/KYE: Know Your Employee - The Future of Corporate Security

Empowering Organizations with Secure, Frictionless Identity Management

VeriDas

INDEX

The Evolving Landscape of Corporate Security

In today's digital age, organizations operate within a complex and ever-changing threat landscape. Cyberattacks are becoming increasingly sophisticated, with malicious actors employing a wide range of tactics to infiltrate networks, steal data, and disrupt operations. The financial consequences of these attacks can be devastating, with businesses facing hefty fines, reputational damage, and even operational shutdowns.

Beyond the digital realm, physical security threats remain a constant concern. Theft, vandalism, and unauthorized access can compromise valuable assets, disrupt workflow, and endanger personnel. The expanding attack surface, with growing numbers of employees working remotely and accessing corporate resources through personal devices, further complicates the security equation. Last year, more than USD$1 trillion in revenue was lost by companies as a consequence of physical security incidents. Economic unrest is expected to be the greatest security-impacting hazard in the next 12 months, a significant increase on the prior year. One in four publicly-listed companies reported a drop in their value following a physical security incident over the last year.

To effectively navigate this challenging environment, organizations need to move beyond traditional security approaches. Siloed solutions that focus solely on physical or digital security are no longer sufficient. As Jordan Avnaim, CISO for Entrust, corroborates: When working in tandem, physical and digital security measures can greatly reduce the risk of attacks businesses routinely find themselves defending against on a daily basis. What's essential is a holistic approach that integrates physical and digital security measures, with a strong emphasis on identity management.

> "Last year, more than USD$1 trillion in revenue was lost by companies as a consequence of physical security incidents.

This ebook will explore the concept of Know Your Employee (KYE), a comprehensive security framework that empowers organizations to gain a deeper understanding of their workforce. By verifying employee identities, controlling access to critical resources, and continuously monitoring activity, KYE strategies can significantly enhance security posture while streamlining workflows and improving the user experience.

Are you ready to learn how KYE can transform your organization's security strategy?
Join us as we delve into the critical trends shaping corporate security, explore the benefits of KYE, and discover how Veridas's innovative solutions can empower you to build a more secure and efficient future.

/Trends and Challenges in Corporate Security in 2024

The Rise of Sophisticated Cyberattacks

The digital age has ushered in an era of unprecedented opportunity, but it has also brought with it a growing threat: sophisticated cyberattacks and insider threats. Malicious actors are constantly innovating and developing new techniques to infiltrate corporate networks, steal sensitive data, and disrupt critical operations. These attacks can have a crippling impact on businesses, leading to significant financial losses, reputational damage, and even operational shutdowns.

RANSOMWARE ATTACKS

Ransomware attacks have become a particularly potent threat. These attacks involve encrypting an organization's data, effectively holding it hostage until a ransom is paid. The consequences can be severe, forcing companies to halt operations, pay hefty ransoms, or even lose valuable data permanently.

IDENTITY FRAUD

Identity fraud is another growing concern, as cybercriminals steal personal information to impersonate legitimate users and gain unauthorized access to systems or accounts.

PHISHING SCAMS

Phishing scams remain a prevalent threat, exploiting human vulnerabilities to trick employees into revealing sensitive information or clicking on malicious links. These attacks can be highly sophisticated, with emails often designed to appear legitimate and impersonate trusted sources.

DATA BREACHES

Data breaches continue to plague businesses of all sizes. Hackers exploit vulnerabilities in security systems to access and steal sensitive data, such as customer information, financial records, and intellectual property. The repercussions of a data breach can be far-reaching, leading to hefty fines, lawsuits, and a loss of customer trust.

INSIDER THREATS

Insider threats pose a significant risk, as disgruntled employees or those with malicious intent may use their authorized access to harm an organization. This can include stealing data, sabotaging systems, or even committing fraud. Employee negligence can also lead to security breaches. Simple mistakes, such as using weak passwords or failing to follow security protocols, can create opportunities for attackers.

The financial impact of these attacks is staggering. The global cost of cybercrime is expected to reach $10.5 trillion annually by 2025[1]. These attacks can cripple businesses, forcing them to invest heavily in recovery efforts and potentially causing irreparable damage to their reputation.

