Whitepaper

How Bridging the Gap Between Zero Trust and Zero Touch with AI Benefits Your Organization

Zero Trust is…

- An overlapping security approach that continues to evolve as an environment changes with new users, devices, applications, and technologies.
- A combination of processes and technology.
- Not a single product or a one-time check list.

Fundamental principles:

- Users access data that resides anywhere, from anywhere, in any way
- External and internal threats exist on the network and endpoints at all times
- Every device, user, and network flow must be authenticated and authorized
- Policies must be contextual, dynamic, and data-driven, not static

Foundational Zero Trust elements

People – Zero Trust starts with people and the need to identify them as trusted users or not – and not just upon intermittent login events but on a continuous basis throughout the app usage lifecycle. This still involves traditional Identity and Access Management (IAM) technologies, but these technologies on their own lack the ability to continuously monitor and validate user trustworthiness and govern access and privileges between intermittent login events. Because users don't tolerate frequent, active re-authentication, this drives the need for authentication technologies that are both unobtrusive and continuous in their application.

Devices – trustworthiness of devices used by people is another foundational attribute of any well-designed Zero Trust architecture. Continual assessment should include whether the device is in a compromised state, is using older software, and has encryption enabled with sufficiently strong password controls to ensure its integrity. An ironic aspect of narrowly network-focused Zero Trust solutions is that they may unwittingly allow fully trustable people to access the network from fully compromised devices and thereby increase, not decrease overall threat exposure. Threat detection and prevention should also span mobile and desktop, and not ignore one or the other or treat as siloes.

Network – in a world of hyper-connected networks, network trust is bedrock for establishing Zero Trust. However, with more workloads moving to the cloud and ubiquitous mobile and Wi-Fi networks, static, rules-based perimeter definitions no longer suffice as the network itself is a dynamic and ever-evolving entity. Moreover, the outdated concept of people and devices being trusted simply based on permission to access the network has proven time and again to be weakest point in network security. Ironically, traditional VPN gateways can make this problem worse by bringing traffic from BYO devices that's destined for the cloud inside the enterprise perimeter, exposing internal networks to lateral traversal threats, only to send it back out again anyway. To adapt to this more dynamic network concept and mitigate ever-changing risks that inherently come with the combo of cloud, mobile/Wi-Fi, and BYO, next generation secure web gateways and service-based network segmentation technologies become a foundational element of Zero Trust architecture. This is based on their ability to dynamically adapt not only to the risk of the network itself but also the people, devices, and apps accessing and using it, both at the time of initial access and throughout the app usage lifecycle.

Apps - securing and properly managing the app layer as well as compute containers and virtual machines is central to Zero Trust adoption. Having the ability to identify and control the technology stack facilitates more granular and accurate access decisions. Unsurprisingly, multi-factor authentication is an increasingly critical part of providing proper access control to applications in Zero Trust environments.

Security Analytics and AI – while it's true you can't combat a threat you can't see, it's also true that needing to a see a threat many times before you can identify and prevent it necessarily leaves you exposed, and on a continuous basis. That's why a well-designed Zero Trust architecture must leverage advanced, AI-based threat identification and prevention, user and entity behavior analytics (UEBA), and other analytics-based approaches to learn from the past, understand what's happening in real-time and apply preventative measures intelligently. The goal is not just identifying threats and data loss events after the fact, but actively preventing threats and data loss from occurring in the first place.

Automation – it's simply not possible for security analysts to be actively involved in every access decision at the time requests are being made or even a small portion. Cost-effective Zero Trust necessarily makes full use of automation and intelligence-based dynamic policy adaptation and response to deliver the real-time Zero Touch experience that people demand while still enabling Security Operation Center (SOC) oversight and interaction in a much more targeted, high-value, and insight-driven way.

