CYBERARK®
The Identity Security Company™

WHITEPAPER

Winning the APJ Regulatory Compliance Battle By Securing Your Identities

Table of Contents

Asia Pacific and Japan (APJ) Region: A Hotbed for Cybercrimes 3

Decoding Compliance Regulations of Key APJ Countries 4

ANZ

 Australia 5

 New Zealand 6

ASEAN

 Malaysia 7

 Singapore 8

 Philippines 9

 Vietnam 9

 Cambodia 10

 Thailand 10

 Indonesia 11

INDIA

 India 12

NORTH ASIA

 Hong Kong 13

 Taiwan 14

 Korea 14

JAPAN

 Japan 15

Tackle Your Compliance Challenges Effectively with CyberArk 16

Asia Pacific and Japan (APJ) Region: A Hotbed for Cybercrimes

The Asia Pacific and Japan region has become a hotbed for cybercrimes.

The increase in cybercrimes is driven by a number of factors: accelerated digital transformation within organizations; ongoing geopolitical conflicts; and increased mobilization of organized cybercriminal groups in Asia. In addition, many global countries are using manufacturing companies located in Asia, which is one of the most cyberattack-prone industries in the world.

Reports indicate a 15% rise in cyber incidents year-over-year, marking an average of nearly 1,963 attacksper week against Asia-Pacific organizations – a trend that's expected to persist in 2024[1]. As a result, 84% of APJ's tech executives have reportedly increased their cybersecurity budgets to secure their organizations through these turbulent times[2].

The underlying cause, however, continues to be the lack of focus on securing all kinds of identities that continue to proliferate as organizations double-down on cloud initiatives. In this complex digital environment where any identity can become privileged, a staggering 62% of APJ organizations continue to believe that only human identities can be privileged, thus exposing themselves to a plethora of risks[3]. It's no wonder why 95% of APJ organizations suffered two or more identity-related breaches in the past year[4].

APJ Cybersecurity Landscape Overview

Security spends growing at a CAGR of

12.8% since 2022

Cybersecurity market valuation to touch

US $52B by 2027

Cost of data breach in 2023 for 35% of organizations is between

US $1M to US $20M

Source: PWC, "2024 Global Digital Trust Insights", May 2024.

As organizations continue to battle increasing attacks on highly privileged identities, regulatory bodies in various APJ countries have put forth stringent compliance policies and regulatory frameworks that enterprises must follow to protect sensitive data and mitigate potential cyber threats.

74%

of security professionals rank identity and access management solutions as one of the most-used tools in achieving compliance[4].

This whitepaper provides a summary of cyber compliance policies and prerequisites across key APJ countries and how CyberArk can help you align with them using the CyberArk Identity Security Platform.

[1] Insurance Business, "APAC Cybersecurity alert: report reveals surge in cyberattacks", 2024.
[2] PWC, "2024 Global Digital Trust Insights", May 2024.
[3] CyberArk, "2024 Identity Security Threat Landscape Report", May 2024.
[4] ISACA, "Privacy in Practice 2024", 2024.

Decoding Compliance Regulations of Key APJ Countries

The global ISACA Privacy in Practice 2024 survey report reveals that only a third of the organizations understand their privacy obligations, while 57% lack confidence in their privacy team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations[5].

The bottom line? For any organization to satisfy compliance and boost their cyber resilience, it's important to fully understand the mandates and work with their security vendors to meet them. Let's start by exploring the compliance regulations and data protection laws of some of the major countries in the APJ region.

Breakdown of the APJ Region

[5] ISACA, "Privacy in Practice 2024", 2024.

ANZ: Australia and New Zealand

Australia

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has developed a strategic directive comprising eight important strategies aimed at offering best practices to organizations in the battle against cyber threats.

Here we explore five of the Essential Eight risk mitigation strategies recommended by the ACSC that are central to securing user data and highly privileged entities.

