Token

Product Brief

BioStick Series

Prevent Phishing & Ransomware
with Gold Standard Biometric MFA

Proactive phishing protection

FIDO compliant, phishing-resistant MFA that eliminates human vulnerabilities and shared secrets which can be exploited.

Biometric identity verification

Even if lost or stolen, biometric user verification ensures that only the registered user can access and use the digital credentials.

Proximity security

Authentication can only be performed when physically near a device. Local MFA eliminates the risk of remote identity attacks.

Domain binding

Cryptographic domain binding ensures authentication is only performed to legitimate services. Phishing sites can no longer be used to steal credentials.

The Future of Enterprise Authentication is Passwordless

Organizations of all types require a secure, passwordless login experience that provides the highest level of assurance and user convenience. Eliminating passwords is the most effective way to prevent phishing, social engineering, and credential theft, which remain the leading attack vectors in successful ransomware attacks and data breaches. Token delivers secure, convenient gold standard biometric MFA.

Moving Beyond Legacy MFA

Next-generation MFA fixes the shortcomings of legacy authentication methods, including vulnerabilities to phishing, man-in-the-middle attacks, sim-swapping, and reliance on users to recognize sophisticated threats.

Legacy MFA is a hassle for users, but the BioStick offers a simpler, passwordless login experience by removing multiple interactional steps with just a quick fingerprint scan.

Token offers a secure, scalable, phishing-proof, gold standard biometric solution, integrating all the benefits of hardware security keys with the flexibility of software-based management.

In comparison to traditional 2FA hardware security keys, a BioStick can only be used by its owner, providing highly secure biometric user identity verification at every login.

BioStick Highlights

Biometric user identity verification

FIDO2/WebAuthn and FIDO U2F compliant

Convenient FIDO authentication via Bluetooth, NFC, and USB

Upgradeable Firmware

Tamper-Resistant Secure Element for safe storage of digital credentials

Compatible with Windows, MacOS, Android, and iOS*

* The availability of non-USB connectivity is subject to the platform's compatibility.

TOKEN BIOSTICK FEATURES

Convenient and Gold Standard Security

Token BioSticks not only offer biometric, FIDO-compliant, phishing-proof multifactor authentication, but also a great user experience. Security and convenience are rarely united, but the Token BioStick Plus provides flexibility and convenience as it can be used across multiple platforms via fully encrypted Bluetooth communications. Users no longer need to plug in their hardware security key and steal a USB port for authentication; one quick tap and fingerprint scan grants them FIDO-secured access in under five seconds. The ease of use promotes user compliance, resulting in a stronger security posture for the entire organization.

Authentication Method Risk Comparison

Attack Vector	Password	Passcode OTP	Legacy MFA & Auth Apps	Passkey	**Token Ring or Token BioStick**
Phishing	X Easy	X Easy	X Easy	✓ No	✓ **No**
Remote Compromise	X Easy	X Easy	X Easy	! Possible	✓ **No**
Fake Website Compromise	X Easy	X Easy	X Easy	✓ No	✓ **No**
Device Theft	! Maybe	! Maybe	X Yes	! Possible	✓ **Not usable**
Cloud Account Hijack	N/A	N/A	X Yes	X Yes	✓ **No cloud used**
Tampering Possible	X Easy	X Yes	X Yes	X Yes	✓ **Not likely (given secure element)**
User Coercion	X Easy	X Yes	X Yes	X Yes	! **Physical in-person only (e.g., with a gun)**

Authentication Use Cases: SSO and Passkeys

A common way to implement passwordless FIDO authentication and hardware security keys is to safeguard existing instances of single sign-on (SSO) or identity provider-based authentication.

The centralization of SSO and IDP systems has improved the end-user experience, but also made it imperative that organizations protect access to these systems from unauthorized personnel. Managing access and authorization, especially privileged access, and identity lifecycles while simultaneously providing adequate security controls and user convenience is a familiar challenge for security teams. Implementing FIDO and hardware security keys is an excellent solution and one that security teams have been searching for. Delivering the highest level of security, phishing-resistant and passwordless authentication, and also the easiest, most convenient experience for end users.

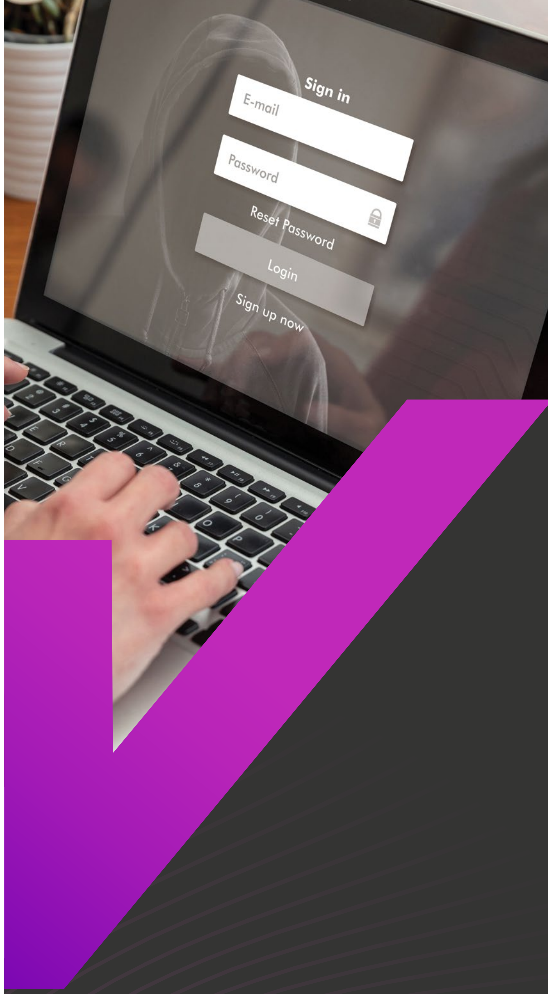
Additionally, a growing range of enterprise products and services are now natively supporting FIDO passkeys for direct authentication between an end user and a relying party. End users of Token hardware security products have the flexibility to choose either (or both) methods as a deployment strategy to align with their organization's needs.

