ZorroSign®

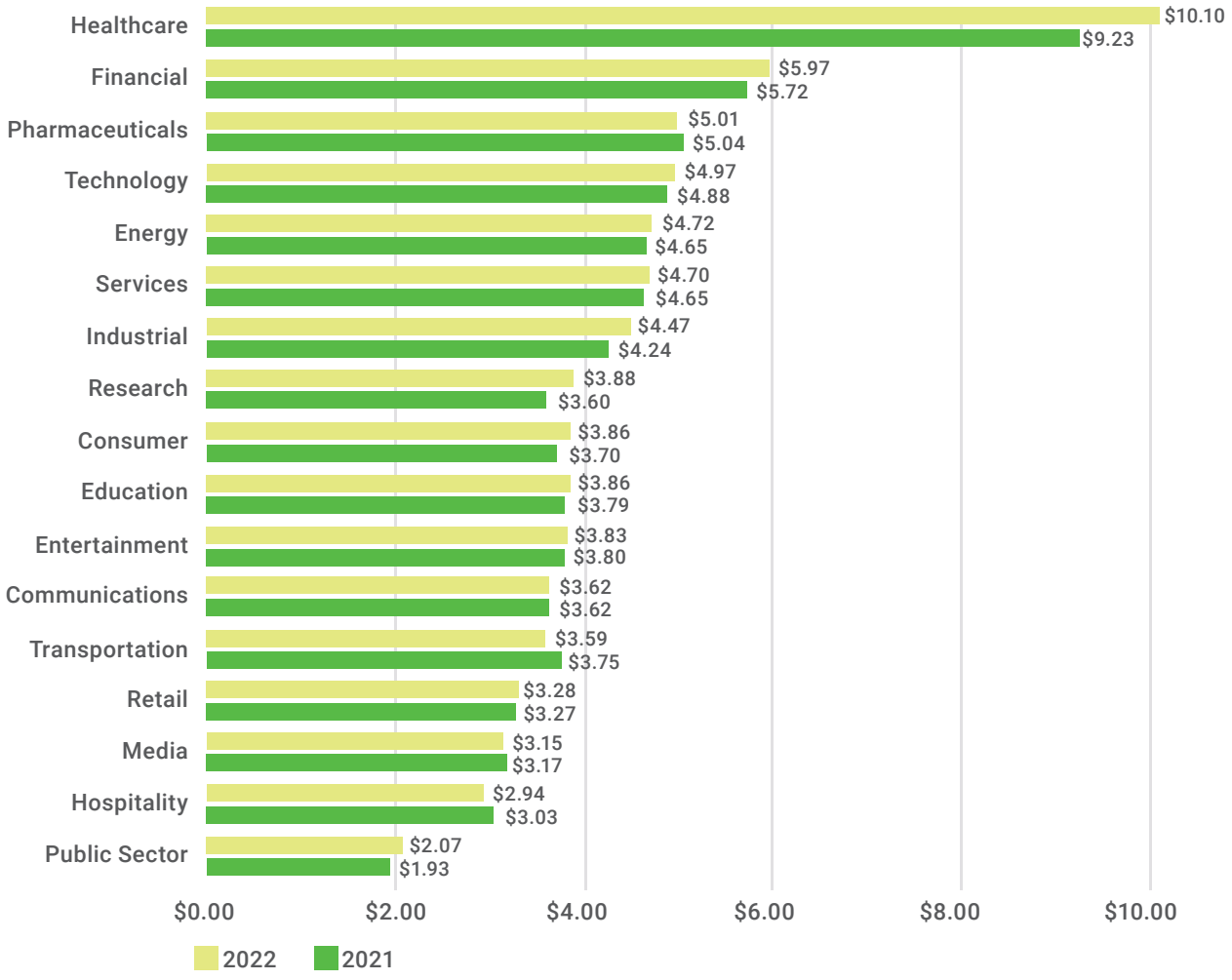
The Growing Risks to Digital Data in 2023

Elevate Data Security with ZorroSign to Protect Your Company's and Your Customer's Information

The ever-growing amount of digital data and the increasing complexity of cyber threats have made data security more important than ever before. In 2023, companies must take steps to elevate your data security to protect both your own information and that of your customers.