The Zero Trust dilemma…

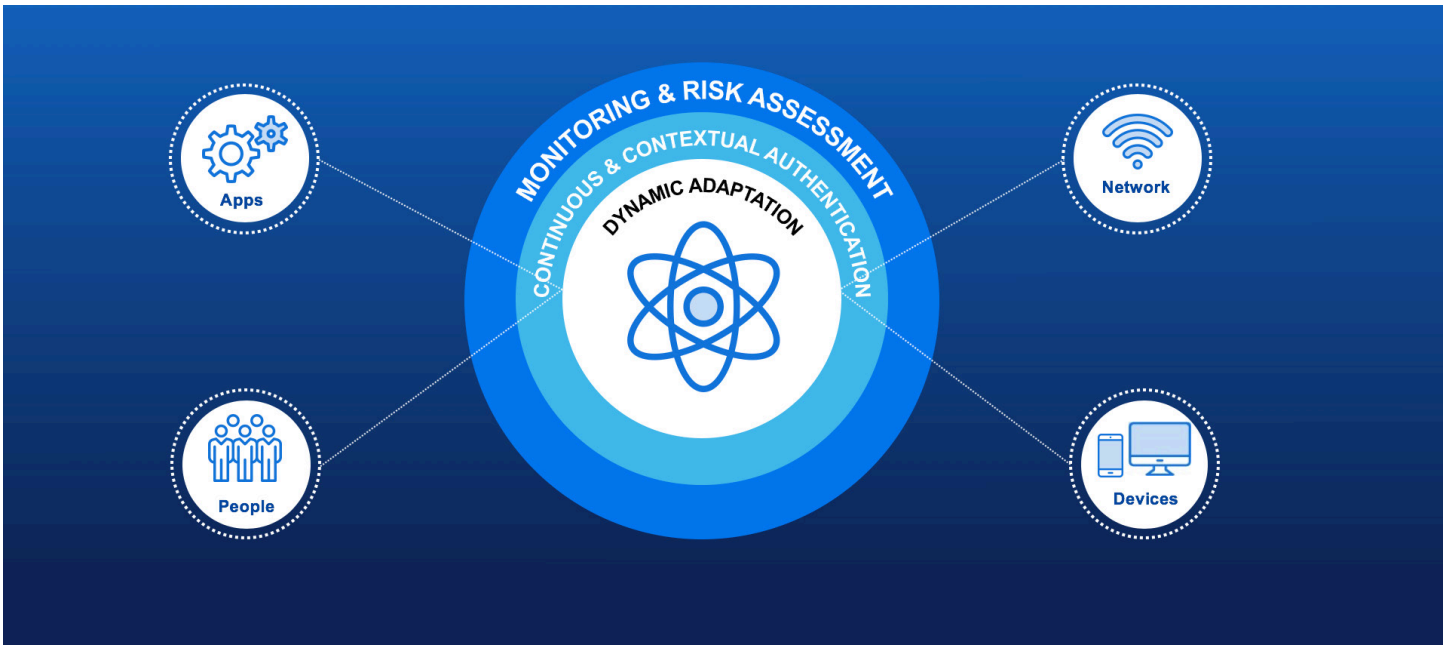
Zero Trust architecture
This is what every security team wants – nobody gets or keeps access to anything until they prove and continue to prove who they are, that access is authorized, and they are not acting maliciously.

Zero Touch experience
This is what users/employees want – immediate gratification with instant access to anything and everything they believe they need without hassles of passwords, timeouts, special permissions, multiple authentications, etc.

Zero Trust Architecture by BlackBerry solves the dilemma

Zero Trust Architecture (ZTA) by BlackBerry incorporates all of the necessary foundational elements and solves the Zero Trust dilemma by applying its strong Security AI and Analytics expertise to deliver the Zero Trust architecture that the security team needs, with the Zero Touch experience that end users crave.

Figure 1: Zero Trust Architecture by BlackBerry



Constant Monitoring and Threat Detection (MTD)
AI monitors mobile and desktop devices and the apps running on them for any new or known threats and takes appropriate action to remediate. This includes support for "safe browsing" to block access to malicious URLs and prevents phishing attacks. BlackBerry's Secure Edge Framework enables MTD to be easily integrated into any app.

Contextual Authentication
AI modeling of user behavior learns whether the user's 'macro' context conforms with trusted behavior and dynamically adjusts the network perimeter to either (i) grant access when behavior is trusted and conformant with policy, (ii) challenge the user when behavior is novel but otherwise conformant with policy, or (iii) block access outright when behavior is either non-conformant with policy or otherwise highly anomalous.