1. **Application whitelisting** of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
2. **Configure Microsoft Office macro settings** to block macros from the Internet and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
3. **User application hardening** to block web browser access to Adobe Flash (uninstall if possible), web advertisement and untrusted java code on the internet.
4. **Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.
5. **Multi-factor authentication (MFA)** including for VPNs, RDP, SSH and other remote access and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

The Australia Compliance Checklist

Complying with ACSC requirements with an identity-focused security strategy: With an integrated identity security strategy, organizations can automatically detect, onboard and secure privileged accounts to protect their most critical resources. Simultaneously, a multi-factor authentication (MFA) strategy powered by user behavior analytics can provide security teams with real-time monitoring to prevent unauthorized access. Finally, implement a least privileged architecture that gives users access to resources based on their roles and prevents them from installing forbidden applications which, in turn, strengthens endpoint security.

New Zealand

The Privacy Act 2020 is the key legislation in New Zealand that is designed to protect personal information collected by businesses and organizations. The act determines how companies handle personal data, emphasizing accountability and transparency in this fast-evolving digital landscape. Some of the key components of the act are discussed below:

1. **Privacy principles:** The act entails twelve privacy principles to safeguard the collection, use, storage and disclosure.
2. **Access directions:** Gives the Privacy Commissioner the power to direct organizations to furnish or correct an individual's data, ensuring meaningful access.
3. **Compliance notices:** This empowers the Privacy Commissioner to issue notices to enforce compliance and rectify violations of the Act.

The New Zealand Compliance Checklist

Complying with the Privacy Act with an identity-focused strategy: Data protection and access management lie at the heart of New Zealand's cybersecurity legislation – and an identity security strategy that extends intelligent privilege controls to all identities can be the key to it. For instance, foundational privileged access management (PAM) capabilities, such as credential vaulting and rotation and session isolation can help protect the most critical assets, whereas combining single sign-on (SSO), MFA and session monitoring can help secure access and satisfy compliance.

ASEAN: Malaysia, Singapore, Philippines, Vietnam, Cambodia,Thailand, Indonesia

Malaysia

Organizations in Malaysia are required to abide by two main regulations to remain cyber resilient in the face of emerging attack methods and effectively protect personal data involved in commercial transactions. Here's a quick overview of these key Malaysian regulations:

1. **Risk Management in Technology (RMIT):** Bank Negara Malaysia established this framework to address the growing threats posed to information and financial systems. It aims to ensure that Malaysian financial institutions effectively manage their cyber-risk exposure by establishing necessary risk frameworks, governance structures, policies and procedures.
2. **Personal Data Protection Act (PDPA):** PDPA came into effect in 2013 to regulate the processing of personal data in commercial transactions and aims to protect individuals' personal data while ensuring responsible usage of the same by businesses. Most businesses in Malaysia that collect, process or transfer personal data as part of their day-to-day operations fall under PDPA.

The Malaysia Compliance Checklist

Complying with RMIT and PDPA with an identity-focused security strategy: For an organization to be RMIT compliant, they should be able to define users' access rights based on their roles, the actions they take within high-risk systems post authentication and how to track them to meet compliance needs. Similarly, section 9 of PDPA states that a user shall take practical steps to protect personal data from unauthorized exfiltration, loss or alteration by implementing securing measures in devices they're stored in.

This can be achieved by focusing on identities and all the actions they take throughout their lifecycle within the enterprise network. Some of the fundamental strategies that can help you align with RMIT and PDPA are:

1. **Securing workforce access:** By combining standard identity and access management (IAM) solutions like SSO, MFA, password manager and session monitoring – security teams can ensure only authorized users gain access to confidential enterprise resources while having end-to-end visibility into user activities needed to mitigate potential threats and satisfy compliance.
2. **Implementing zero standing privileges (ZSP):** While manual access provisioning can increase admin work and disrupt the user experience, a ZSP-enabled environment can dynamically elevate entitlements for a particular user to enable access for a given time frame and then revoke it to secure the environment once the job is done. All this happens in real-time without manual intervention and while maintaining a detailed log of user activities, thereby boosting operational efficiency and security.

Singapore

The Personal Data Protection Act (PDPA) governs Singapore's data privacy regulations. First enacted on October 15, 2012, it was soon updated to keep with the pace of the GDPR per the Personal Data Protection (Amendment) Act 2020 (together, the "Act"). According to the Personal Data Protection Committee of Singapore (PDPC), companies covered under the Act must focus on:

1. **Ethical collection of personal data:** This requires organizations to notify individuals about the purpose of collecting data or disclosing their data on or before such collection.
2. **Care of personal data:** Companies must implement security arrangements to safeguard personal data from unauthorized access, loss and other cyber risks.
3. **Individual's right over personal data:** Individuals should be granted access to their data on request and provided information about the use of their data or disclosure.

