Osterman Research Surveys Show IT & Security Decision-Makers Plan Investments in Multi-Factor Authentication & Zero Trust Solutions to Counter Rising Cyberthreats

WALL, NJ – December 13, 2021 - **BIO-key International, Inc.** (Nasdaq: BKYI), an innovative provider of Identity and Access Management (IAM) and Identity-Bound Biometric (IBB) solutions, today announced research findings from IT decision-maker surveys conducted with **Osterman Research**, a leading cybersecurity, data protection and information governance market research firm. The two research programs surveyed over 290 security and IT professionals across a variety of mid to large organizations to determine the factors influencing their application and investment in multi-factor authentication (MFA) and Zero Trust cybersecurity. Zero trust is a more secure paradigm providing ongoing verification of trustworthiness. The survey research is available on the BIO-key website via these links: The State of MFA and Why Zero Trust is Important.

The research revealed a wide gap between what IT and security decision makers understand to be highly secure MFA methods and the methods currently implemented within their organizations. As a result, most organizations (63%) plan to increase future investments in MFA for employees over the next five years, particularly with a focus on passwordless security features (40%).

While earlier security approaches assumed people and devices within a network were trustworthy, Zero Trust approaches reject this assumption and require ongoing verification of trustworthiness. Broad awareness of security threats to organizations and enterprises is proving to be a key driver of Zero Trust adoption. For example, 53% of IT and security decision makers said that they were influenced to adopt more secure solutions by high profile ransomware incidents such as SolarWinds, Colonial Pipeline and JBS. Furthermore, 38% of respondents said the pandemic era digital transformation influenced their adoption of Zero Trust.

MFA Awareness and Current Adoption at Odds

Single-Factor Authentication (SFA) is a method where users access resources by having them present only one way of verifying their identity, such as the use of a password. While most organizations surveyed still rely on password-based authentication for employee security, many have plans to move to passwordless solutions. Companies are using passwordless authentication even less with their customers, and most companies surveyed have no current plans to move customer access to passwordless MFA solutions.

While decision makers were found to have a good understanding of the need and value of multi-factor authentication and its applications, the research demonstrated a serious disconnect between what decision makers perceive to be highly secure MFA methods and what they have implemented for authentication. For example, although 60% of respondents perceived biometrics to be one of the most secure MFA methods, only 27% of organizations use them for employees and only 13% do so for

customers. The majority of decision makers plan to address this disconnect with increased investment in MFA solutions, especially around biometric authentication.

Additional insights include:

- An average of 70% of employees and 40% of customers are required to use MFA to access corporate applications and data.
- Only 26% of those surveyed believe passwords as an authentication method are highly secure, yet 85% of organizations still use them for employee access and 78% continue to use passwords for access by customers.
- 40% of organizations plan to implement passwordless authentication workflows for employees.
- When working with customers, only 9% of organizations have implemented passwordless authentication workflows for customers, while 23% are planning to do so.

The Driver for Implementing Zero Trust

A second research program focused on the trends which have impacted respondents' decisions to embrace a Zero Trust architecture. Key drivers for deploying this architecture noted as "extremely impactful" or "highly impactful" by respondents include:

- High profile ransomware incidents (53%)
- Work-from-home workforce (51%)
- General ransomware attacks (51%)
- Credential theft (45%)
- Pandemic-accelerated digital transformation (38%)

Most respondents were looking to external factors and other risk awareness as key drivers to adoption. Organizations see Zero Trust approaches as enabling stronger cybersecurity protections primarily focused on internal matters. Key deployment drivers include:

- 78% of respondents view confidential files — secret, sensitive, and other protected information held within the organization — as the most important data source to include in Zero Trust initiatives.
- 73% of respondents who make decisions on IAM for employees consider Zero Trust solutions as a key design modification.

Survey Methodology

BIO-key conducted two surveys in partnership with Osterman Research. Study findings are based upon 294 completed surveys. The MFA and Passwordless Survey was composed of 169 individuals in organizations with a median of 1,500 employees. The Zero Trust Survey polled 125 IT and security decision-makers in mid-and large-sized organizations (11,992 average employees; 1,500 median employees).

Visit BIO-key's website to view these research studies and other relevant content.

About BIO-key International, Inc. (www.BIO-key.com)
BIO-key has over two decades of expertise in providing authentication technology for thousands of organizations and millions of users and is revolutionizing authentication with biometric-centric, multi-factor identity and access management (IAM) solutions, including its PortalGuard IAM solution, that provides convenient and secure access to devices, information, applications, and high-value transactions. BIO-key's patented software and hardware solutions, with industry leading biometric capabilities, enable large-scale on-premises and cloud-based Identity-as-a-Service (IDaaS) solutions, as well as customized enterprise solutions.

BIO-key Safe Harbor Statement
All statements contained in this press release other than statements of historical facts are "forward-looking statements" as defined in the Private Securities Litigation Reform Act of 1995 (the "Act"). The words "estimate," "project," "intends," "expects," "anticipates," "believes," and similar expressions are intended to identify forward-looking statements. Such forward-looking statements are made based on management's beliefs, as well as assumptions made by, and information currently available to, management pursuant to the "safe harbor" provisions of the Act. These statements are not guarantees of future performance or events and are subject to risks and uncertainties that may cause actual results to differ materially from those included within or implied by such forward-looking statements. These risks and uncertainties include, without limitation, our history of losses and limited revenue; our ability to raise additional capital; our ability to protect our intellectual property; changes in business conditions; changes in our sales strategy and product development plans; changes in the marketplace; continued services of our executive management team; security breaches; competition in the biometric technology industry; market acceptance of biometric products generally and our products under development; the duration and severity of the current coronavirus COVID-19 pandemic and its effect on our business operations, sales cycles, personnel, and the geographic markets in which we operate; delays in the development of products and statements of assumption underlying any of the foregoing as well as other factors set forth under the caption see "Risk Factors" in our Annual Report on Form 10-K for the year ended December 31, 2020 and other filings with the Securities and Exchange Commission. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date made. Except as required by law, the Company undertakes no obligation to disclose any revision to these forward-looking statements whether as a result of new information, future events, or otherwise. Additionally, there may be other factors of which the Company is not currently aware that may affect matters discussed in forward-looking statements and may also cause actual results to differ materially from those discussed. In particular, the consequences of the coronavirus outbreak to economic conditions and the industry in general and the financial position and operating results of our Company, in particular, have been material, are changing rapidly, and cannot be predicted.

Engage with BIO-key
Facebook – Corporate: https://www.facebook.com/BIOkeyInternational/
LinkedIn – Corporate: https://www.linkedin.com/company/bio-key-international
Twitter – Corporate: @BIOkeyIntl

Twitter – Investors: @BIO_keyIR
StockTwits: BIO_keyIR

BIO-key Media Contact
Mary Amenta
Matter Communications
BIO-key@matternow.com
860-550-1736

Investor Contacts
William Jones, David Collins
Catalyst IR
BKYI@catalyst-ir.com
212-924-9800