In the face of these evolving threats, it's crucial for organizations to adopt a holistic approach to security that encompasses both physical and digital security measures, with a strong emphasis on identity management. By verifying employee identities, controlling access to critical resources, and continuously monitoring activity, organizations can significantly enhance their security posture, mitigate insider threats, and protect their valuable assets.

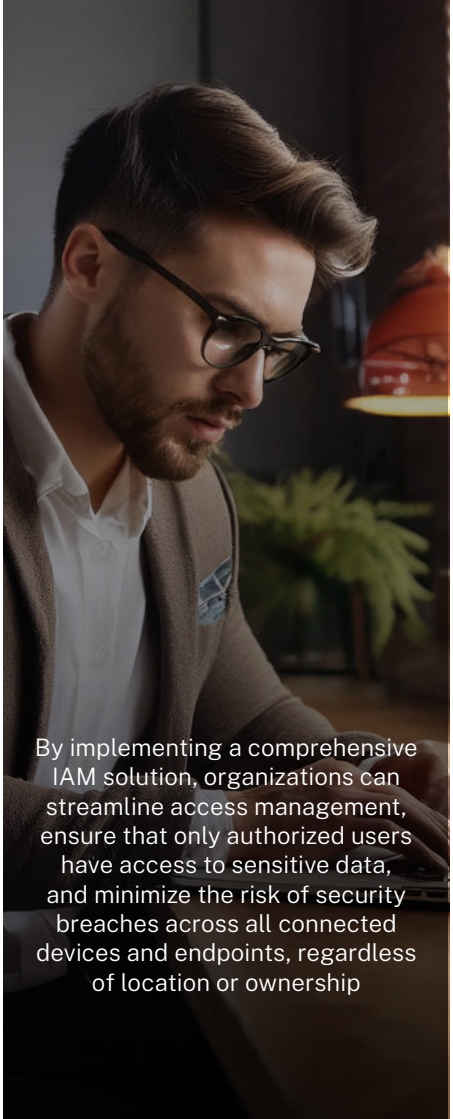
> The global cost of cybercrime is expected to reach $10.5 trillion annually by 2025.

1 - Cyber Security Ventures

The Expanding Attack Surface

The digital landscape is constantly evolving, with a growing number of devices and endpoints connecting to corporate networks. This includes traditional desktops and laptops, as well as a vast array of mobile devices, tablets, Internet of Things (IoT) devices, and cloud-based applications. This expanding attack surface presents a significant challenge for organizations seeking to maintain a robust security posture.

Securing remote workers has become a pressing concern. The rise of remote work arrangements necessitates securing access for employees who may be located outside the traditional office environment. This can make it difficult to enforce security protocols and monitor employee activity effectively.



By implementing a comprehensive IAM solution, organizations can streamline access management, ensure that only authorized users have access to sensitive data, and minimize the risk of security breaches across all connected devices and endpoints, regardless of location or ownership

BYOD (Bring Your Own Device) environments add another layer of complexity. When employees use their personal devices for work purposes, organizations lose some control over the security of those devices. Malicious actors may target these devices to gain access to corporate networks.

Identity & Access Management (IAM) solutions are essential for mitigating the risks associated with the expanding attack surface. Robust IAM solutions provide centralized control over user access, allowing organizations to:

- **Authenticate users:** Verify the identity of users attempting to access corporate resources.
- **Authorize access:** Gran users access to specific resources based on their roles and permissions
- **Audit access:** Track user activity and identify any suspicious or unauthorized access attempts.

The Human Factor: The Weakest Link

Despite the sophistication of modern security systems, the human element remains a critical vulnerability. **Human error** plays a significant role in cybersecurity breaches, often creating openings that attackers can exploit.

Simple mistakes like using weak passwords, clicking on suspicious links, or failing to report suspicious activity can have devastating consequences. Phishing scams, for instance, rely on human error by tricking employees into revealing sensitive information or clicking on malicious links that can download malware or grant unauthorized access to systems.

Social engineering tactics are particularly effective in exploiting human vulnerabilities. These tactics manipulate emotions, exploit trust, and create a sense of urgency to trick employees into taking actions that compromise security. For example, a social engineering attack might involve impersonating a trusted source, such as an IT administrator, and requesting sensitive information or access credentials.