Besides PDPA, financial institutions (FI) in Singapore are also bound by Technology Risk Management (TRM) Guidelines put forth by the Monetary Authority of Singapore (MAS). The TRM guideline is a collection of best practices intended to help FIs strengthen cybersecurity and mitigate potential risks.

Here are some of the key regulations with respect to managing user access and securing privileged accounts:

1. Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers.
2. FIs should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes.
3. FIs should establish a password policy and a process to enforce strong password controls for users' access to IT systems. Multi-factor authentication should also be implemented to safeguard critical resources from unauthorized access and risks stemming from credential compromise.
4. Access to privileged accounts should only be granted on a need-to-use basis while logging activities of these accounts for review and monitoring purposes.

The Singapore Compliance Checklist

Complying with PDPA regulations with an identity-focused security strategy: Singapore's compliance requirements are very similar to that of Thailand's as both nations follow PDPA guidelines to protect consumer data. To ensure organizations in Singapore are securely collecting, processing and storing personal data, it is imperative organizations implement a strong phishing-resistant authentication alongside the least privilege framework to minimize chances of unauthorized access.

Complying with TRM guidelines with an identity-focused security strategy: The TRM regulations underscore the importance of enabling role-based access with continuous monitoring and MFA to secure access to highly sensitive resources. All of these capabilities can be best realized by layering existing IAM solutions with a security-first mindset. This approach can be equally effective in enabling access toprivileged accounts on a need-to-use basis, which is one of the important regulations with respect to securing privileged access. To know more about TRM guidelines and how CyberArk can help, read the whitepaper on Addressing the Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines.

Philippines

The Philippines passed the Data Privacy Act 2012 to protect the fundamental human right of privacy and communication while ensuring the free flow of information to promote innovation and growth. The Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that is located in the Philippines, or those who maintain an office, branch, or agency in the Philippines.

The Philippines Compliance Checklist

Complying with the Data Privacy Act of 2012 with an identity-focused security strategy: Securely storing and processing sensitive personal information is the key to complying with this regulation for businesses based in the Philippines. A holistic identity security strategy that allows them to securely store critical customer data in threat-resistant cloud vaults and also monitor who's accessing them and when to prevent unauthorized access can help meet the compliance criteria. Security compliance in the Philippines can be attained through a strategic blend of foundational PAM and IAM capabilities.

Vietnam

Vietnamese organizations must comply with two common regulations: the circular by the State Bank of Vietnam (SBV) for Financial Services Institute (FSI) organizations and the Vietnam Cybersecurity Law by the Government.

The latest SBV regulation for IT security is Circular 09/2020, in which Article 28 (Access Management) requires organizations to manage users or groups of users' access to critical systems and adhere to specific password policies. The regulation also requires organizations to adopt measures to monitor the use of administrator's accounts and limit the use of administrator's accounts to a fixed duration of time that's long enough to carry out a given task.

Regarding the Vietnam Cybersecurity Law, the detailed document, Decree 53/2022/ND-CP, contains regulations about controlling admin access to critical systems that are similar to SBV's Circular 09.

The Vietnam Compliance Checklist

Complying with the SBV and Vietnam Cybersecurity Law with an identity-focused security strategy: As both the regulations revolve around managing access to business-critical resources, organizations can leverage their existing IAM solutions to streamline their compliance processes while strengthening overall security posture. For example, by layering step-up authentication with the regular SSO, businesses can ensure that only legitimate users are granted access to the network. Additionally, implementing the least privilege framework across all identities, along with just-in-time access for a seamless user experience, can further reduce risks of data theft stemming from unauthorized access.