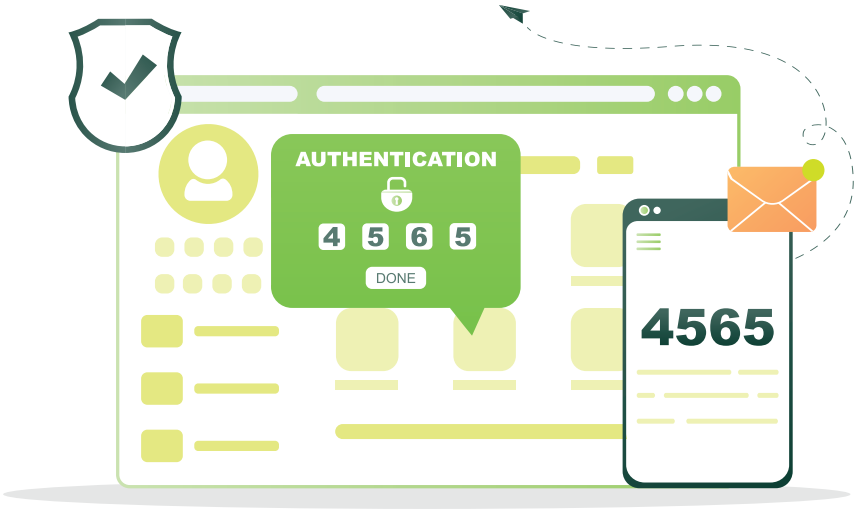
One of the main risks to digital data today is the **increasing sophistication of cyber attacks**. Hackers are using more advanced techniques to bypass traditional security measures—such as using machine learning to evade detection and launching targeted phishing and spear-phishing attacks against specific organizations. Companies must be prepared to defend against these types of attacks by implementing advanced security measures, such as artificial intelligence-based security solutions, and regularly updating and patching your systems.

Average Cost of Data Breach by Industry



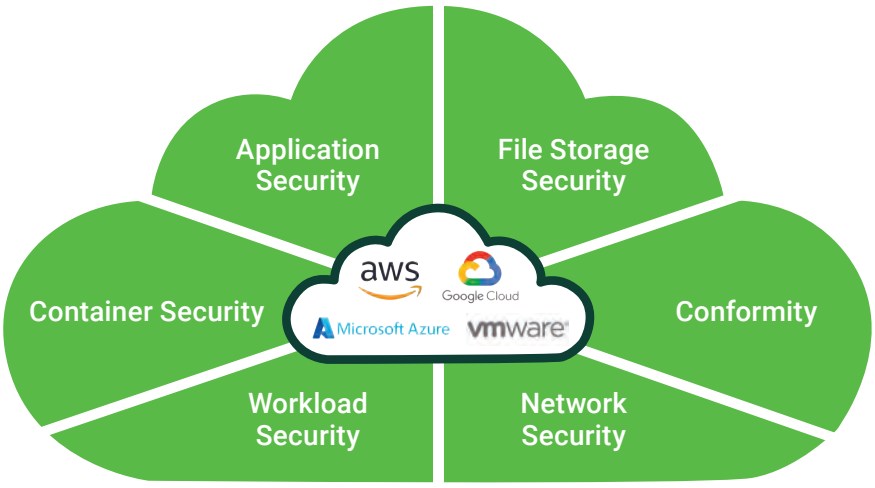
Source: https://www.ibm.com/resources/cost-data-breach-report-2022

Another risk to digital data in 2023 is the growing number of connected devices and the Internet of Things (IoT). **As more devices are connected to the internet, the attack surface for hackers becomes larger, making it easier for them to gain access to sensitive information.** Companies must take steps to secure your IoT devices and to ensure that those devices are not used as a means to gain access to other systems.