Employee training and awareness programs are essential for mitigating the risks associated with human error. By educating employees about common cybersecurity threats and social engineering tactics, organizations can empower them to identify and avoid scams, protect sensitive information, and report suspicious activity. These programs should be:

- **Regularly updated:** Keep pace with evolving attack techniques to ensure employees are aware of the latest threats.
- **Interactive and engaging:** Utilize a mix of training methods, including simulations and real-world scenarios, to enhance knowledge retention and behavior change.
- **Tailored to specific roles:** Address the specific vulnerabilities and threats employees encounter

> By fostering a culture of security awareness and equipping employees with the knowledge and skills they need to identify and avoid threats, organizations can significantly reduce the risk of human error-related breaches and strengthen their overall security posture.

/KYE: A New Concept for Corporate Security

In today's complex threat landscape, traditional security measures that rely solely on passwords and physical access control cards are no longer sufficient. Organizations need a more comprehensive approach to securing their assets and data. This is where the concept of Know Your Employee (KYE) comes into play.

Introducing the KYE Concept: A New Paradigm in Corporate Security

KYE is a strategic security framework that goes beyond simply verifying employee identities during the onboarding process. It's a continuous process that focuses on gaining a deeper understanding of your workforce throughout their employment journey. This involves verifying identities, managing access controls, and monitoring employee activity for suspicious behavior.

Why is KYE so important? Traditional authentication methods, like passwords and key cards, are vulnerable to theft, loss, and social engineering attacks. Hackers can easily exploit weak passwords or trick employees into revealing credentials.

KYE offers a more robust approach by:

Strengthening identity verification: Utilizing multi-factor authentication and biometrics can significantly enhance the security of employee logins.

Enhancing access control: KYE allows for granular access controls, granting employees access to specific resources based on their roles and responsibilities. This minimizes the potential for unauthorized access and data breaches.

Promoting continuous monitoring: KYE encourages monitoring employee activity for suspicious behavior that may indicate compromise or malicious intent.

The benefits of a comprehensive KYE approach are numerous:

Improved security posture: Mitigates the risk of unauthorized access, data breaches, and insider threats.

Enhanced user experience: Streamlines access to resources by replacing complex passwords with more convenient and secure authentication methods.

Reduced IT costs: Eliminates the need for frequent password resets and manual access control management.

Increased compliance: Helps organizations meet regulatory requirements for data protection and access control.

By implementing a KYE strategy, organizations can transform their security posture, build trust with their employees, and create a more secure and productive work environment.

The Pillars of KYE: Building a Strong Foundation for Security

The KYE framework rests upon three key pillars that work together to create a robust security posture, and address the critical apects of employee identity, access, and activity, ensuring a comprehsive approach to security.

REAL IDENTITY VERIFICATION

The foundation of any KYE strategy is establishing trust through verifying the authenticity of employee identities. This process goes beyond simply checking government-issued IDs during onboarding. KYE leverages advanced solutions to ensure the legitimacy of employee identities and prevent unauthorized access.

This can involve techniques like:

Document verification:
Utilizing sophisticated tools to validate the authenticity of government-issued IDs and passports.

Selfie and Liveness Detection:
Verifying the identity presenting the document through a secure selfie capture process. Liveness detection technology ensures the person presenting the ID is a live person, further mitigating the risk of fraudulent activity.

ACCESS CONTROL

KYE moves beyond simply verifying identity; it also focuses on granting employees access to authorized resources based on their roles and responsibilities. This principle of least privilege ensures that employees only have access to the data and systems they need to perform their jobs effectively. KYE strategies implement robust access control measures like:

Role-based access control (RBAC):
Assigning access permissions based on predefined roles within the organization. An employee in the marketing department wouldn't have access to the same systems as someone in finance.

Attribute-based access control (ABAC):
Granting or denying access based on dynamic attributes, such as location, device type, or time of day. This ensures additional security layers beyond simply the employee's role.

Data Loss Prevention (DLP):
Implementing technologies that prevent sensitive data from being accidentally or maliciously transferred or shared outside of authorized channels.