Cambodia

The National Bank of Cambodia (NBC) has established guidelines to help banking and financial institutions (BFI) create a secure technology ecosystem as they increasingly use technology to support various business processes. The process of authorization ensures that the requested activity or access to an object is possible, given the necessary conditions for the identity to be authenticated are met. Some of the control and security practices enumerated below need to be considered:

1. Implementing multi-factor authentication for privileged users.
2. Instituting strong controls over remote access by privileged users.
3. Restricting the number of privileged users.
4. Granting privileged access on a 'need-to-have' or 'need-to-do' basis.
5. Maintaining audit logging of system activities performed by privileged users.
6. Ensuring that privileged users do not have access to systems logs in which their activities are being captured.
7. Conduct regular audits or management reviews of the logs.
8. Prohibiting sharing of privileged IDs and their access codes.
9. Disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring.
10. Protecting backup data from unauthorized access.

The Cambodia Compliance Checklist

Complying with NBC guidelines with an identity-focused security strategy: The above-mentioned security practices range from securing authentication to managing privileged access and maintaining an audit trail of user activities so that security teams have complete visibility of their environments. By extending foundational IAM tools with session monitoring and recording solutions to all workforce identities, banking and financial institutions in Cambodia can breeze through their compliance assessments.

Thailand

The Personal Data Protection Law (PDPA), implemented in June 2022, is the main consumer data protection law in Thailand. The law entails the rights individuals have over their personal data, provides guidelines that organizations must adhere to legally collect and use consumer information and describes the penalties for possible violations.

Key principles under the PDPA are highly influenced by the European Global Data Protection Regulation (EU GDPR), but there are still some unique Thai perspectives on the law regarding how data processors and controllers perform their duties:

1. **Section 37:** The data controllers shall apply appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of personal data, and such measures must be reviewed when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate security and safety.
2. **Section 40:** The data processor shall apply appropriate security measures for preventing unauthorized or unlawful loss, access to, use, alteration, correction or disclosure, of personal data and notify the data Controller of the personal data breach that occurred.

The Thailand Compliance Checklist

Complying with PDPA Law with an identity-focused security strategy: With a strong commitment to ethically collect, process and protect individual data, businesses in Thailand can greatly strengthen their compliance with an integrated identity security strategy. Here's how:

1. **Strong, threat-resistant authentication:** This will ensure that only authorized users have access to sensitive consumer data, thereby reducing the risks of data theft.
2. **Better visibility for ease of compliance:** By using session recording and protection with strong multi-factor authentication, businesses can maintain a detailed audit trail of user activities taken inside environments containing high-risk consumer data.
3. **Zero standing privileges:** By ensuring no workforce identities have standing access to critical consumer data, organizations can greatly reduce risks stemming from over-entitled identities and meet compliance regulations.

Indonesia

Headquartered in Jakarta, the Financial Services Authority (OJK) is an Indonesian government agency that has been regulating and supervising the financial services of the country since its establishment in 2011. Its foundational regulation, the Financial Services Authority Act, requires entities to manage their user passwords and session privileges in all systems and have tools to detect unauthorized access.

The Indonesia Compliance Checklist

Complying with the FSA Act with an identity-focused security strategy: While protecting user credentials of highly-privileged entities have been an integral capability of all PAM programs, businesses can extend it to all identities with the potential of becoming privileged to strengthen security and streamline compliance processes. The use of multi-factor authentication powered by user behavior analytics can enable them to detect malicious login attempts and subsequently float a complex verifier to check if they are indeed who they claim to be.

India

India

The Reserve Bank of India has released a comprehensive Master Direction (Information Technology Governance, Risk, Controls and Assurance Practices) on IT governance, risk, controls and assurance practices for regulated entities (REs) such as banks and NBFCs. The directive covers five key areas of IT governance: strategic alignment, risk management, resource management, performance management and business continuity/disaster recovery management. REs are expected to put in place a robust IT service management framework to ensure the operational resilience of their IT environment.

The Master Direction calls for:

1. Access to information assets be allowed only where a valid business need exists and kept up to date for administering need-based access to an information system.
2. Personnel with elevated system access entitlements to be closely supervised with all their systems activities logged and periodically reviewed.
3. REs to adopt multi-factor authentication for privileged users of critical information systems and critical activities, basis the RE's risk assessment.