Continuous Authentication
After initial access grant, Continuous Authentication assesses the 'micro' context of a user's ongoing behavior and decides if access should be allowed to continue. Combining biometric, app usage, and process invocation patterns across mobile and desktop, Continuous Authentication provides 'n-factor' authentication that is stronger than traditional 2-factor authentication and virtually impossible for malicious user to spoof because it goes beyond 'what you have' and 'what you know' to 'who you are' behaviorally and across multiple dimensions.

Dynamic Policy Adaptation and Response
Dynamically and intelligently applies the right policy, at the right time to ensure policies are optimized for the user's current context and are neither too strict, nor too lenient. AI-based, prevention-first Endpoint Detection and Response (EDR) thwarts attacks before they can execute and automates investigation and response with playbook-based workflows.

Real world example

An employee just left their smartphone in a restaurant during lunch hour after using it to check emails and access apps in the cloud and on the corporate intranet.

A typical static mobile policy, e.g. based on a 30-minute timeout, combined with a 'network-only' approach to Zero Trust necessarily leaves data exposed in this case because the legitimate user was already and recently granted access. For the malicious user who now picks up that phone, this means:

- Access from this mobile/Wi-Fi network won't be denied
- Access to apps was just granted, re-authentication won't come into play
- Timeout may eventually come into play, but only after active use stops

The irony of this all-too-common case: it is the legitimate user's beneficial and productive behavior that leads to this exposure. But, to be clear: it's not the user's fault, but rather the fault of the static, context-unaware policy and overly narrow 'network-centric' conception of Zero Trust focused on the initial access grant.

How Zero Trust Architecture by BlackBerry handles this case…

ZTA by BlackBerry continuously monitors solution continuously monitors all devices and apps and applies strong AI to understand how people use devices, apps, and networks to actively prevent data loss and optimize, not degrade, the legitimate user's experience.

Contextual Authentication
The restaurant is already known to be a low-trust location for this user. Device and/or app timeouts would already have been adjusted to reduce the threat window associated with any 'left-behind' device. In addition, if the user subsequently accesses apps from another device in another location – e.g., upon logging back into their laptop when returning to the office – ZTA by BlackBerry would detect that event and take proactive action to lock the 'left-behind' phone and/or its apps until it's been recovered by the legitimate user.

Dynamic Policy Adaptation: Timeout is dynamically reduced upfront upon the user's initial usage in the restaurant, and then the device and its apps are explicitly locked when the user's return to the office is detected.

Continuous Authentication
Additional layers of AI-based defense based on a combination of passive biometrics and anomalous usage detection ensure that only the legitimate user can enjoy continued access to apps and services.

Dynamic Policy Adaptation: A malicious user is automatically challenged and blocked from accessing apps when they fail passive biometrics checks and/or exhibit anomalous behavior that doesn't fit with legitimate user's learned, trusted behavior. This eliminates any remaining threat should the malicious user gain access before reduced timeout expires.

BlackBerry AI techniques

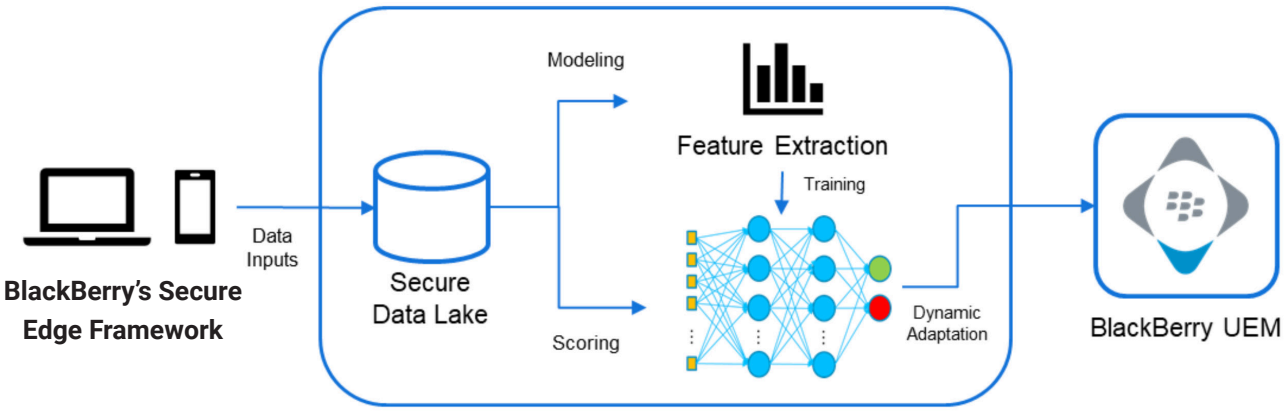
BlackBerry uses a combination of AI techniques that work together as "ensemble" to deliver Continuous Monitoring & Threat Detection, Contextual Authentication, and Continuous Authentication.