Source: https://hitachi-systems-security.com/infographic-how-to-secure-the-iot-environment/

Further, the use of cloud services and the increasing amount of data that is stored in the cloud has also increased the risk of data breaches. Companies must ensure that your cloud services are properly configured and that you are using a **reputable provider** with a strong track record of security. Companies also need to implement strong access controls and encryption to protect data stored in the cloud.



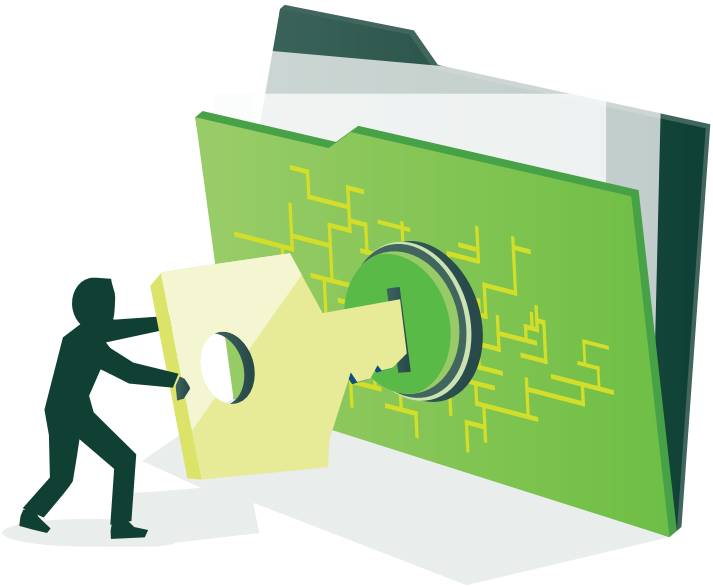
Source: https://manrai-tarun.medium.com/cloud-security-risks-and-threats-in-2020-75bbbb8edae9

Protecting data against the growing risks in 2023 requires a **multi-layered approach** that includes regular updates and patching, securing IoT devices, properly configuring cloud services, adopting advanced security measures such as:

- **Blockchain technologies** for tamper-proof record keeping with no single point of failure
- **Digital signature technologies** to authenticate and authorize remote transactions
- **Identity-as-a-Service** solutions for scalable identity and access management (IAM)
- **Passwordless authentication** to reduce the human risk in security systems

Organizations that fail to take these steps will be at a higher risk of data breaches and will be more vulnerable to cyberattacks.

It is important to remember that data security is not only important to protect your company's information but also to protect the personal data of your customers and employees.



Source: https://paubox.com/resources/what-is-a-threat-vector-and-why-is-it-important-to-define/

Why Add Blockchain Technologies to Your Security Stack?

It has long been claimed that blockchain technology has the potential to revolutionize the way companies approach security. By leveraging the decentralized and immutable nature of blockchain, companies can enhance your security stack and protect against a wide range of threats.

One of the main benefits of blockchain technology is its ability to provide secure and tamper-proof record keeping. The decentralized nature of blockchains ensures that there is no single point of failure—which also means that hackers cannot easily compromise the system. Additionally, the use of cryptography and consensus mechanisms ensures that once data is recorded on the blockchain, it is extremely difficult to alter or delete.

Another security benefit of blockchain technology is its ability to provide secure and transparent transactions. By using smart contracts, companies can automate and streamline processes, while also ensuring that all transactions are recorded in a transparent and immutable manner. This can help to reduce the risk of fraud and increase trust between parties.

Blockchain technology can also be used to improve supply chain management. By using blockchain, your organization can track products and goods as they move through supply chains—providing real-time visibility into the status and location of products. This can help to improve efficiency, reduce costs, reduce fraud, and increase transparency.

