

appearing for sale on the dark web[3]. The incredible increase of interconnected devices, unverified code, and passwords cause an explosive growth of vulnerabilities referred to as cyber chaos[4].

Dangers of Remote Work and Travel

Many healthcare organizations have increased the number of employees working from home and have expanded telehealth services. Workplace devices leaving the organizational environment, or remotely connecting with it, creates new attack vectors. Threat actors have taken advantage of remote workers by spoofing private branch exchange (PBX) systems[5]. PBX attacks involve threat actors telling remote workers they have a voicemail message, then directing them to a website engineered to phish credentials.

A similar attack has been leveraged against telehealth workers who use a VPN to connect to the workplace. In addition to exploiting the known vulnerabilities of VPNs, attackers have faked internal emails telling workers there is an issue with their connection. Employees are then directed to another credential-harvesting website to resolve the fake connection issue[6].

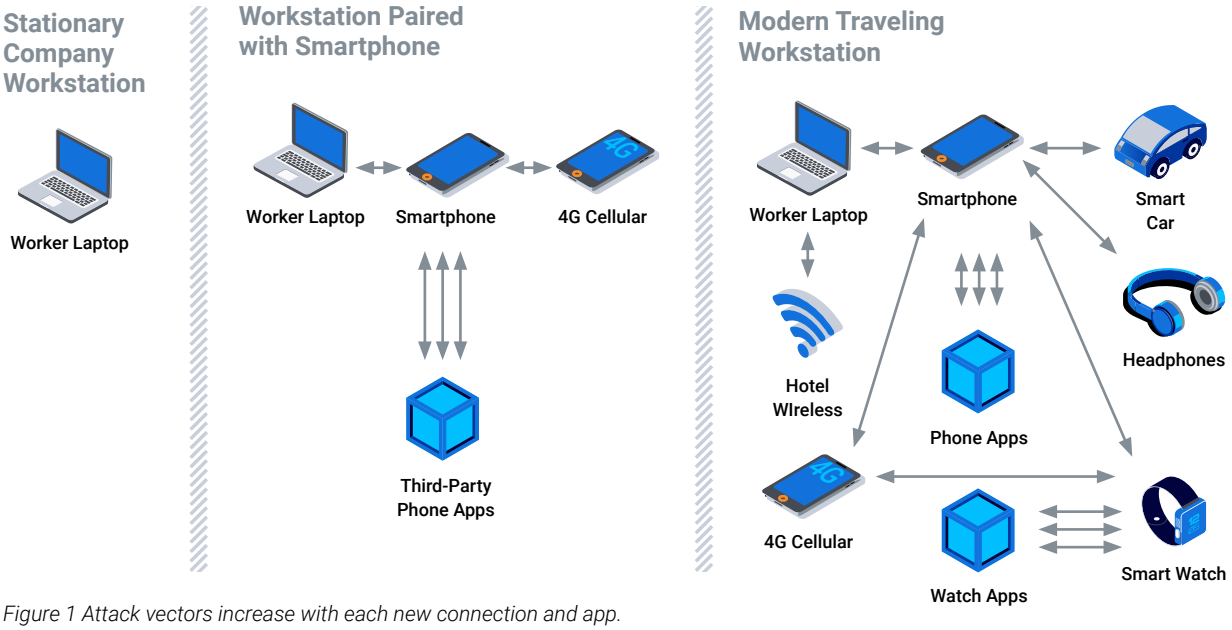

Figure 1 Attack vectors increase with each new connection and app.

Travelling healthcare employees will often sync their devices to rental vehicles and connect to free wireless networks provided by hotels or businesses. These actions potentially expose workplace data to countless threats both during the travel period and after these devices reconnect with workplace infrastructure. On-site security teams have little, if any, capability for determining what workplace data has been exposed, where, or to whom on travelling devices.

