Token

Product Brief

Stop Ransomware Attacks With Next-Generation MFA

Token Ring provides the strongest MFA for the ultimate protection against ransomware, data breaches, and BYOD vulnerabilities

Why Legacy MFA is No Longer Enough

It's a simple fact — the overwhelming majority of successful ransomware attacks and data breaches start with a phishing email followed by the cybercriminals defeating the victim's legacy MFA solution. CISA, the Cybersecurity and Infrastructure Security Agency, an operating component of the U.S. Department of Homeland Security reports that phishing attacks account for 90% of ransomware. Similar reports have been issued by leading cybersecurity providers, including Cisco and others.

Legacy MFA is 20-year-old technology and is being defeated every day with simple attack methods that include SIM-Swapping and BYOD device corruption, MFA Prompt Bombing/MFA fatigue attacks, malicious websites stealing credentials and OTPs, and session hijacking and stealing session cookies.

On top of this, organizations now face the nearly impossible task of protecting against attacks that harness the incredible power of generative-AI, where the traditional hallmarks of a phishing email are absent. What happens when even the best-trained users encounter emails that are perfectly crafted using generative AI to appear like a normal email?

Next-generation MFA is the strongest possible way to reduce cybersecurity vulnerabilities and protect organizations from cybercriminal attacks.

Next-Generation, Wearable MFA with Token Ring: The Ultimate in Enterprise Security

Token Ring is a next-generation passwordless, biometric, FIDO2 compliant, wearable authenticator that delivers the strongest MFA available. It protects your organization's privileged users against cyberattacks that steal user credentials and defeat legacy MFA. It does this by mitigating the methods used by cybercriminals in 90% of ransomware attacks. Token Ring prevents MFA fatigue, Adversary-in-the-Middle (AitM), and other attacks frequently used by cybercriminals to breach organizations.

Token Ring eliminates the vulnerabilities of legacy MFA and the need for users to be an expert at identifying sophisticated phishing emails, a task that is becoming increasingly challenging with cybercriminals' adoption of generative AI.

Secure Credentials, Secure Authentication, Secure Organization

Compromised user credentials and cybercriminals defeating legacy MFA are by far the #1 contributing factor to data breaches and ransomware losses. That's why the ability to keep credentials safe is a must for every organization. Unfortunately, legacy MFA solutions cannot offer the security and level of assurance that a person is who they claim to be. Token Ring secures user credentials by safely storing them on an EAL5+ certified secure element.

Token Ring Provides an Easy Path to Passwordless Access

If your users don't have a password they know, it cannot be stolen or phished by cybercriminals. Token Ring incorporates intuitive touch and biometric user verification that allows only the authorized user to authenticate and only when they intend to. Thus, it provides all the benefits of MFA plus passwordless login in a single step.

Token Ring secures user credentials by safely storing them directly on the ring. With a 508-dpi capacitive touch fingerprint sensor for on-device biometric matching, Token Ring delivers the highest level of security available.

Wearable Authentication that's Always Safe and Always Available

Token Ring is effective against phishing attacks, BYOD vulnerabilities, lost and stolen credentials, weak passwords, credential stuffing, and easily stolen SMS one-time passcodes. It's also extremely flexible as it can be used across multiple devices via fully encrypted and secure NFC and Bluetooth communication technologies — allowing the user to switch between them as needed. Easy to implement, Token Ring delivers FIDO2 support and works with all leading IAM and SSO solutions.

Moreover, since it always remains with the user, it is safe and immediately available for authentication. Only the authorized user can use the device and no attacker can access the user biometrics, credentials, and keys stored on it. Since biometrics never leave the ring, they can never be stolen from a mobile device, server, or the cloud — a big plus for compliance.

Easy 3-Step Enterprise Security with Token Ring

Token Ring is changing the enterprise security landscape with innovative, extremely secure wearable biometric authentication. Packed with cutting-edge security technology in a tiny footprint, Token Ring delivers the strongest authentication possible in 3 easy steps:

STEP 1	STEP 2	STEP 3
Token evaluates the customer organization's current MFA security posture	Token provides a fast and easy proof of concept	Token implements the ring for authorized users

Token Ring addresses enterprise-wide security requirements for multiple users and unlimited use cases. We are dedicated to the fast implementation of our solution and committed to ensuring that all users enjoy a convenient authentication experience every time they use Token Ring.

Technical Specs

LEDs Status Indicator The multi-color LEDs relay a variety of information, including the battery level, fingerprint scan success, authentication success, Bluetooth/NFC status, and more.

