ManageEngine
DataSecurity Plus

BUILDING CYBER RESILIENCE

A comprehensive guide to addressing

DATA SECURITY THREATS

www.datasecurityplus.com

Table of Contents

1. Introduction

> *Murphy's law states, "Anything that can go wrong will go wrong."*
>
> *But we prefer Maya Angelou's, "Hoping for the best, prepared for the worst, and unsurprised by anything in between."*

It's no secret that the amount of data created, stored, and shared across mediums is increasing exponentially every year. A Statista report states that nearly 150 zettabytes (ZB) of data is forecasted to be generated in 2024, in contrast to just 60ZB in 2020. While only 2% of that data is stored year over year, that still leaves over 3ZB of data to be stored and secured by organizations worldwide in 2024, and that number is only increasing.

1ZB is equal to 1 billion TB.

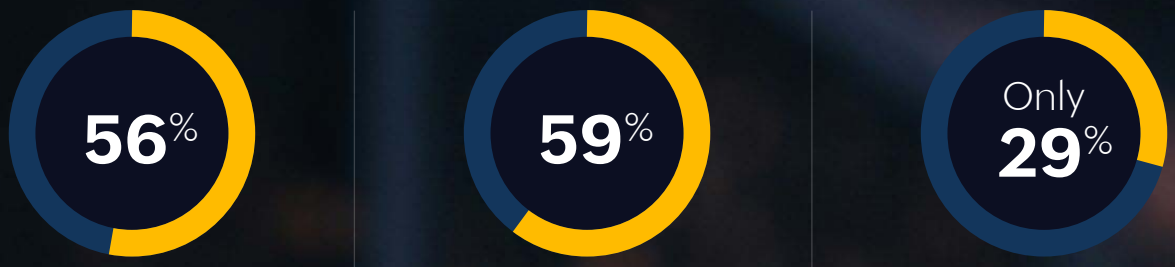
Most security analysts and CISOs are aware of this projection and are preparing to rapidly scale up to efficiently secure and manage such large volumes of data. This guide is meant to aid in that endeavor, starting with a quick background on the evolving landscape of data security, followed by examining the current challenges faced by organizations and industries in protecting their data, and ending with developing a data security policy tailored to the specific requirements of your organization.

1.1. What is data security?

In a nutshell, data security refers to the protection of digital data in storage, in use, and in transit from unauthorized access, use, disclosure, alteration, or destruction. It involves implementing measures to ensure the confidentiality, integrity, and availability of data.

1.2. Importance of data security

Whether you are a small and medium-sized business (SMB) or an enterprise organization, building cyber resilience to preemptively and effectively fend off malevolent entities stands as an unequivocal necessity. A resilient system is one which can ensure business continuity in the event of cyberthreats. A strong, cyber resilient strategy begins with a proper data security program, which can help you:



Source: CNBC | Momentive Q3 2021 Small Business Survey

1.3. The current threat landscape

The current data security landscape is marked by escalating threats and an evolving array of challenges. Cybersecurity incidents continue to rise, with ransomware, malware, and social engineering attacks taking the top spots. Growing trends such as zero-day exploits, large-scale DDoS attacks on mobile networks, IoT attacks, and AI-enabled disinformation and deepfakes are forecasted to be significant threats in the coming years. Notably, industries such as healthcare, finance, and manufacturing are among the most affected. As data breaches become more sophisticated, cybersecurity experts advocate for a holistic data security approach, combining technologies and complex interconnected systems that can provide continuous protection across all attack surfaces. Gartner's 2023 cybersecurity report outlines three key priorities for organizations to prepare for:

Responsive systems:
Focusing on improving organization readiness with efficient threat intelligence and management

Restructuring approaches:
Focusing on consistent solutions across platforms and greater attack coverage

Rebalancing practices:
Focusing on human-centric security design and improving human management

2. What makes data security harder in this day and age?

In this age of information, where the avenues of threats are countless, protecting data on an enterprise level is not easy, and it's definitely not for the faint-hearted. Here are some reasons why it's getting increasingly harder to protect data.