3 https://www.cnn.com/2020/05/06/tech/data-breach-passwords-protection/index.html
4 https://blogs.blackberry.com/en/2020/05/blackberry-spark-suites-bringing-order-to-the-chaos
5 https://www.hipaajournal.com/voicemail-phishing-scam-identified-targeting-remote-healthcare-workers/
6 https://www.hipaajournal.com/fake-vpn-alerts-used-as-lure-in-office-365-credential-phishing-campaign/

Zero Trust is the logical approach to cybersecurity in a world where workplace devices interact with outside networks and the IoT. When securing everything is not viable, organizations must limit their risks by interacting with low-risk and trustworthy entities. Virtual trust, for users, devices, data, or other networks, must begin at zero and be built up and maintained over each engagement.

Cybersecurity: A Complicated or Complex Problem?

Creating or implementing effective cybersecurity solutions relies on understanding the nature of the trust problem created by IoT devices and mass interconnectivity. Today, building secure workplace environments is not a complicated problem, but a complex[7] one.

To clarify, complicated problems involve several components which interact with each other in predictable ways. People can predict the output of a complicated system if they know the inputs. For example, building a submarine is a complicated task. There are many interconnected systems within a submarine that must function a particular way for the submersible to work. Since each of these interconnected systems ultimately behave in a predictable way, engineers are able create a highly complicated submarine given enough time and resources.

Complex problems, however, have many interconnected systems, but the interaction between them is unpredictable. Even when people know the inputs, the outputs can at best, only be guessed. Systems like financial markets and the global climate are complex. With complex systems, we may be able to understand pieces of the larger puzzle, but we remain unable to reliably predict conclusive outcomes.

Modern cybersecurity may have been a complicated problem in the past, when workstations were isolated to business environments. Today, the growth of IoT devices, the speed of technological innovation, and sheer volume of new software code make effective cybersecurity a complex problem (a.k.a. beyond the realm of human prediction).

Technology, however, can perform calculations and operations with a speed and efficiency that humans cannot. Enlisting the aid of predictive modelling, artificial intelligence (AI), machine learning (ML), and continuous authentication offers analysts effective ways to tackle complex security problems.

What Is Zero Trust?

Zero Trust, as the name implies, is a security model built around the idea that nothing inside or outside of an organization can be trusted. The foundation of Zero Trust architecture came from the Jericho Forum in the early 2000s, where security specialists discussed cloud computing and de-perimeterization[8]. The phrase Zero Trust was coined by John Kindervag, a principal analyst at Forrester Research Inc., in 2010[9].

"Creating or implementing effective cybersecurity solutions relies on understanding the nature of the trust problem created by IoT devices and mass interconnectivity."

7 https://thearmyleader.co.uk/team-of-teams/
8 https://blog.banyansecurity.io/blog/the-evolution-of-zero-trust
9 https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

AI's Role in Zero Trust

One distinct advantage of AI is its lightning-fast ability to process and find correlations in massive data sets. It is precisely this ability that allows AI to accurately predict the identity of users, the safety of files, and legitimacy of activities. Some of the ways AI can be used to implement Zero Trust include:

- **User and Entity Behavior Analysis:** AI can monitor user activity, location, and biometrics and compare them to normal patterns to determine if an actor is trustworthy. Account access can be automatically modified to reflect changes in trust, and re-authentication steps can be initiated when trust scores drop too low.
- **Malware Prevention:** AI can be taught to identify unknown or zero-day malware through training on millions or billions of safe or malicious files. Highly trained AI can successfully detect both known and previously unknown malware by analyzing a file's features pre-execution. This capability gives AI-driven security agents a predictive advantage over threats and can easily replace traditional trust-based models of file security.
- **Threat Hunting:** Mathematical models can be deployed directly on endpoints to monitor their activity and report anomalous behavior. On-device threat detection capabilities allow endpoints to quickly report suspicious activity, launch automated remediation, and isolate themselves from other resources during an attack.

The Zero Trust model greatly benefits from AI's ability to make predictions based on aggregating and analyzing data. It allows organizations to move away from one- and two-factor authentication strategies that have long been examined and exploited by threat actors. Trust, when vetted by AI, becomes a continuous process of safe and expected engagements rather than a one-time presentation of credentials.

"The Zero Trust model greatly benefits from AI's ability to make predictions based on aggregating and analyzing data."