Advisory for SEBI Regulated Entities (REs) Regarding Cybersecurity Best Practices

The Securities and Exchange Board of India (SEBI) is a statutory regulatory body established in 1992 to protect the interest of investors investing in securities, along with regulating the securities market. SEBI regulations are centered on data breach protection, vulnerability assessment and penetration testing (VAPT), log retention and audits. The following are some of SEBI's key regulations to secure user authentication:

1. Strong password management policy implemented with periodic review of accounts of ex-employees, no reuse of passwords across multiple accounts and no storing them locally on the system.
2. Multi-factor authentication enabled for all users that connect using online/internet facility and also, particularly for virtual private networks, webmail and accounts that access critical systems.
3. Maker-checker framework strictly implemented and MFA enabled for all user accounts, especially for user accounts accessing critical applications.

The India Compliance Checklist

Complying with RBI and SEBI's regulations with an identity-centric approach: India's compliance policies are centered on securing user access, monitoring privileged identities and protecting user credentials. This can be achieved by securing all identities with the right levels of privilege control using an integrated identity security strategy.

1. **Secure credentials** by vaulting and rotating them automatically to reduce chance of credential theft. Although used traditionally in securing highly-privileged identities, extending it to all workforce identities can greatly strengthen an organization's security posture.
2. **Enable multi-factor authentication** powered by user behavior analytics to dynamically monitor user logins based on AI-generated risk profiles based on the user's login history and prevent malicious threat actors from breaking into the network.

North Asia: Hong Kong, Taiwan and Korea

Hong Kong

In 2016, the Hong Kong Monetary Authority (HKMA) introduced the Cybersecurity Fortification Initiative (CFI) to improve the cyber resilience of the country's banking system. The initiative was underpinned by three pillars: the Cyber Resilience Assessment Framework (C-RAF), the Professional Development Programme (PDP) and the Cyber Intelligence Sharing Platform (CISP).

A few years later, to keep up with the evolving security landscape, the HKMA conducted a holistic review of the CFI and found that over 90% of banks found C-RAF useful in identifying gaps that went unrecognized in the past. This paved the way for the launch of CFI 2.0 in late 2020, following industry consultation.

Of the three pillars that define the Cybersecurity Fortification Initiative, C-RAF is the most critical in assessing risks. It enables authorized institutions (AIs) to evaluate their own risk profiles and benchmark the level of resilience required to accord appropriate protection against cyberattacks.

The Hong Kong Compliance Checklist

Complying with C-RAF with an identity-focused security strategy: Evaluating your own risk profile requires continuous, real-time monitoring of all identities – human and machine – across the complete enterprise estate. Here's how to do it with an integrated identity security strategy:

1. **Mitigate risks** by securing highly privileged identities using phishing-resistant multi-factor authentication (MFA) powered by a robust user behavior analytics (UBA) engine that leverages AI to discern typical logins from malicious ones.
2. **Secure credentials** by centrally vaulting and rotating them to prevent credential abuse and reduce the risk of unauthorized access. An otherwise critical capability of your PAM program that you can layer with existing security solutions to maximize risk reduction.
3. **Enforce the principle of least privilege (PoLP)** across all identities using just-in-time (JIT) access to ensure users have access to the resources only when they need them and for a fixed duration of time, thus reducing risks stemming from prolonged exposure.
4. **Streamline audit and compliance** by extending session recording and monitoring controls to all high-risk sessions. This provides AIs with a detailed audit trail of user activities within sensitive apps, enabling them to easily meet C-RAF compliance mandates.

Taiwan

Taiwan's cybersecurity and data protection regulations are governed by two main legislations:

1. **Personal Data Protection Act (PDPA):** This is the main statute for personal data protection in Taiwan. It was first introduced in 1995 and significantly amended in 2010, with the amendments becoming effective in 2012. The PDPA outlines the principles for data processing, individual rights and the responsibilities of data controllers and processors. It also includes provisions for the appointment of data protection officers and the handling of data breaches.
2. **Cyber Security Management Act (CSMA):** Announced in June 2018, the CSMA is the core legislation for cybersecurity in Taiwan. It applies to government agencies and specific non-government entities, including critical infrastructure providers and state-owned businesses. The act mandates the establishment of cybersecurity maintenance plans, incident reporting within one hour of discovery and completion of damage control measures within 36 to 72 hours, depending on the severity.