CONTINOUS MONITORING

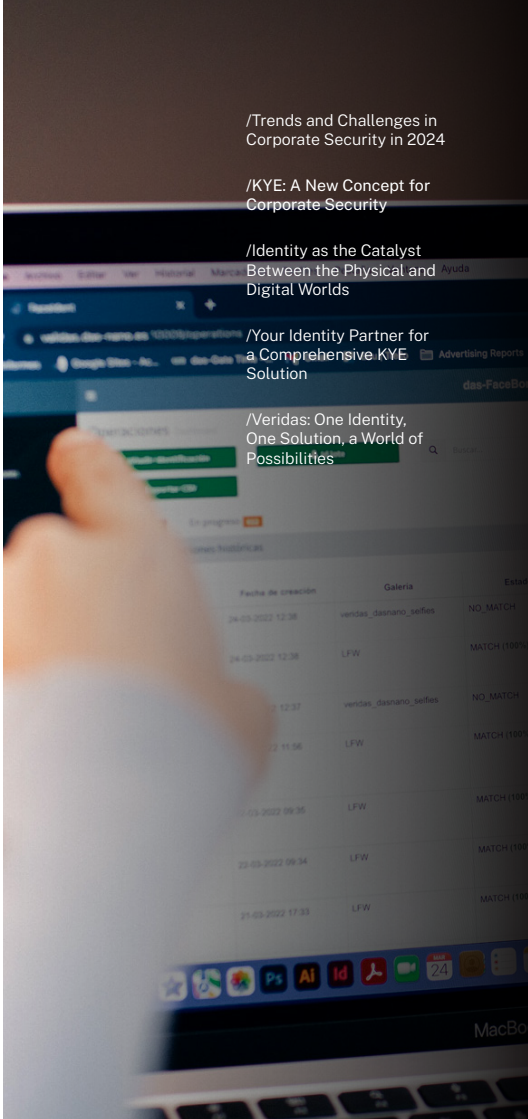
The KYE approach goes beyond initial verification and access control; it emphasizes continuous monitoring of employee activity. This helps to identify any suspicious behavior that may indicate compromise or malicious intent. KYE utilizes monitoring solutions to track:

User login attempts:
Monitoring login attempts for unusual activity, such as failed logins from unexpected locations or attempts outside of regular working hours.

File access and download activity:
Tracking access and download attempts for sensitive data to identify potential data breaches or exfiltration attempts.

Unusual activity within applications:
Monitoring employee activity within specific applications for any unauthorized actions or deviations from standard protocols.

These three pillars – identity verification, access control, and continuous monitoring – work together to create a comprehensive and effective KYE strategy. By implementing these measures, organizations can significantly enhance their security posture, build trust with their workforce, and create a more secure and productive work environment.



The Benefits of KYE: A Secure and Efficient Future for your Organization

Implementing a KYE (Know Your Employee) strategy offers a multitude of benefits that go beyond simply safeguarding your data. It can transform your security posture, enhance employee experience, and streamline operations, ultimately contributing to a more successful and efficient organization.

Enhanced Security Posture

Reduced Risk of Unauthorized Access and Data Breaches:
A Ponemon Institute study revealed that the global average cost of a data breach in 2023 reached a staggering $4.35 million. KYE mitigates these risks by strengthening identity verification, enforcing granular access controls, and enabling continuous monitoring. This multi-layered approach significantly reduces the opportunities for unauthorized access and data breaches, protecting your organization's critical assets and financial well-being.

Improved Employee Experience

Frictionless Access to Resources:
Imagine a work environment where employees don't need to juggle complex passwords or wait for IT support to reset forgotten credentials. KYE solutions like biometric authentication offer a more convenient and secure way to access resources, boosting employee satisfaction and productivity. A study by Unisys found that 72% of employees believe that strong authentication solutions improve their overall work experience.

Reduced IT Costs

Lower Overhead Expenses:
Managing password resets, access control changes, and security incidents can be a significant drain on IT resources. KYE streamlines these processes, automating tasks and reducing the need for manual intervention. Additionally, the reduction in security breaches lowers the associated costs of investigation, remediation, and regulatory compliance. A report by Gartner predicts that security and risk management spending will reach $168 billion in 2023. Implementing KYE can help optimize these expenses by focusing resources on proactive security measures.

By investing in KYE, organizations gain a significant return on investment (ROI) by fostering a more secure, efficient, and employee-centric work environment. The benefits extend beyond immediate cost savings, contributing to a stronger brand reputation, increased customer trust, and ultimately, a more competitive advantage in today's digital landscape.

/Identity as the Catalyst Between the Physical and Digital Worlds

The digital age has blurred the lines between the physical and digital realms. This is particularly evident in the realm of security, where physical and digital identities are becoming increasingly intertwined.

