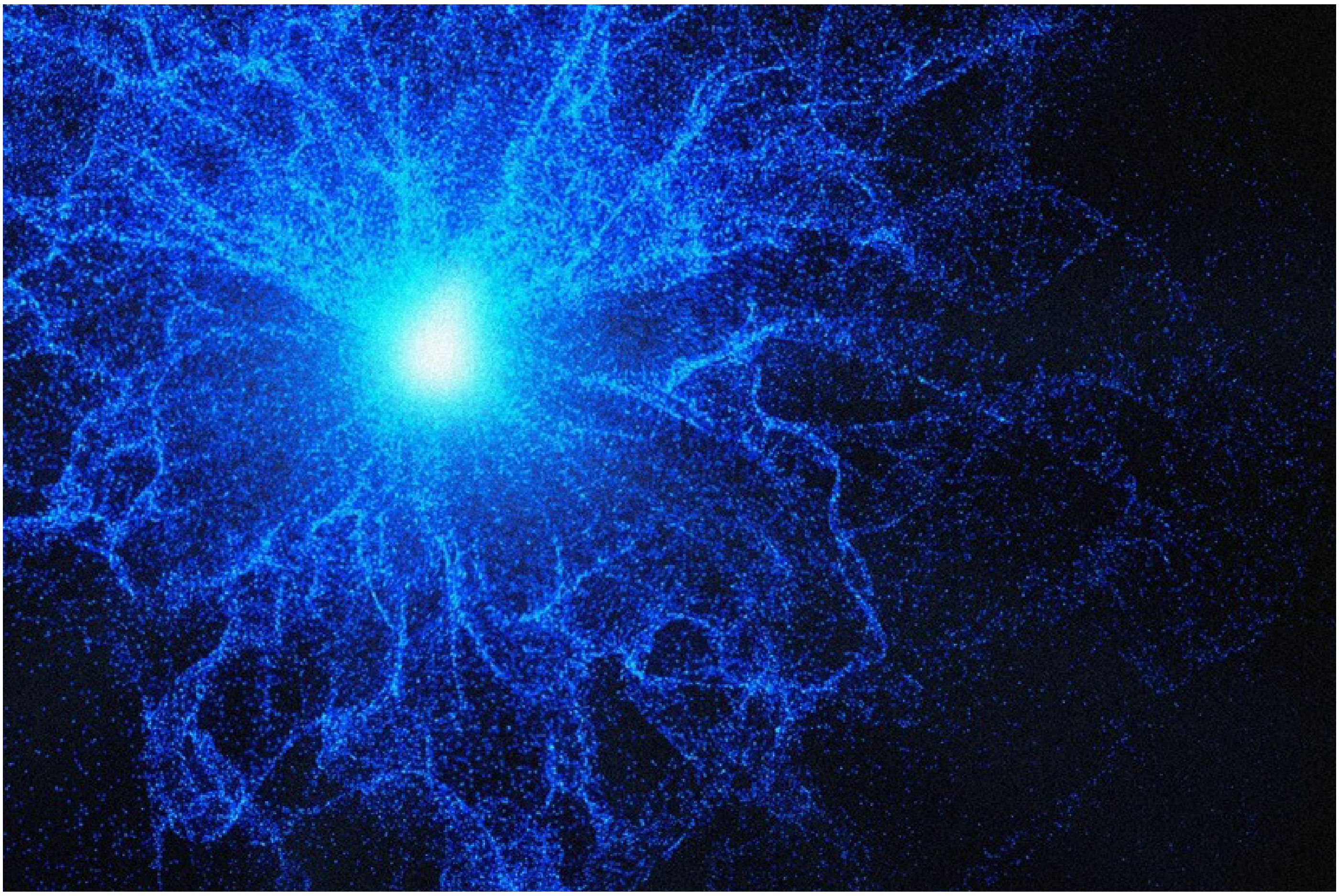
BlackBerry
Intelligent Security. Everywhere.