The Taiwan Compliance Checklist

Complying with Taiwan's regulations with an identity-focused security strategy: Protecting personal data starts with controlling access to it and also knowing what happens to the data when it's being accessed. It's a combination of enabling secure access and monitoring user activities which, in turn, enables security teams to promptly identify security incidents and take steps to remediate them. An identity-focused security approach can help businesses do exactly that by layering foundational IAM solutions to secure all identities and strengthen security posture. Therefore, companies in Taiwan can greatly benefit from an identity-focused security strategy in demonstrating PDPA and CSMA compliance.

Korea

Korea's data protection framework is governed primarily by the Personal Information Protection Act (PIPA). It was first implemented in 2011 but has undergone significant amendments, most recently in 2023. PIPA applies to public and private sector organizations that collect, process and use personal data.

The act also requires organizations to implement appropriate security measures to prevent unauthorized access, alteration or destruction of confidential user data. Some of the other sector-specific laws and guidelines applicable in Korea are:

1. **Electronic Financial Transactions Act (EFTA):** According to Article 21 of the EFTA, electronic financial business operators must establish and operate an information protection system to ensure the safety and reliability of electronic financial transactions. This involves technical and managerial measures such as access control to electronic financial transaction systems, encryption of transaction information, installation and operation of intrusion detection systems, and regular security inspections.

2. **Guidelines for the Use of Cloud Services in Financial Institutions:** When financial institutions use cloud services, they must ensure that the security measures provided by the cloud service provider meet the security requirements of the financial institution. The guidelines stipulate the evaluation of the cloud service provider's security certification, data protection measures, service continuity plans, and incident response capabilities.
3. **Cloud Security Assurance Program (CSAP):** When public institutions use cloud services, those services must be CSAP certified. The CSAP certification assesses whether the cloud service provider meets the government's security standards. Evaluation criteria include physical security, network security, access control, data protection, and incident response.

The Korea Compliance Checklist

Complying with Korea's cybersecurity regulations with an identity-focused approach: Access control and session monitoring are the common links across all Korean regulations. An integrated identity security strategy that brings together existing IAM solutions can help businesses attain compliance and strengthen their security posture. It all begins with the adoption of the Zero Trust framework, where basic authentication tools, such as SSO and adaptive MFA can be layered using a security-first mindset to enable secure access to all identities as they work their way through the heart of the enterprise. While session monitoring was largely applied to privileged accounts in the past, extending it to all identities in today's threat landscape can significantly improve an organization's threat resilience and compliance posture.

Japan

Japan

The main data protection law in Japan is the Act on the Protection of Personal Information (APPI), Act No. 57 of 2003. Some of the key requirements include obtaining consent to collect personal data, using legal bases to process them and implementing security measures to protect personal data.

With regard to access control, organizations are required to adopt necessary steps to prevent unauthorized access to personal data, including physical security measures. The law also decrees that organizations adopt access controls and provide their staff with adequate training to ensure they handle personal data properly.

The Japan Compliance Checklist

Complying with APPI Law with an identity-focused security strategy: Access control and protection is at the heart of Japan's data protection regulations. A robust identity security strategy based on the PoLP that secures all identities right from the point of login to their entire lifecycle across the enterprise estate is central to protecting personal data. By combining some key IAM solutions, such as SSO, MFA, session monitoring and password managers – organizations in Japan can readily meet compliance regulations.

Tackle Your Compliance Challenges Effectively with CyberArk

It's clear that compliance is no longer just about how consumer data is stored but rather how it's collected, processed and used. Authorities have developed the regulations that makes compliance and security inseparable, driving organizations to adopt an integrated security strategy.

At CyberArk, we believe every identity should be secured with the right levels of privilege control for enhanced security and ease of compliance. For more than two decades, we have been helping organizations secure all kinds of identities – human and machine – with our integrated CyberArk Identity Security Platform.

If you have concerns about your organization's data compliance posture, read the CyberArk Blueprint or contact us for prescriptive guidance and advisory consultation.

READ THE BLUEPRINT

About CyberArk

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®
The Identity Security Company™