Moreover, blockchain technologies such as **Hyperledger Fabric** (private, permissioned) and **Provenance Blockchain** (public, permissionless) can be used to enhance cyber security by providing encrypted and immutable identity management. Blockchain-based identity and access management (IAM) systems provide secure and decentralized storage of identity data, making it more difficult for hackers to steal or compromise sensitive information.

By incorporating blockchain technology into your security stack, companies can enhance your security posture and protect against a wide range of threats. Blockchains provide:

- Secure and tamper-proof record keeping,
- Secure and transparent transactions,
- Improved supply chain management, and
- Enhanced identity management.

Together, **these make blockchain technology an attractive option for companies looking to improve your security**. Organizations that are able to leverage blockchain technology to improve your security will be strongly-positioned to succeed in the years ahead!

Why Add Digital Signature Technologies to Your Security Stack?

Digital signature solutions provide a secure and efficient way for companies to authenticate and authorize electronic transactions, and can play an important role in your security stack.

One of the main benefits of digital signature solutions is that they provide a secure and tamper-proof way to authenticate electronic transactions. By using digital signatures, you can ensure that the parties involved in a transaction are who they say they are, and that the transaction has not been tampered with—from contract creation, to conveyance, signing, and storage. This can help to reduce the risk of fraud and increase trust between parties.

Another key benefit of digital signature solutions is that they can help to streamline and automate business processes. By using digital signatures, companies can **eliminate the need** for paper-based signatures and reduce the time and costs associated with manual processes. This can help you to improve efficiency and reduce costs.

Digital signature solutions also provide a secure way for companies to comply with regulatory requirements: Many industries have regulations that require companies to provide secure and tamper-proof records of transactions. Digital signature solutions can help companies meet these requirements by providing a secure, auditable, and immutable record of transactions.

Moreover, digital signature solutions can also be used to authenticate and authorize remote transactions—increasingly common in today's digital world. With digital signature solutions, companies can ensure secure transactions across employees, partners, and customers working remotely . . . on any online device, anywhere in the world. This can greatly improve security and reduce the risk of fraud.

By incorporating digital signature solutions into your security stack, companies can improve your security posture and reduce costs. Digital signature solutions:

- Provide a secure and tamper-proof way to authenticate and authorize electronic transactions,
- Streamline and automate business processes,
- Help organizations comply with regulatory requirements, and
- Enable secure remote transactions.

Companies that adopt digital signature solutions elevate the security of your digital assets while improving efficiency and reducing costs.

Why Add Identity-as-a-Service Solutions to Your Security Stack?

Identity and access management (IAM) is a critical aspect of any company's security stack, and identity- as-a-service (IDaaS) solutions can provide a cost-effective and efficient way to manage this aspect of your security.

One of the main benefits of IDaaS solutions is that **they allow companies to outsource the management of user identities and access to third-party providers**. Such outsourcing can free up internal resources and allow companies to focus on your core competencies. Additionally, IDaaS providers are typically able to offer a higher level of security expertise than companies might successfully achieve in-house.

Another key benefit of IDaaS solutions is that **they provide a centralized platform for managing user identities and access across an organization**. This centralization can help to improve security and compliance by ensuring that all users are properly authenticated and authorized to access the resources they need. IDaaS solutions can also provide real-time monitoring and reporting, allowing companies to quickly detect and respond to security incidents.

IDaaS solutions also allow for greater flexibility and scalability. As organizations grow and change, your security needs will evolve as well. IDaaS solutions can easily adapt to such changes, and can be scaled up (or down) to meet the specific needs of your company—reducing costs, improving efficiency, and elevating security.

Further, IDaaS solutions also provide enhanced security features such as multi-factor authentication (MFA) and/or passwordless authentication, helping to protect against identity theft and other cyber threats. This can be especially important if your company handles sensitive data or operates in regulated industries.