The Convergence of Physical and Digital Identities

The Blurring Lines of Security Environments:

Traditionally, physical security relied on separate systems and credentials. Access control cards or keys granted entry to buildings and restricted areas, while usernames and passwords facilitated access to digital resources. However, these siloed approaches create vulnerabilities. Lost badges can be used for unauthorized access, and weak passwords can be compromised, jeopardizing both physical and digital security.

The Rise of Integrated Solutions:

The growing interconnectedness of our world is driving a convergence in security solutions. Organizations are increasingly adopting integrated security systems that combine physical access control systems with digital identity management platforms. These integrated systems leverage a single set of employee credentials to grant or deny access to both physical locations and digital resources.

For example, imagine an employee approaching the office building. As they walk towards the entrance, they step into the field of view of a facial recognition terminal mounted near the door. The terminal automatically scans their face and compares it to the stored facial templates in the company's identity management system. Upon successful authentication, the door unlocks, allowing the employee to enter.

Inside the building, the employee can use another facial recognition terminal to activate the elevator. The terminal again scans their face and, upon successful authentication, presents a touch screen interface where the employee can select their desired floor. The elevator automatically takes them to their designated floor.

At their desk, the employee can continue using a dedicated facial authentication system to log in to their workstation. The terminal scans their face and, upon successful authentication, automatically logs them in to their computer, providing access to all necessary company resources, including internal systems and applications.

This seamless experience demonstrates the power of a unified identity approach that utilizes facial recognition terminals to streamline access across physical and digital environments. By eliminating the need for physical credentials, mobile apps, and passwords, organizations can enhance security, improve user experience, and reduce IT overhead.

The Need for a Unified Approach:

This convergence of physical and digital security highlights the critical need for a unified approach to identity management. By leveraging a single platform to manage both physical and digital access, organizations can:

> By adopting a unified approach to identity management, organizations can create a more secure and user-friendly security environment, fostering a productive and efficient work experience for their employees.

Enhance security

Mitigate the risk of unauthorized access by streamlining the authentication process and eliminating the need for multiple credentials. A compromised password no longer translates to compromised physical access, and a lost badge becomes less of a security concern.

Improve user experience

Provide employees with a more convenient and efficient way to access resources, regardless of location or device. Employees no longer need to juggle multiple logins and credentials, simplifying their workday.

Reduce IT overhead:

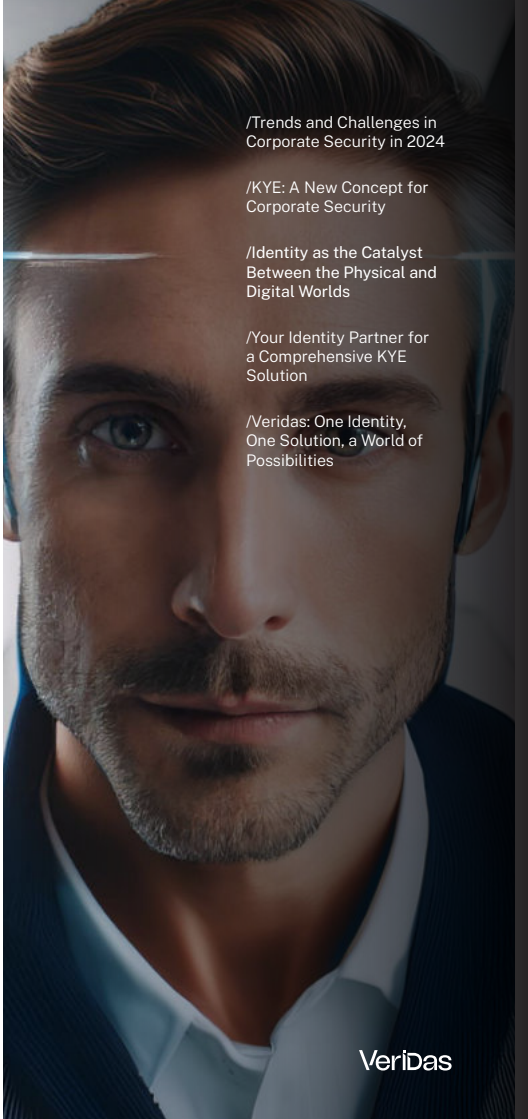
Simplify user provisioning and access management, streamlining IT operations and reducing administrative costs. A single platform for managing identities translates to less time spent managing multiple systems and credentials.