2.1. Logistics of data storage and protection

Managing the flow of data from creation to storage to protection is complicated because of:

The sheer amount of data

While big data analytics offer valuable insights, the exponential growth of data makes it harder for organizations to manage large datasets efficiently.

Larger user communities

As more users join global networks, data traverses various geographical locations and diverse network infrastructures, leading to more entry points and targets.

Global networking

Interconnectedness facilitates the swift propagation of threats—a single compromise can cascade through vast networks, affecting individuals, organizations, and even entire industries.

The value of data

Whether for financial gain, corporate espionage, or to disrupt critical operations, attackers are motivated by the potential profits derived from stealing, tampering with, or destroying data.

2.2. Cloud computing

As organizations migrate their data to the cloud, striking a balance between accessibility and security becomes hard because of:

A lack of data visibility

The decentralized nature of cloud environments makes it challenging for organizations to maintain a comprehensive understanding of where their data resides, who has access to it, and how it is being utilized.

Cloud misconfigurations

Inadvertent human errors, such as improperly setting access controls, exposed storage buckets, or incorrectly configured network settings, create potential entry points for unauthorized access and data breaches.

Unauthorized access to cloud data

Either because of targeted attacks, poor access management, or vulnerabilities in cloud infrastructure, malicious actors can exploit unintended access points and gain unauthorized entry.

2.3. IoT and mobile devices

The advent of the Internet of Things (IoT) and the widespread use of mobile devices makes data security harder, primarily because of:

Diverse ecosystems

Various devices from different manufacturers running on different platforms and protocols make it challenging to ensure data security on all devices.

Weak authentication and authorization

The lack of robust authentication and authorization mechanisms coupled with insecure communication channels make connected devices susceptible to unauthorized access.

Firmware vulnerabilities

Insecure coding practices and a lack of timely security patches can leave devices exposed to known vulnerabilities.

Difficulty in patching

Poorly executed integrations between IoT devices and mobile platforms with existing IT infrastructure may create security gaps.

2.4. AI

The very advancements that empower artificial intelligence (AI) in improving cybersecurity measures can also pose challenges because of:

Data privacy issues

The requirement of large datasets to train AI models can bring ethical and legal complications surrounding the privacy of individuals whose data is used.

Mass adoption of AI

The rapid adoption of AI technologies can outpace traditional security measures and the establishment of standardized security protocols.

Model poisoning

Attackers manipulate training data to compromise the integrity of AI models, leading to biased or incorrect insights from deceptive data.

AI-driven attacks

Attackers use machine learning algorithms to continuously evolve their tactics, techniques, and procedures, making it difficult for organizations to detect and mitigate attacks.

3. Common data security threats

Regardless of their size or sector, all businesses face a common array of threats that necessitate proactive measures. From the dynamic challenges posed by a wide variety of cyberattacks to the risks of accidental data exposure, insider threats, and the subtle complexities of shadow IT, threats are abundant.

3.1. Cyberattacks

Cyberattacks encompass a wide range of tactics and techniques designed by individuals, organized groups, or nation-states to disrupt, steal, alter, or destroy digital information. Let's quickly go through some common forms of cyberattacks, including what they are, how they originate, what their goals are, and what type of data they target:

Type	What it is	How it originates	Goal	Target
Ransomware	Malicious software that encrypts victims' data, rendering it inaccessible until a ransom is paid	Malicious emails, infected websites, or vulnerabilities in outdated software	Direct financial gain	Any data on the infected system
Social engineering	Tricks individuals into divulging confidential information or performing actions that compromise security	Phishing emails, phone calls, or impersonation	Gain access to systems and data	Login credentials, financial information, or PII
Malware	Malicious software that when installed can spread and affect computer systems	Downloading infected files or clicking malicious links	Disrupt, damage, or steal data	Any data on the infected system
DDoS	Floods the target website with a massive volume of fake traffic, rendering it inaccessible	Attackers use a network of compromised computers, known as botnets	Disrupt services	Stop legitimate users from accessing a service or website

3.2. Accidental exposure

Accidental exposure occurs when sensitive information is inadvertently made public. A 2023 WinZip report on data security found that human errors, system misconfigurations, and inadequate data protection protocols are the primary factors leading to accidental exposure.