Unsupervised Learning
Learns trusted and normal behavior and locations for individuals, groups, and roles, and dynamically applies policy tuned to the user's context and current risk profile.

Deep Learning
Turns passive biometrics and other behavioral and security analytics into continuous, 'n-factor' authentication of the legitimate user. Solves practical problems with traditional 'login + timeout' model where there's no guarantee that the current user is still the same legitimate user that was initially granted access to a device, network, or app.

Anomaly Detection
Applies supervised and unsupervised techniques to app usage and security analytics to distinguish exploit patterns from normal usage, for malicious outsiders and malicious insiders alike.

Figure 2: BlackBerry Intelligent Security AI-based risk modeling & scoring across all endpoints



Modeling inputs

Context

- Location
- Date and time
- App/services used
- Network used

Biometrics

- Motion/touch metrics
- Device orientation angles
- Device tremor
- Mouse movements
- Keystroke speed

App Usage & Security Analytics

- Authentication
- Process Initiation
- Search/Download
- Send/Forward
- Share/Open In
- Copy/Paste
- Screen Capture

Secure Edge Framework ensures data integrity

For any AI-based security approach to succeed, it's critical to ensure integrity of the data that's used in modeling and risk scoring processes. Compromise of data going into the system necessarily can compromise the validity of risk scores and dynamic policy adaptations based on them. BlackBerry protects the integrity of inputs into its AI modeling and scoring with its Secure Edge Framework (SEF).

This framework has four main components that are based on a combination of BlackBerry and Cylance's proven, best-of-breed technologies for endpoint security and threat detection:

Secure Boostrap
Enables only authorized endpoints to submit data, and prevents an endpoint from 'spoofing' any other endpoint and maliciously submitting compromised data into the system or to perform a 'denial-of-service'-style of attack.

Device Compliance
Maintains device compliance by performing rooted/jailbreak detection and other compliance checks to safeguard the Secure Edge Framework from being compromised even when the device on which it is running is compromised.

Mobile Threat Defense
Detect and prevent previously unknown threats from compromising an otherwise compliant device or app.

Security Analytics
Implements a turnkey analytics library and supporting APIs to make it easy for apps implementing BlackBerry's Secure Edge Framework to instrument and securely submit the most important subset of analytics needed to perform Contextual and Continuous Authentication.

Secure Internet Gateway

As outlined above, lines that define internal and external networks are increasingly dynamic and blurred, and usefulness of traditional VPN gateways and firewalls is diminished as a result. At the same, time the distinction between firewalls and web gateways is also blurred, and we often see these two capabilities combined in cloud-based gateway offerings. Traditional network firewalls could fulfill this role when all incoming and outgoing traffic passed through it and the majority of threats were packet-level attacks such as denial of service, buffer overflow exploits, malformed packet exploits, etc. And while these types of threats still exist, the expansion and sophistication of attacks has moved to the app level with a focus on hijacking, phishing, data extraction, and similar attacks.

To address this evolving view of the network, the Zero Trust architecture must incorporate a Secure Internet Gateway (SIG). Beyond enabling VPN-less access, the SIG provides the following additional capabilities to meet the Zero Touch objective of ubiquitous, secure, and VPN-less mobile access and extends that capability to any device.