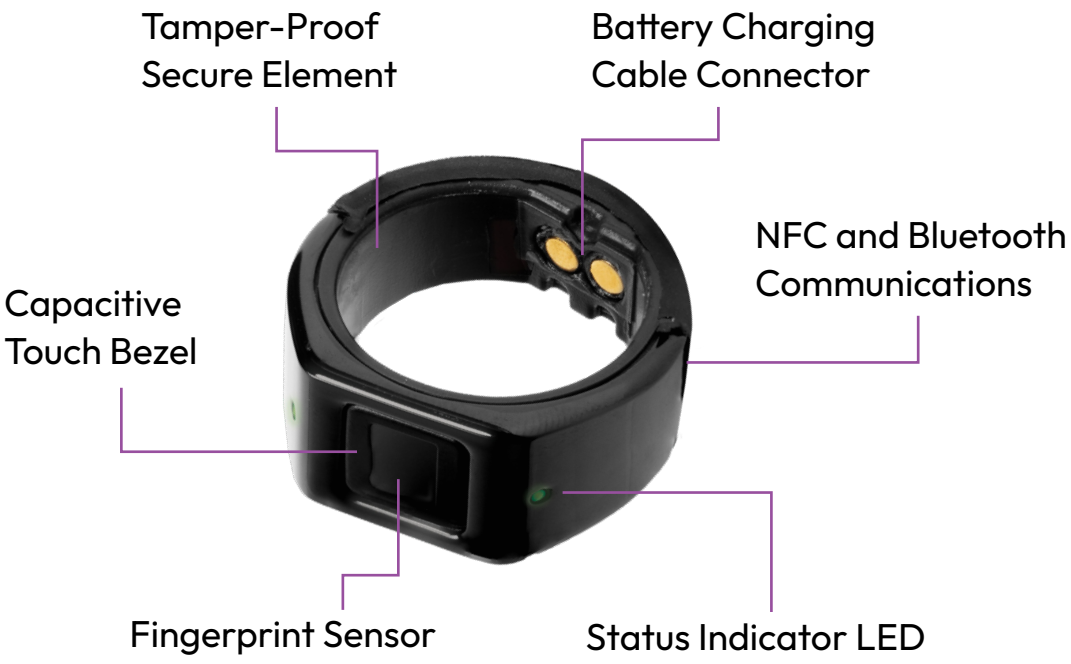
Fingerprint Sensor The fingerprint sensor handles user verification and authentication by matching the scanned fingerprint to the stored fingerprint template directly on the ring. Only the registered user's fingerprint can enable authentication on the ring.

Capacitive Touch Bezel The Token Ring has a capacitive touch bezel that serves as the gestural input for the ring and enables verifying user presence and intent.

Secure Element The Secure Element generates and securely stores all user FIDO credentials. It is tamper-proof and will be destroyed if any attempt is made to access it by physical disassembly.

NFC and Bluetooth Interface Supports encrypted and secure Bluetooth and NFC wireless transfer of data, ensuring seamless use across all popular devices.

Battery Charging Cable Connector This allows the user to charge their Token Ring with a simple USB C cable – no charging station or dock is required. The charging cable is included with the ring.



Token

Device and OS Support

- Mobile via Bluetooth and NFC
  - iOS
  - Android
- Computer via Bluetooth and NFC
  - Windows
  - MacOS

Authentication method: FIDO2

- FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments
- Every key generated by the Token's FIDO2 authenticator is stored on the device itself, in a Common Criteria EAL5+ certified secure hardware environment
- All cryptographic signing is implemented using the ES256 Elliptic Curve algorithm
- Support for up to 100 unique resident keys
- PIN or passwordless supported
- PIN and biometric verification supported

Fingerprint sensor

- 508 dpi capacitive touch
- 5.45mm x 6.10mm
- 8 bit greyscale resolution

LED light

- Multicolor status indication

Secure element

- EAL5+ Verified. Tamper-Proof
- Storage for 100+ keys

Bluetooth

- BLE 5.4
- Touch enabled

NFC

- NFC enabled
- Touch enabled

Battery

- ~20 hours with normal use
- Time to fully charge: 45 – 90 minutes
- Recovery charge 5 minutes

Charger

- USB C 5 volt

Form factor: ring

- Ring sizes: 6 - 14 whole sizes*
- Dimensions: size 10 ring – 28mm OD 25mm ID
- Weight: 2 – 5 grams

Water resistance

- IP68 water and dustproof enclosure rating

Operating temperature

- 0°- 60° C

Next-Generation MFA versus Legacy MFA

	TOKEN	SMS	AUTHENTICATION APPS	HARDWARE KEYS	PASSKEYS
Biometrics protected via local device storage and matching	✓	✗	✗	✗	✗
Works with leading IAM Solutions	✓	✓	✓	✓	✓
Effective against phishing attacks	✓	✗	✗	✗	✓
Keys stored locally only	✓	✗	✗	✓	✗
No BYOD vulnerabilities	✓	✗	✗	✓	✗
Secured with biometrics	✓	✗	✗	✗✓	✗✓
Passwordless login support	✓	✗	✗	✗	✓
Easy to implement	✓	✓	✗	✓	✓
No 6 to 12-digit OTP codes to enter	✓	✗	✗	✗✓	✓
FIDO 2.1 Support	✓	✗	✗	✓	✓

The Benefits of Biometric Wearable Authentication

1. **Only the authorized person can use the device** for device and network access.
2. No more lost or stolen dongles means **fewer help desk calls,** dongle replacements, and less loss of productivity.
3. The **biometrics never leave the ring** – they cannot be stolen from a device or server.
4. **The secrets/keys cannot be accessed by an attacker.** They are stored in an embedded and tamper-proof Secure Element.

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**.