Buyers' Guide
IT Professionals

FREEFORM DYNAMICS

in association with

BlackBerry

Zero Trust: securing the endpoint

How continuous authentication could help secure the work-anywhere world

Freeform Dynamics, 2020

WHY ENDPOINT SECURITY MATTERS

Long gone are the days when an organization's ability to secure its IT largely matched its ability to secure its physical network. Today, your users - and perhaps more importantly, your valuable data - can be almost anywhere. Mobile and remote working was on the rise even before the Covid-19 pandemic accelerated the process, and now it is near-ubiquitous.

So the 21st century network edge is not your office: it's your house, pocket, wrist, or anywhere else that your connected business technology happens to be. That's also now where the 'attack surface' is, and therefore where the threats are, too. That means endpoint security is essential - we all make mistakes, and increasingly we are all targets for malicious operators. Indeed, our mobile devices need even more protection than our office PCs, partly because they move but also because they are often not centrally managed.

BUT WE MUST MAINTAIN USABILITY TOO

One of the risks of adding security without addressing usability is that if you make a process more awkward, users will seek workarounds. The result? Passwords on sticky-notes, people using private email accounts for company business, company data saved on unencrypted USB sticks, and more. Security must be strong, yet easy to use - ideally, it should appear largely transparent to the authorised user.

1. CHANGING NEEDS

THE OLD WAYS	THE CHALLENGE	THE NEW WORLD
Security policies are usually pre-set: one set of policies for in-office devices, another for mobile, and so on. VPNs may provide secure remote connectivity.	Many users use multiple devices and work at multiple sites, including working from home or another remote location at least some of the time. Plus cybercrime is on the rise.	Flexible and versatile security adapts to the user's location. The focus is on protecting user identities and credentials, and sensitive data, but without degrading the user experience.

2. THE RISK ENVIRONMENT

Endpoint threats include device loss and theft, ransomware, WiFi attacks, phishing and other ways of stealing credentials and data.	More complex working patterns increase the attack surface, but applying inflexible security responses or solutions risk increasing it still further.	Adaptive and context-aware endpoint security policies adjust to the current local threat level, while valuable data is independently protected.

3. BUSINESS EVOLUTION

Along with the financial risks of credential theft, preventing data loss or theft is typically both a business imperative and a regulatory requirement.	As digitalization proceeds and mobility grows, we must protect more endpoints, more locations, and more data of many more different types.	Secure mobile working allows organizations to respond flexibly, both to new economic or socio-political opportunities, and to new risks and threats.

ZERO-TRUST AND CONTINUOUS AUTHENTICATION

SOLVING THE SECURITY CHALLENGES

We live in a world where devices and credentials can be lost, stolen or compromised, and where malware can encrypt or destroy our data. That means we can't automatically trust any endpoint security element on its own. Instead, we can achieve strict verification by continuously authenticating users, working in the background to profile their usage and activity. We then check for anomalies and adapt our security posture according to the currently-perceived level of risk, all with little or no extra burden on the user. Here's some key concepts:

ZERO TRUST, ALWAYS SEEK CONFIRMATION

Trust nothing without verification. For example, you might require the user to use multi-factor authentication (MFA) on a known device via a recognized application. Other key elements of zero trust are least-privilege access and microsegmentation, giving users access to only the data and infrastructure elements they need or are authorized for.

CONTEXTUAL AUTHENTICATION

Your security policy should be dynamic and adaptive. Has the device entered a trusted location, or a country with a different regulatory regime? Has the user's behavior changed? You may want to add more security challenges, or if the risk level has fallen, perhaps you can remove some.

BIOMETRICS: IT'S NOT JUST FINGERPRINTS

Face and fingerprint recognition are useful but can be fooled. Harder to trick can be passive biometrics such as using device telemetry. Seeing if the user is left/right handed, how they hold the device, their typing and swipe patterns, and their usage patterns, such as times of day and app activity, can all be usable biometrics to feed into continuous authentication.

BEHAVIORAL ANALYTICS AND CONTEXTS

A key indicator of risk is unusual behavior, but what counts as 'usual' can vary by context. For instance, what's typical for a user in one location at one time of day and year might be very unusual otherwise. Similarly, is the IP address a known one? Are the apps ones that this user typically uses? Is the user simultaneously logged-in on multiple devices in different locations?

CONFIDENCE SCORING

Real-time adaptation and response requires the ability to identify anomalous behavior very rapidly, and flag it with a confidence score that allows appropriate action to be taken automatically. This is a task where AI-based machine learning can comfortably outperform humans.

REMEDIATION AND RESPONSE

If a device moves from one risk level to another, the need for authentication changes too. For instance, at higher risk levels you might shorten the login time-outs, decrease the number of PIN tries allowed, or require re-authentication with MFA before certain apps or data can be accessed. You may even want to wipe sensitive apps and data from the device.

REMEMBER: THE DEVICE IS JUST A VEHICLE. When a device is stolen or a user account is cracked, most perpetrators are after just one thing: money. The two obvious routes to that are identity fraud, and stealing data for resale or ransom. Zero trust and continuous authentication mean that stolen access credentials can only be used by the correct user in a recognized context, which protects both the device and the data it has access to.

UNDERSTANDING THE OPTIONS

Like many other areas of IT, building endpoint security can feel a bit like assembling a jigsaw. Different tools supply different pieces of the puzzle, and even when you think you have bought correctly, you may finish the picture only to find that there is a piece missing - or a piece that simply does not fit with the others.

The list below therefore approaches the puzzle from a functional perspective. For completeness, you could first assess how confident you are in your ability to answer these questions positively today. Then move on to answer them for the endpoint security solutions you're evaluating.

Solution assessment: key considerations

	Level of confidence		
	High	**Medium**	**Low**
Do I have full risk and security visibility across all my endpoint and edge devices?	☐	☐	☐
Can I provide remote users with secure access without needing to use a VPN?	☐	☐	☐
Do my user access policies dynamically adapt to changing risk and authentication profiles?	☐	☐	☐
Are there ways to assess risk and respond automatically, e.g. using behavior and AI/ML?	☐	☐	☐
Do my tools properly share policy changes with each other, e.g. between desktop and mobile?	☐	☐	☐
Must I install software agents or additional applications on my endpoints?	☐	☐	☐
Can I automatically disable, re-enable or even wipe endpoint apps and data?	☐	☐	☐
Can I add protection for new endpoint classes as required, e.g. wearables, smart vehicles, IoT, etc?	☐	☐	☐
Are passive biometrics supported, such as usage patterns and device telemetry?	☐	☐	☐
Can I embed data security into normal productivity apps, and link in third-party zero trust apps?	☐	☐	☐
Can users opt-out of some monitoring, e.g. geolocation, in return for a higher risk score?	☐	☐	☐

ABOUT FREEFORM DYNAMICS

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better-informed investment decisions.

For more information, and access to our research library, visit www.freeformdynamics.com.

ABOUT BLACKBERRY

BlackBerry 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.

BlackBerry. Intelligent Security. Everywhere.

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