Human errors

- Sending emails to the wrong recipients
- Unintentional data sharing
- Lack of awareness about data security policies

Misconfigurations

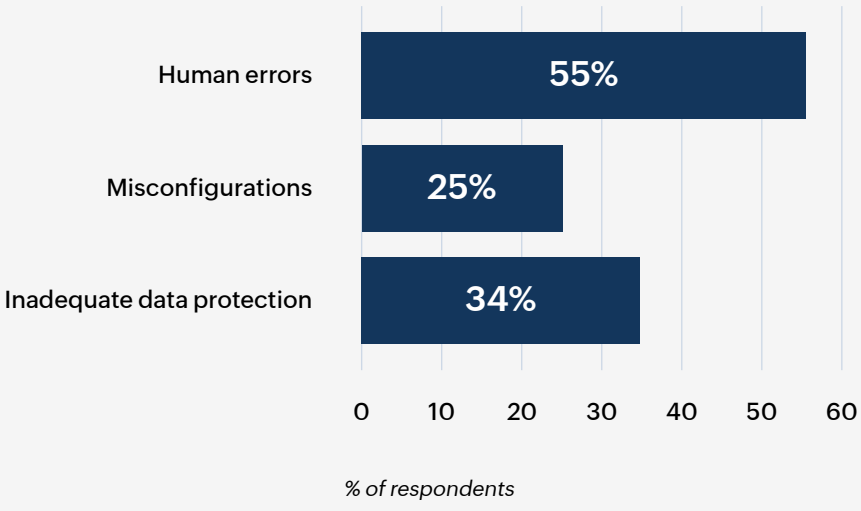
- Inappropriate file permissions
- Misconfigured access controls
- Using default configurations
- Programming errors

Inadequate data protection

- Weak encryption
- Outdated security patches
- Inadequate access controls
- Poor endpoint security

Common factors leading to accidental exposure

Source: Winzip 2023 Data Seurity Report



3.3. Insider threats

Insider threats occur when employees or any authorized personnel compromise the data security of an organization intentionally or unintentionally. While insider threats come in many forms and sizes, they all fall under three categories:

- **Malicious insiders:**
  Disgruntled employees or paid criminal agents use their legitimate or stolen credentials to disrupt, steal, or misuse data.
- **Careless users:**
  A negligent user clicking phishing emails, deleting sensitive files, using an unsecured public network, or using weak credentials can lead to data leakage.
- **Third-party contractors:**
  Inadequate or ignorant security practices by third-party vendors can create security gaps.

Real-life example:

An employee of Google's autonomous car subsidiary, Waymo, downloaded 14,000 confidential IP files (marketing data, test drive videos, and confidential PDFs) using his credentials to establish his own self-driving car start-up.

3.4. Shadow IT

Shadow IT refers to the use of unauthorized applications, services, or devices within an organization without the knowledge of the IT department. This phenomenon typically arises as a result of one of the following reasons:

- **Proactive employees:**
  Employees independently adopt external tools or services to improve productivity or meet specific business needs, bypassing formal IT channels.
- **Ease of accessibility:**
  Too much red tape for accessing applications or services within an organization can drive employees to resort to unauthorized means for quicker and easier access.
- **Unsatisfactory internal IT services:**
  If internal IT services are perceived as inefficient, employees may turn to external alternatives that better suit their needs.
- **Lack of awareness:**
  Either due to ignorance or inadequate IT policies, many employees may be unaware of the potential dangers of using unauthorized applications.