The Role of Biometrics in KYE

In today's evolving security landscape, traditional authentication methods like passwords and access cards are becoming increasingly vulnerable. Biometrics, the science of verifying a person's identity based on unique physical or behavioral characteristics, offers a powerful solution for KYE strategies.

Advantages of Biometric Authentication:

- **Enhanced Security:** Biometric characteristics like facial features or voice patterns are unique to each individual. Unlike passwords or access cards, which can be lost, stolen, or shared, biometrics provide a more secure and reliable way to verify identities. This significantly reduces the risk of unauthorized access to sensitive data and resources.
- **Improved Convenience:** Biometric authentication eliminates the need for employees to remember complex passwords or carry multiple access cards. Employees simply scan their fingerprint, face, or iris to gain access, streamlining the login process and improving user experience.
- **Reduced Risk of Human Error:** Forgotten passwords or lost access cards can lead to security breaches and productivity disruptions. Biometric authentication removes this human element, providing a more reliable and consistent method for user verification.



Biometrics: Security and Convenience with Privacy Considerations

Despite the undeniable advantages, the use of biometrics in KYE raises concerns about privacy and data security. Here's how organizations can address these concerns:

- **Transparency and Consent:** Organizations must be transparent about how they collect, store, and use biometric data. Employees should be informed about the security measures in place and have the option to opt-in or opt-out of biometric authentication.
- **Data Security:** Biometric data should be encrypted and stored securely. Organizations should implement robust data security practices to minimize the risk of unauthorized access or data breaches. Regular security audits and penetration testing are crucial to ensure the integrity of biometric data.
- **Compliance with Regulations:** Different regions have varying regulations regarding the collection and use of biometric data. Organizations must comply with all applicable data privacy laws to ensure responsible biometric practices.

Finding the Right Balance:

By adopting a responsible approach that prioritizes security, convenience, and privacy, organizations can leverage the power of biometrics to strengthen their KYE strategies. Investing in robust data security measures, fostering transparency with employees, and complying with relevant regulations can help build trust and ensure the responsible implementation of biometric authentication within the KYE framework.

Biometric technology is constantly evolving, with advancements in facial authentication and voice authentication offering even more secure and convenient authentication methods. As technology matures and user concerns are addressed, biometrics is likely to become an even more prominent tool for KYE and identity verification across various industries.

Zero-Data ID: A Privacy-Centric Identity Solution

Zero-Data ID: A Privacy-Centric Identity Solution for KYE

The growing use of biometrics in KYE strategies raises valid concerns about user privacy and data security. However, solutions like Zero-Data ID address these concerns by eliminating the need to store actual biometric data. This patented technology simplifies data handling, opens up possibilities for a limitless number of users due to 1:1 matching (unlike traditional 1:N comparisons), and avoids the need for a large central database.

This is where Zero-Data ID emerges as a game-changer. Zero-Data ID is a revolutionary biometric authentication technology patented by Veridas that provides a secure and privacy-centric approach to KYE. Unlike traditional methods that store biometric templates inside the access

terminals or hardware, Zero-Data ID utilizes a sophisticated mathematical process to create a unique identifier (a "cryptographic token") based on the user's biometric data which is only stored on the individual's device, and that can only be activated by combining the use of their face with a biometric qr stored on their cell phone.

Here's how Zero-Data ID protects user privacy:

- **No Biometric Data Storage:** This technology eliminates the need to store sensitive biometric templates on servers or in the storage system of the terminals themselves. Instead, the Zero-Data ID process generates a unique token that mathematically represents the biometric data without actually storing it. It is the user himself, who stores this information in his device, which can only be used in conjunction with his face. In this way, this information becomes private and non-transferable, since it needs a second authentication factor, which in this case, is the user's face.

- **Enhanced Security**: Zero-Data ID doesn't compromise security. The generated token remains unique to each user and cannot be replicated or forged, offering a robust layer of authentication. It can also be renovated as many times as desired.

- **User Control:** With our ZeroData ID, the user has control over their biometric information. The user's biometric vector is stored in the QR code that the user carries with them. In the authentication process, the terminal extracts the user's biometric vector and compares it with the one stored in the ZeroData ID.