White Paper



The Inevitable Ascent of Zero Trust

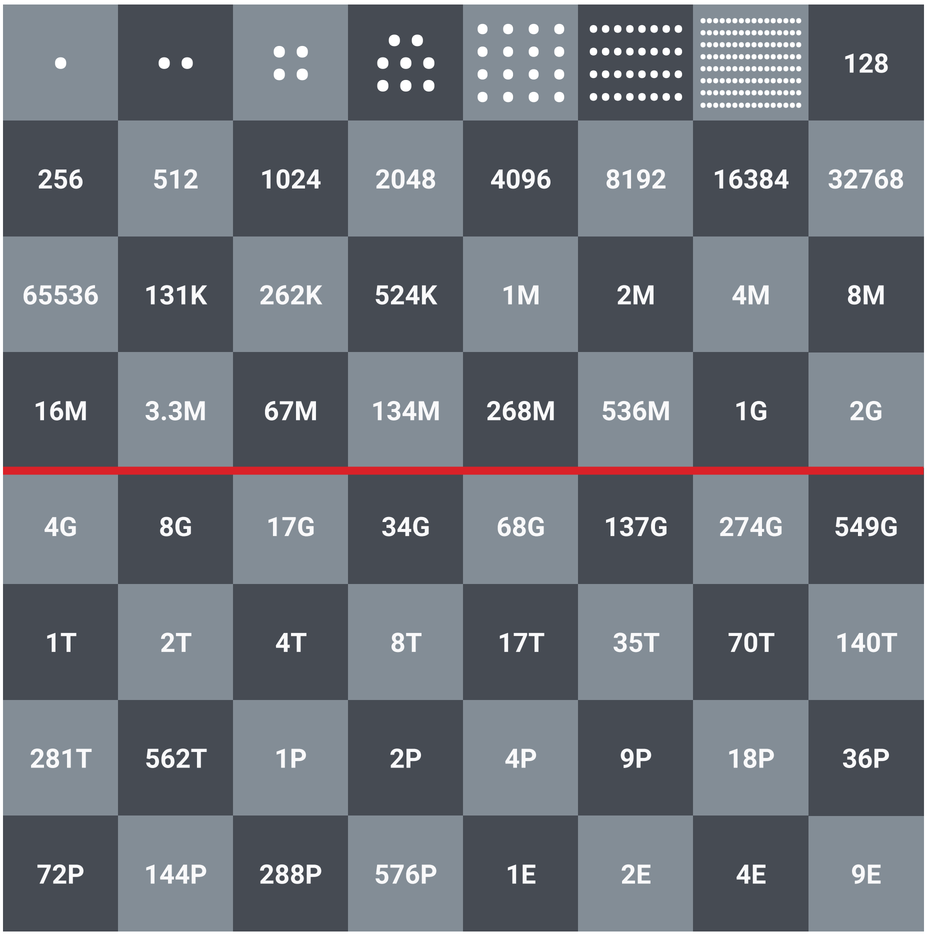
Ensure User Activities Are Trustworthy Without Interrupting Workflow

Understanding the Problem of Trust

There is a story about the creation of the game of chess that illustrates why cybersecurity solutions cannot rely on traditional trust models. The story goes that the inventor of chess presented the game to a king. The king was very impressed and offered the creator whatever he wished as a reward. The creator requested a single grain of rice for the first square of the chessboard. Also, each square after the first would receive double the rice of the previous square, until the end of the chessboard was reached.

The request initially seemed quite manageable to the king, but as time progressed it became apparent that fulfilling it was impossible. The doubling rice was an exponentially expensive request, ultimately requiring quintillions (264 – 1) of grains. The king could not honor the request, so he allegedly executed the inventor for insolence.

The chess board / rice problem is similar to the endpoint security dilemma facing many organizations today. In the early days of computing, securing an employee workstation was a manageable task. When multiple workstations joined a network, or several connected networks (and ultimately, the Internet), securing the environment became considerably more difficult. Now, with the growth of interconnected Internet of things (IoT) devices, securing all technology touching workplace resources is nigh impossible.



●	●●	●●●●	●●●●●●●●	●●●●●●●●●●●●●●●●	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	●●	128
256	512	1024	2048	4096	8192	16384	32768
65536	131K	262K	524K	1M	2M	4M	8M
16M	3.3M	67M	134M	268M	536M	1G	2G
4G	8G	17G	34G	68G	137G	274G	549G
1T	2T	4T	8T	17T	35T	70T	140T
281T	562T	1P	2P	4P	9P	18P	36P
72P	144P	288P	576P	1E	2E	4E	9E

> “The chess board / rice problem is similar to the endpoint security dilemma facing many organizations today.”

Figure 1. One grain of rice doubled per each square quickly grows to unfathomable proportions.