Proactive Security

In recent years, there has been a notable shift among security researchers and professionals. Organizations must no longer rely on a reactive security approach; they must shift their focus to future-proof, preventive security controls.

Identity threat prevention has been especially critical and top of mind, the concern being validated clearly in 2025 threat reports and trends. Credential abuse has seen a steady rise YoY as the most common attack vector, fueling the sentiment "hackers aren't breaking in, they're logging in". The methods used to steal credentials are not sophisticated, yet remain effective due to inevitable human vulnerabilities associated with access and authentication. The use of GenAI has made it easy for attackers to create suave phishing emails and flawless phishing websites, tricking users into revealing their passwords and legacy MFA codes. Combine that with social engineering, AiTM, SIM swapping, prompt bombing, and the 84% increase[1] in Infostealer malware, and it's no surprise identity threat prevention has been making headlines.

Token products can harden proactive security for organizations and their users. Providing the future-proof, biometric, FIDO-certified, gold standard for secure authentication required in 2025 and beyond.



Average cost of a data breach hit a record high of **$4.88 million**[1] in 2024. IBM

TOKEN BIOSTICK TECHNICAL SPECS AND OPTIONS

	Token BioStick	**Token BioStick Plus**
USB-C	✓	✓
Bluetooth		✓
NFC		✓
Biometric user identification	✓	✓
FIDO2 Compliant	✓	✓
FIDOU2F	✓	✓
Upgradable Firmware	✓	✓

Two Models. One Seamless User Experience.

Both models in the Token BioStick series are fully field-upgradable, work seamlessly with the same applications and the Token software platform, and offer a consistent user experience across the board. This ensures that regardless of which Token BioStick is chosen, users and enterprises benefit from the same great features and ease of use.

The key difference between the models lie in their connectivity options. The base Token BioStick offers only USB connectivity; the Token BioStick Plus adds Bluetooth functionality and NFC capability. Additionally, the Plus has an internal, rechargeable battery to make it fully functional even when not connected to a USB port.

Technical Specifications

- Charges via 5V USB-C connection
- Operating Temperature: 0°C to 60°C (32°F to 140°F)
- Charging Time: Approximately 2 hours
- Tamper-Resistant Secure Element supports up to 100 unique resident keys/credentials
- 508 DPI capacitive fingerprint sensor
- BLE 5.4
- Battery Life: Lasts up to one week between charges
- Immediate Usability: Operates whenever plugged in, regardless of battery charge level

The deployment of FIDO security keys resulted in **zero account takeovers, four times faster logins**, a **92% reduction in IT work calls**, and a **95% reduction in password resets.**[2]

Reduction of IT Support Needs

Token hardware products are designed to address enterprise IT requirements in two distinct ways:

1. **Token BioSticks prevent ransomware and data breaches that result from inadequate authentication methods, including legacy forms of multifactor authentication (MFA).**
2. **Token BioStick authenticators significantly reduce the frequency of password resets, a common IT support request.**

Studies conducted by Google, Hyper, and others have demonstrated that the deployment of FIDO security keys resulted in zero account takeovers, four times faster logins, a 92% reduction in IT work calls, and a 95% reduction in password resets.[2]

Designed for Mass Deployment

Organizations can manage their Token hardware security keys using the Token Authenticator Console. It offers seamless key management, ordering, shipping, and return processing. Administrators gain comprehensive access to hardware assignments, status updates, logging information, and the ability to customize Token security hardware for specific groups without compromising the security of biometric authentication or private keys.

Professional Services

Token offers a wide range of professional services to assist organizations through the adoption of Token's FIDO security keys, including:

- IDP configuration
- Integration with existing ecosystems
- Token Product training
- End User Setup and Registration

We understand the urgency to secure your organization's vulnerable assets and identities with phishing-resistant authentication. Our dedicated engineers are here to support in whatever way your individual organization needs.

[1] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
[2] https://fidoalliance.org/

About Token

In a world of stolen identities and compromised user credentials, Token is changing the way our customers secure their organizations by providing passwordless, FIDO2-compliant, biometric, multifactor authentication. To learn more, visit **www.tokenring.com**.