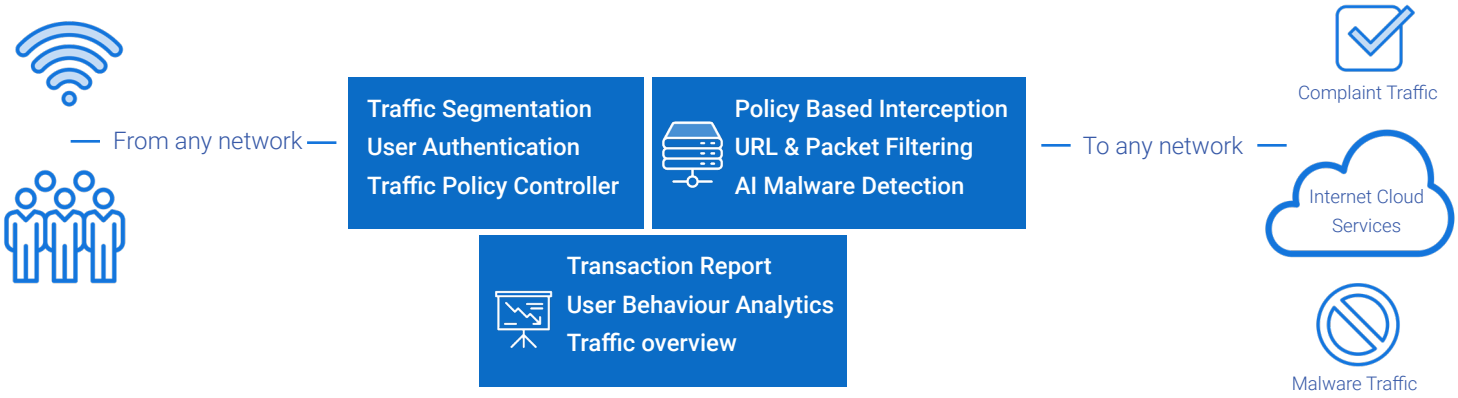
Contextual and Continuous Authentication

As outlined above, authentication in Zero Trust architecture must be contextual and continuous and occur throughout the app usage lifecyle, including when using the SIG to ensure that people remain continuously authenticated and will dynamically block access to network and apps as needed if their authentication status comes into question at any point.

Traffic Segmentation

One of the goals of a Zero Trust network is to segment traffic such that it can be efficiently locked down, yet still provide immediate and ubiquitous access when trust is and remains established. A key challenge is maintaining a dynamic permission model in an ever-changing network environment, with new people, devices, and apps that may come online at any time. In a complex multi-tier data center deployment, there may be a myriad of network appliances and firewalls rules in play which are often difficult to visualize or manage. Therefore, answering even the most basic question of 'who has access to what' can be surprisingly difficult and becomes more difficult as more third party hosting and cloud service providers participate in the delivery of apps. And even after an initial configuration is laboriously and painstakingly put together, ongoing maintenance becomes a costly and risk-inducing problem based on the possibility of misconfiguration and other human- or process-related errors.

Figure 3: Secure Internet Gateway



The SIG addresses these challenges by enabling a software defined network with configuration policies that can segment the traffic based on privileges in a more centralized and dynamic manner without requiring changes to be made and made correctly and consistently across a myriad of physical networking components. In addition, BlackBerry's AI-based model can help automate the necessary segmentation configuration based on learned traffic access patterns for users, groups and roles and can also detect anomalies in real-time and immediately remediate by denying access.

Threat Prevention

In addition to authentication and segmentation, The SIG will combine policy-based interception and standard URL and packet filtering with advance and proactive AI-based malware detection and threat prevention leveraging the other ZTA components. With the SIG, enabling dynamic and flexible network and apps access in service of Zero Touch objectives protects the enterprise from device and network-born threats that can undermine overall security and expose the enterprise to malicious service disruptions and/or data loss.

Reporting and Analysis

To provide visibility and enable focused management, the SIG will provide reporting and analysis that includes not just transactional and traffic reporting, but also User Behavior Analytics. This provides SOC personnel with a complete perspective on how people and devices are using network and apps, and enables them to implement more optimal policies and controls that achieve a balance between Zero Trust and Zero Touch objectives.

Zero Trust Architecture by BlackBerry – total solution, full coverage across all endpoints

While other solutions address parts of the problem, ZTA by BlackBerry provides a total solution for Zero Trust with full coverage across the full spectrum of devices, network, apps and people.

- Provides a path from Zero Trust architecture to Zero Touch experience powered by strong AI
- Works across all endpoint types for complete coverage and better insight into trusted behavior
- Provides continuous monitoring and threat detection to ensure data and AI integrity
- Provides contextual and continuous authentication that spans devices, networks, apps, and people
- Builds on an open platform to enable seamless integration with existing solutions

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.