Attack Vectors Increase as Devices Are Added

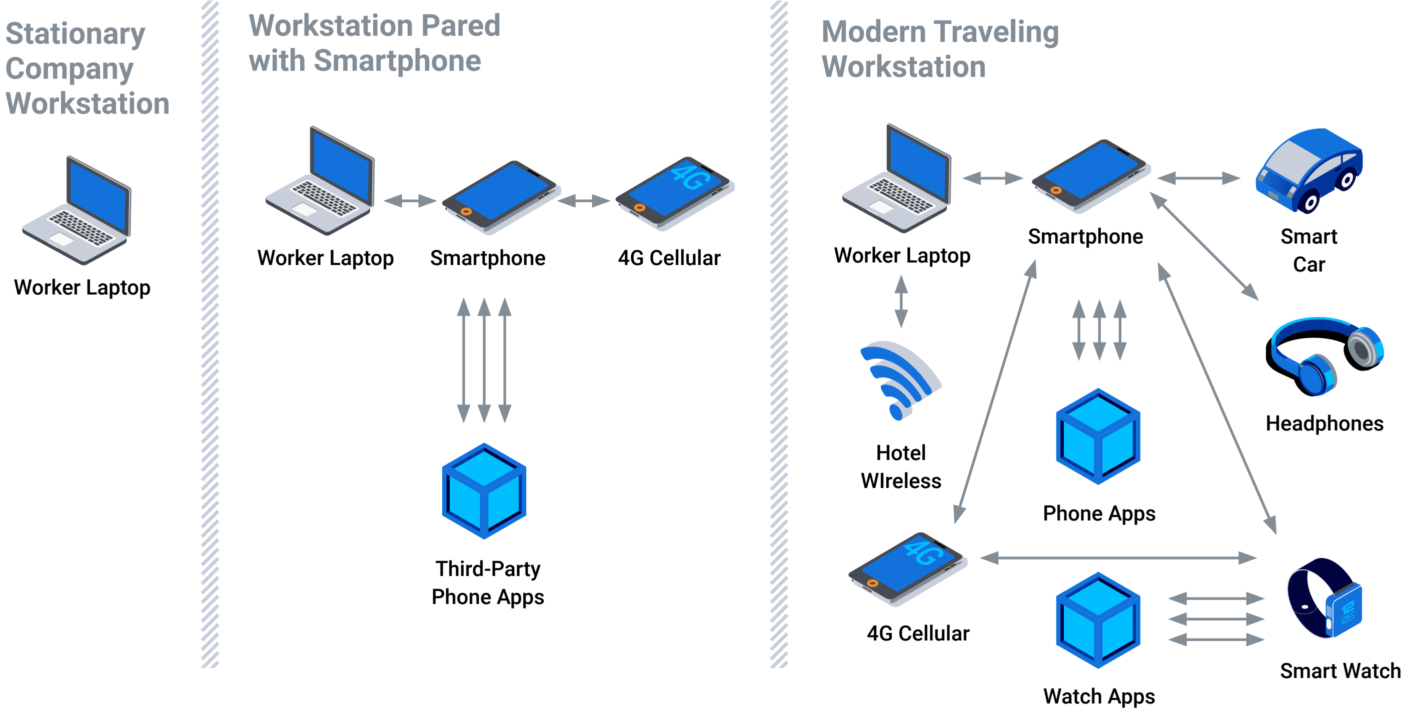


Figure 2. Attack vectors (represented by gray arrows) increase with each additional device, application, and network connection.

To illustrate this point, consider a worker who has a single company-assigned laptop. Securing the laptop is fairly easy, but this employee also accesses company assets with their smartphone. How secure are the various apps on the smartphone? No one knows. The worker also, on occasion, listens to music on their smartphone using an advanced Bluetooth® headset (IoT device) created by an unknown manufacturer.

These devices are all paired with a car, which stores music, contact lists, and other information on its own internal system. As the employee travels, they connect their laptop and smartphone to several public-area networks so they can check email and work on projects.

How secure are the business resources now? The attack surface covering organizational resources increases with each additional application, device, and network connection. This dilemma clearly demonstrates that organizations must adopt a Zero Trust approach to security.

Trusting entities by default, or based upon a one-time confirmation, is simply not a viable security strategy. The best approach for limiting risk is to trust nothing by default, but to build up and maintain trust with actors over sustained engagements.

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[1] 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.

> "With complex systems, we may be able to understand pieces of the larger puzzle, but we remain unable to reliably predict conclusive outcomes."

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[2]. The phrase Zero Trust was coined by John Kindervag, a principal analyst at Forrester Research Inc., in 2010[3].

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 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 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 ensure that 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.

> "Real-time analysis of contextual data on users, devices, and locations can ensure that activities are trustworthy without interrupting their workflow."

Why Zero Trust?

How does an 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?

The Zero Trust model can benefit 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[4]. 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 business environment through traditional techniques becomes untenable when workplace devices interface with a sprawling IoT. Organizations must realize that 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 the security issues created by technological advancement. 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 employees and contractors.

For more information, go to http://www.blackberry.com/sparksuite.

[1] https://thearmyleader.co.uk/team-of-teams/

[2] https://blog.banyansecurity.io/blog/the-evolution-of-zero-trust

[3] https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

[4] 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 175M 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.