Veridas and Zero-Data ID:

Veridas, a leading provider of KYE solutions, has patented Zero-Data ID technology. By integrating Zero-Data ID into its KYE platform, Veridas offers organizations a powerful solution that:

- **Strengthens Security:** Provides a robust layer of authentication without compromising user privacy.
- **Boosts User Confidence:** Empowers users by keeping their biometric data under their control.
- **Simplifies Compliance:** Reduces the need for organizations to manage and secure sensitive biometric data, easing compliance with data privacy regulations.

Veridas' Zero-Data ID powered KYE solutions offer a future-proof approach to identity verification, balancing the need for security with user privacy concerns. This innovative technology paves the way for a more secure and user-centric KYE experience.

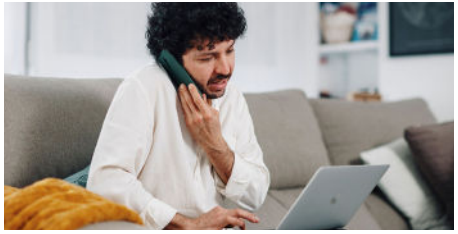
/Your Identity Partner for a Comprehensive KYE Solution

Veridas's KYE Product Suite

Veridas empowers organizations to implement a robust Know Your Employee (KYE) strategy with a comprehensive suite of products designed to secure physical and digital access across your entire organization.

Veridas Physical Access Control Terminals:

- **Zero Data Terminal:** It's a terminal with a second-factor authenticator that allows users to carry their data with them. Designed for any environment, its robust design ensures durability in harsh conditions and functionality in unsupervised spaces.



Veridas Digital Identity Solutions:

Beyond physical access, Veridas offers a range of digital identity solutions to strengthen your KYE strategy:

- **ID Verification (IDV):** Veridas' IDV solution allows you to verify the authenticity of government-issued IDs for tasks like onboarding new employees or processing payroll advances. This helps mitigate the risk of fraudulent activity and ensures you're working with legitimate individuals.

- **Voice Authentication for Password Resets:** Empower employees to reset forgotten passwords through secure voice authentication. This eliminates the need for complex security questions or password resets through potentially compromised email accounts.

- **Voice Authentication for Employee Services:** Facilitate a more natural and user-friendly experience for employees by enabling them to access services like requesting benefits information, or scheduling appointments through secure voice authentication.

- **Facial Authentication for Secure Access:** Veridas' facial authentication technology goes beyond physical access control. Employees can leverage their unique facial features for secure and convenient access to a variety of digital resources, including:

  - **Unlocking Work Computers:** Eliminate the need for remembering complex passwords and streamline the login process for employees.

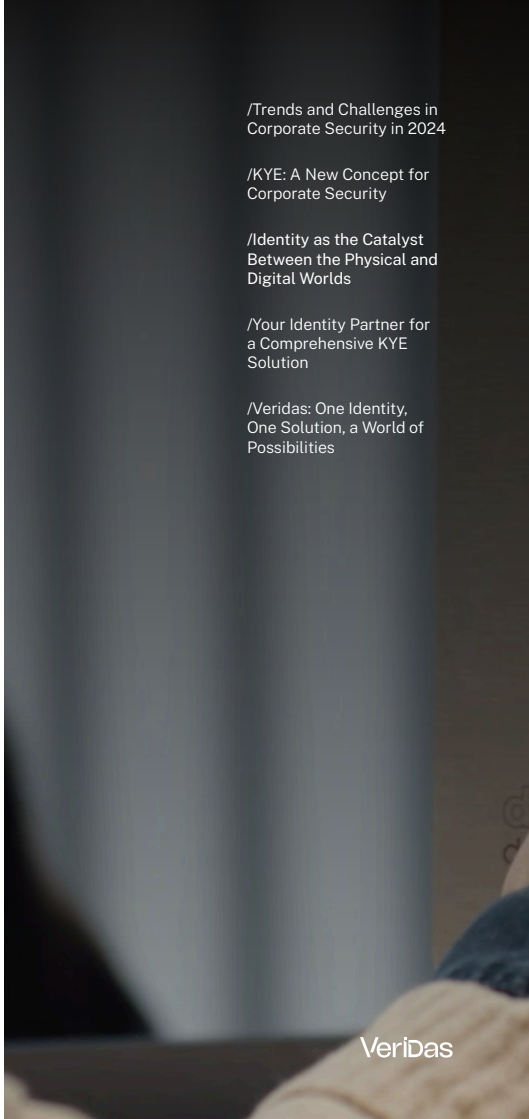
- **Accessing the Intranet:** Securely access company intranet portals containing sensitive information and internal resources using facial recognition.
- **Accessing Employee Benefit Applications:** Simplify access to employee benefit applications, allowing employees to manage their benefits plans and information with a quick facial scan.