By incorporating IDaaS solutions into your security stack, companies can improve your security posture and reduce costs. IDaaS solutions provide:

- A cost-effective and efficient way to manage user identities and access,
- A centralized platform for managing security across organizations, and
- Enhanced security features such as MFA and passwordless authentication which protect against identity theft and other cyber threats.

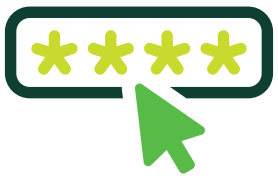
Organizations that adopt IDaaS solutions gain a strategic advantage in securing your digital assets and complying with regulatory requirements.

Why Add Passwordless Authentication Capabilities to Your Security Stack?

Passwordless login capabilities provide a secure and convenient way for companies to authenticate users and can play an important role in your security stack by minimizing the human risk-factor.

Hacked or stolen passwords are one of the weakest links in cybersecurity today. Many attacks begin with a hacked or stolen password, and artificial intelligence (AI) can hack even longer passwords more quickly than you might guess. A recent Home Security Heroes report showed their AI password cracker could hack most passwords in under a minute—and 65 percent in under an hour.

One of the main benefits of passwordless authentication is that it eliminates the need for users to remember and manage multiple passwords. With users not needing to write down their passwords, and unable to share their passwords, the risk of password-related security breaches, such as phishing, brute force attacks, and password reuse is significantly reduced.



Another key benefit of passwordless login is that it provides a more **seamless and user-friendly experience**. With passwordless login, users can authenticate themselves with a variety of methods such as biometric authentication, one-time passcodes sent via SMS, or a security key. This facilitates user adoption and reduces the risk of users circumventing security measures.

Passwordless login also provides a way to secure remote transactions, as users can authenticate themselves without the need to be physically present at a location. This is particularly useful in today's digital world where remote work and online transactions are becoming more and more prevalent.

Moreover, passwordless login capabilities can also be integrated with multi-factor authentication (MFA) to **provide an additional layer of security**. MFA can help to protect against identity theft and other cyber threats by requiring users to provide multiple forms of authentication—critically important for companies that handle sensitive data or operate in regulated industries.

By incorporating passwordless login capabilities into your security stack, companies can improve your security posture and reduce costs. Passwordless authentication:

- Eliminates the need for users to remember and manage multiple passwords,
- Provides a more seamless and user-friendly experience,
- Secures remote transactions, and
- Can be integrated with multi-factor authentication.

Organizations that adopt passwordless login capabilities better secure your digital assets, improve user adoption, and reduce the risk of security breaches.

Why Add ZorroSign to Your Security Stack?

ZorroSign, Inc. is a leading provider of digital signature and document management solutions that helps companies to elevate your data security. By incorporating ZorroSign's data security platform built on blockchain into your IT security stack, you gain the strengths of blockchain technologies, digital signatures, IDaaS, and passwordless authentication to elevate your security posture and reduce costs.

One of the main benefits of ZorroSign's data security platform is that its blockchain architecture provides a **secure and tamper-proof** way to authenticate electronic transactions. By using private (Hyperledger Fabric) or public (Provenance Blockchain) blockchains for digital signatures, companies can ensure that the parties involved in a digital transaction are who they say they are—no matter where in the world they might be signing—and that the transaction has not been tampered with. This security reduces the risk of fraud and increases trust between parties.