Top technologies employees use without proper authorization:

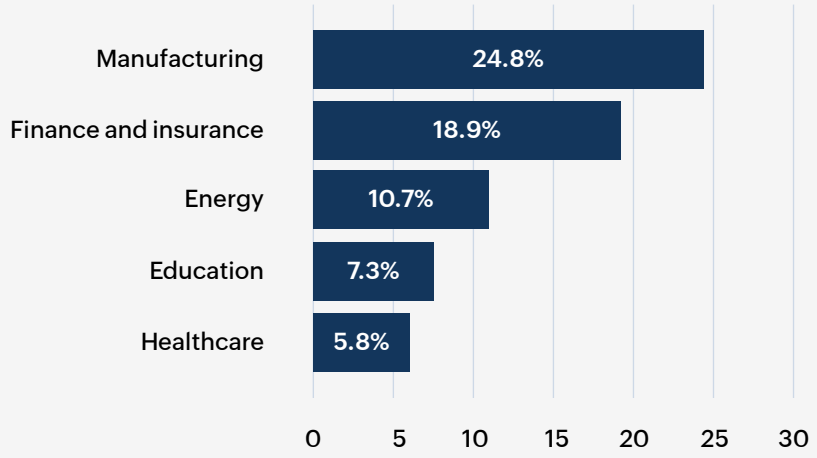
- Cloud-based applications
- Collaboration tools
- File sharing platforms
- Communication services

4. Industry-wise data security threats

A Statista report found that the manufacturing sector witnessed the highest proportion of cyberattacks globally, comprising almost 25% of the total incidents in 2022, followed by finance, energy, education, and healthcare. While threats such as cyberattacks, accidental exposure, and insider threats are common to all of these industries, as described above, they also grapple with distinct challenges.