Humans' Role in Zero Trust

Security specialists have several tools available for implementing a Zero Trust framework. With AI largely handling detection and response, analysts can focus on other tasks like ensuring access to organizational resources is secure. As the modern healthcare workforce becomes increasingly mobile, businesses must find new and secure ways to provide remote work services. Being able to secure and monitor a wide variety of mobile technology is a critical component of modern cybersecurity solutions.

Businesses should consider the following factors when selecting tools for their in-house security personnel:

- Can employees reliably and securely access work resources remotely?
- Can work resources be securely accessed from any device?
- Does a solution address multiple ownership models and platforms, including Windows®, iOS®, Android™, macOS®, and Linux®?
- Is the solution scalable, and can it easily map to new technology?
- Are work resources available both online and offline, and accessible without using a VPN?

- Does a solution offer a single interface for performing security tasks, or will analysts be forced to divide their attention among multiple interfaces?
- Can security analysts ensure workers are using trusted applications on a secure mobile device?

Cultivating a viable Zero Trust environment requires organizations to also grapple with the pace of technological innovation and changing business practices. Work is increasingly being conducted outside of the physical office and on personal devices. Simply put, Zero Trust cannot be confined to traditional network perimeters. It must encompass access to business data from any device, anywhere.

Achieving Zero Touch in a Zero Trust Environment

One major concern for organizations considering a Zero Trust model is how the framework will impact their users. Employees will seek workarounds to avoid intrusive or disruptive verification processes and may introduce new vulnerabilities in their attempts to create shortcuts. This means creating a minimally intrusive, or Zero Touch experience for users, is a key component of a robust Zero Trust framework.

Using AI-driven solutions to conduct continuous authentication is a viable way to enjoy the best of both worlds. Real-time analysis of contextual data on users, devices, and locations can verify whether activities are trustworthy without interrupting their workflow. Users are only asked to re-verify their identity when engaging in particularly high-risk transactions or behaving in an anomalous manner. The vast majority of daily tasks are low risk operations and will never trigger a re-authentication request.

Why Zero Trust?

How does a healthcare organization stand to benefit by adopting a Zero Trust security model? To understand the numerous benefits of Zero Trust, consider the following:

- How would your environment benefit from only dealing with positively identified and continuously authenticated users?
  - What programs, policies, or practices would no longer be necessary?
  - What new opportunities could be pursued once your organization can be 100% confident about user identity?
- What changes could occur in your organization if every device was verified as trustworthy throughout each engagement?
  - How would your technology selection change?
  - How would worker productivity change?
- How would your organization's security posture benefit if access rights could be modified in near-real-time to reflect the current trust level of users and devices?
  - Would the ratio of office workers to remote workers change?
  - Could the IT security staff be utilized in new and effective ways?

"Cultivating a viable Zero Trust environment requires organizations to also grapple with the pace of technological innovation and changing business practices."

The Zero Trust model can benefit healthcare organizations in many surprising ways that are not immediately obvious. For example, in 2020, phishing attacks were involved in over 80% of reported security incidents[10]. Zero Trust limits the amount of damage a compromised user can inflict by restricting their access and requiring re-authentication when unexpected behaviors occur.

Likewise, Zero Trust makes it difficult for threats to propagate throughout the environment undetected since they leverage resources and modify access in highly suspicious ways. Common vulnerabilities like missed software patches and system updates are less disastrous under the continuous scrutiny and restrictive posture of the Zero Trust model.

Conclusion

Zero Trust is the rational approach when interacting with modern technology and systems. Securing the workplace environment through traditional techniques becomes untenable when workplace devices interface with a sprawling IoT. Healthcare organizations must realize they cannot vet every outside app, device, and network encountered by their employees.

However, interacting with known, trusted, and continuously authenticated entities is a viable solution for security issues created by technological advancement and remote work. Likewise, AI can greatly augment security teams by performing brute-force analysis and remediation at speeds and volumes beyond human ability.

BlackBerry Spark® Suite brings together the security, management, and productivity tools to meet your Zero Trust goals with a Zero Touch approach for your healthcare employees and contractors.

Limiting contact to verified trustworthy actors and relying on AI to perform detection, monitoring, and response operations can offset many emerging cyber risks. For more information, review BlackBerry's Zero Trust Model Meets Zero Touch Experience web page.

---

10 https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

MKTG 20-DTA-12081 | 200909