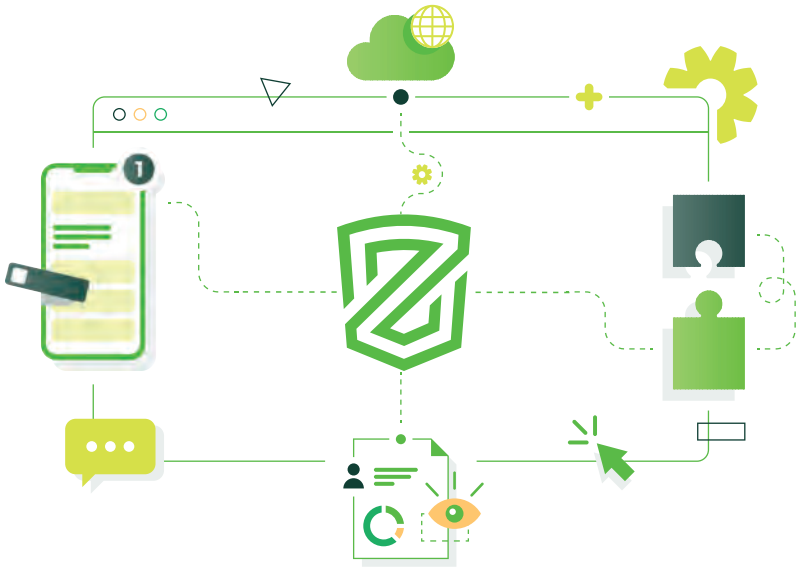
Another key benefit of ZorroSign digital signatures is that they help to **streamline and automate** business processes. By using digital signatures, you can eliminate the need for paper-based signatures and reduce the time and costs associated with such manual processes. This improves efficiency, reduces costs, and allows your organization to "go green" with more sustainable and ecologically-friendly business operations.

ZorroSign's data security platform built on blockchain also provides a secure way for companies to comply with regulatory requirements. Many industries have regulations that require companies to provide secure and tamper-proof records of transactions—ZorroSign helps companies to meet such requirements by providing a secure and auditable record of transactions.

Further, ZorroSign delivers IDaaS capabilities created to enhance online user experiences, secure access to critical enterprise applications, and reduce IT resource-related expenses with efficient identity and access management (IAM) and privileged access management (PAM).

The overarching goal of all IDaaS solutions is to ensure users are who they claim to be—and to give users access to applications, data, systems, or other digital resources as authorized by your organization. ZorroSign meets this goal via MFA and passwordless authentication, and the patented Z-Forensics ("4n6") token—a kind of digital seal that captures the complete audit trail and the document's DNA. The Z-Forensics token **securely reads** the information from ZorroSign's servers so it can be accessed by the document originator or third parties (with permission from the originator) when requested.

Only ZorroSign's patented **Z-Forensics token** allows you to manage permissions as to who gets to see what level of information about the transaction and the document; stores the ZorroSign security encryption certificates (which—unlike other digital security certificates—never expire); and can verify, validate and authenticate both digital and printed (paper) version of electronically signed documents.



Finally, ZorroSign leverages passwordless authentication via the biometric security of Apple and Android mobile devices—logging in to the device (and ZorroSign app) with hardware biometric capture features such as face, fingerprint, and iris scans. Such biometric login facilitates passwordless user authentication at the device-level for subsequent ZorroSign digital signatures and document management.

ZorroSign also validates multiple dimensions of authentication based on the transaction security needs:

- **What you know** — your ZorroSign login password or knowledge-based authentication
- **What you have** — your PC or mobile device
- **Who you are** — biometrics such as finger prints, eye iris on the device securing who can access it

And ZorroSign's dynamic knowledge-based authentication (KBA) feature—provided by LexisNexis—requires the knowledge of private information of the individual to prove that the person providing their identity information is the actual person.

With ZorroSign's user authentication options, it is almost impossible for an imposter to sign a document on the ZorroSign platform, ensuring legal enforceability and signature attribution.

United, these dynamic and integrated technologies allow ZorroSign to provide unmatched privacy and security for your users: Blockchain technology, digital signatures, IDaaS capabilities, patented Z-Forensics, and passwordless authentication all in one readily integrated platform.

Companies looking to deliver superior data security should incorporate ZorroSign into your security stack. When the risk is personal and everything is on the line: Block it down!

ZorroSign®

Contact ZorroSign today to learn more!
Visit ZorroSign.com or email sales@zorrosign.com