Distribution of cyberattacks across worldwide industries in 2022

Source: Statista



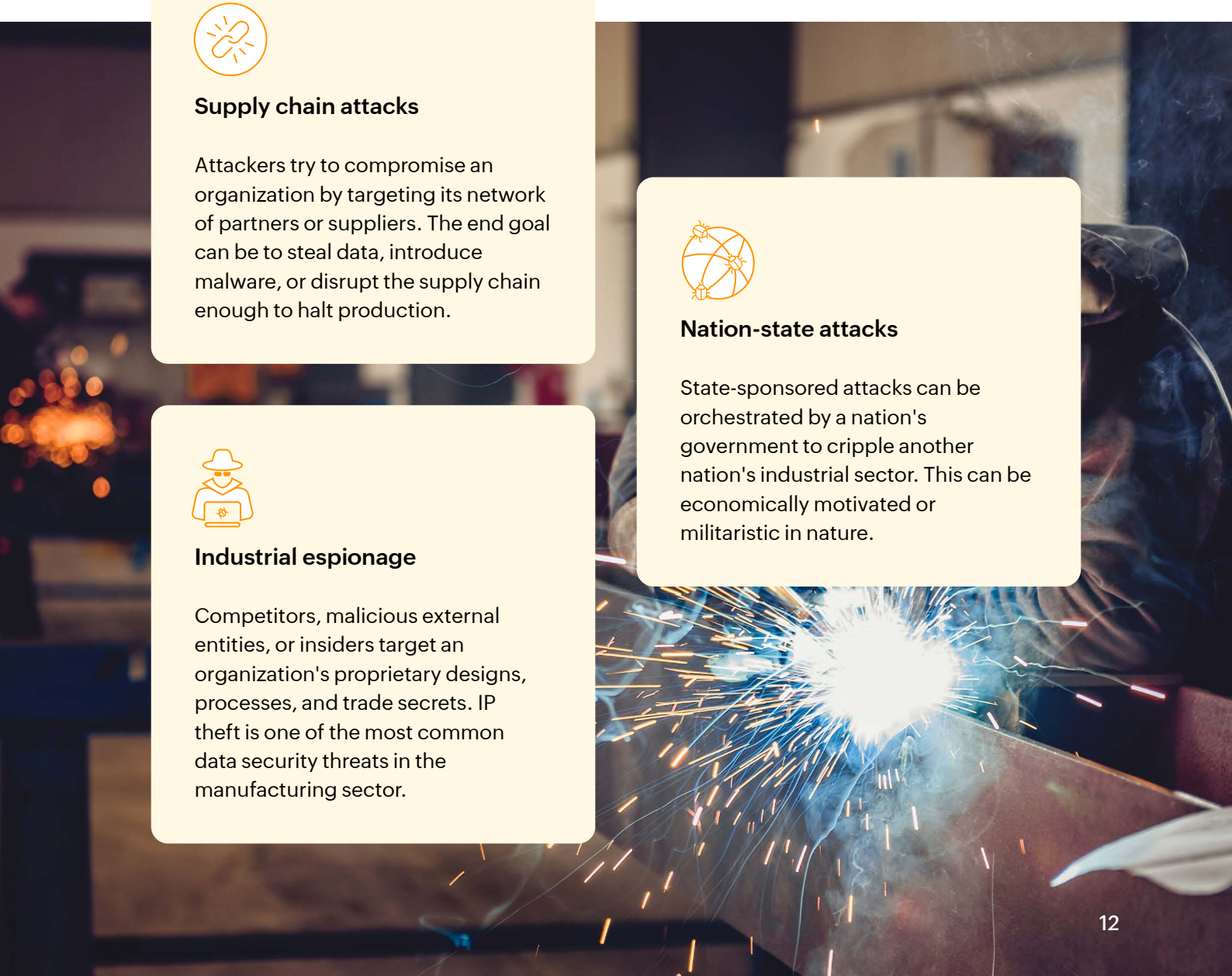
4.1. Manufacturing

30% of extortion attempts in 2022 targeted the manufacturing industry.

- IBM threat intelligence report

Acute time sensitivity, the value and necessity of the product being manufactured, and a lack of employee awareness create a happy hunting ground for attackers. Integrating interconnected systems and smart technologies into production processes only makes it more enticing. Common attack vectors such as ransomware, phishing, and IoT devices are highly effective.

For example, a company that doesn't want to endure production delays would be inclined to pay ransomware attackers. In other cases, tricking employees with a phishing attack may be easier because manufacturing companies have employees from a vast hierarchy of technical expertise, including those who aren't aware of phishing. While such threats are prevalent and exhausting, manufacturing organizations are also susceptible to a few other threats specific to that industry.



Supply chain attacks

Attackers try to compromise an organization by targeting its network of partners or suppliers. The end goal can be to steal data, introduce malware, or disrupt the supply chain enough to halt production.

Nation-state attacks

State-sponsored attacks can be orchestrated by a nation's government to cripple another nation's industrial sector. This can be economically motivated or militaristic in nature.

Industrial espionage

Competitors, malicious external entities, or insiders target an organization's proprietary designs, processes, and trade secrets. IP theft is one of the most common data security threats in the manufacturing sector.

4.2. Finance

In the world of finance, the phrase "information is currency" is often more true than "currency is currency".

As we rely more on digital platforms, smart grids, and IoT devices, the potential for redirecting payments, selling data, and exploiting critical files for ransom is very high at banking, investment, and insurance institutions.

Phishing attacks to steal financial credentials, DDoS attacks to bring down financial sites, and supply chain attacks to compromise merchant sites are all widespread. There are also banker trojans, spoofing, and advanced persistent threats (APTs).

Banker trojans

This is software that poses as legitimate until installation, after which it can covertly capture login credentials, financial transaction details, and even manipulate transactions.

APTs

Hackers gain access to a network and remain undetected for an extended period while they steal data.