These digital identity solutions complement Veridas' physical access control offerings, creating a comprehensive KYE ecosystem.

The Veridas Advantage:

Veridas' KYE product suite stands out thanks to:

- **Unmatched Security:** Leveraging cutting-edge biometrics like facial recognition and voice authentication, Veridas solutions provide a robust layer of security for physical and digital access.
- **Enhanced Convenience:** Biometric authentication eliminates the need for complex passwords or physical credentials, streamlining user experience and reducing login fatigue.
- **Scalability and Flexibility:** Veridas solutions can be tailored to meet the specific needs of your organization, regardless of size or industry.



/One Identity, One Solution, a World of Possibilities


1
2
3
4

Veridas Physicall KYE Security

Parking/Garage Entry

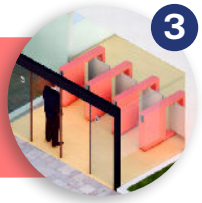
Fast, Seamless and Secure access into and out of a parking facility not because of the car plates but because of the authorised identity of the driver.

Facial access to delivery entrances

Easy and fast access into the building's multiple entrances for authorized suppliers, contractors, and business partners.

Employee access and management

Zero Data badge access linked to the user's identity and connected to a Time & Attendance based system that keeps track of your employees' work schedules, as well as breaks, clocking in and clocking out.



Streamline visitor access

Improved visitor experience by providing them with an automated check-in that they can do from home or at the corporate kiosks, and granting them access privileges during restricted time slots upon confirmation from the person with whom they have the appointment.


6
8
7
5

Veridas Digital KYE Technology

5

Remote access to corporate resources

Control who accesses what, when and how. It restricts access to certain privileged content according to the identity of the user. Perfect for home office or remote work.

6

Digital Facial Authentication

For IT, enter the personal work computer and log in to company resources such as Intranets, CRM, Restricted Documentation Systems, etc. without the need to use a password that can be stolen, only with one's own identity.

7

Voice Authentication for Password Reset

When an employee needs to reset their password, they will be prompted to repeat a specific phrase, which will have been previously recorded at enrollment. The system will compare the current voice sample with the recorded voice profile to verify the user's identity and a new password will be set.

8

Voice Authentication for Benefits

To request services related to employee benefits, as well as access to insurance resources, request for psychology or coaching appointments, etc...

/The Future of KYE and Corporate Security Redefined

The landscape of corporate security is constantly evolving. As cyber threats become more sophisticated, organizations must adopt a proactive approach to securing their physical and digital assets. KYE (Know Your Employee) emerges as a game-changer in this ever-changing environment. By focusing on robust identity verification, granular access control, and continuous monitoring, KYE empowers organizations to create a more secure and resilient security posture.

The Future of KYE: Innovation and User-Centricity

The future of KYE lies in continuous innovation and a commitment to user-centricity. Advancements in biometrics, artificial intelligence (AI), and blockchain technology will further enhance the security and convenience of KYE solutions. At the same time, ensuring user privacy and fostering trust will remain paramount.

Veridas: Your Trusted Partner for KYE Success

Veridas stands as your trusted partner in navigating the evolving landscape of KYE and corporate security. We offer a comprehensive suite of KYE solutions, including cutting-edge biometric authentication tools, digital identity verification services, and secure physical access control terminals. With a commitment to innovation, security, and user experience, Veridas empowers organizations.

Embrace Veridas KYE solutions and unlock a future of secure, efficient, and user-friendly work environments. Let's build a future of trust and security together.

> Contact Veridas today and discover how our KYE solutions can transform your organization's security posture.

Contact Info

Alfonso U. Santos
Global Sales & Marketing Director
ausantos@veridas.com

Kevin Vreeland
General Manager USA
kvreeland@veridas.com

Just be you

veridas.com