Spoofing

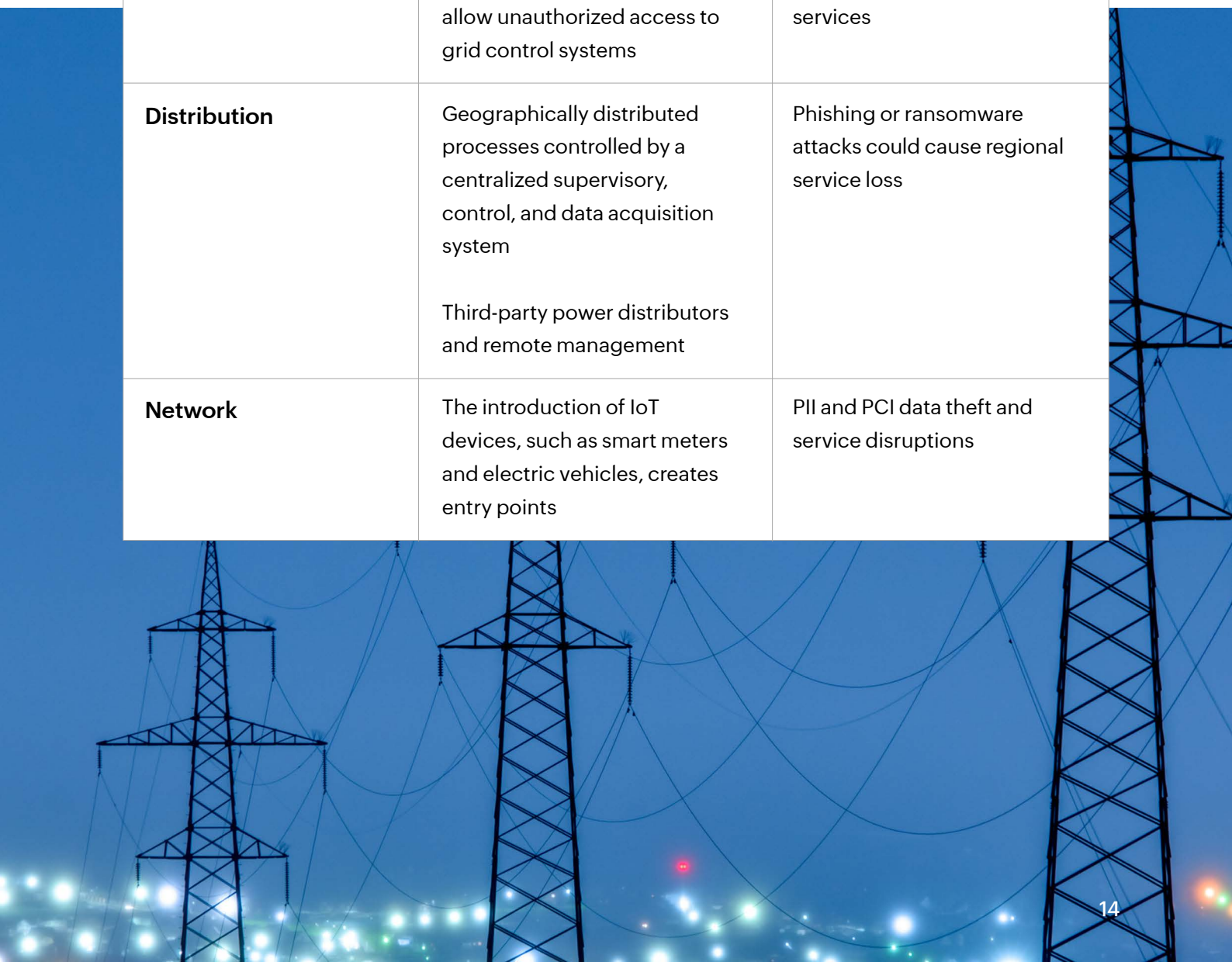
Users' login credentials are captured using a fake website with the same layout and a similar domain as a legitimate financial institution's website.

4.3. Energy

Digitization, in a way, forces critical infrastructure systems to be exposed to the internet, making them an easy target. The Colonial Pipeline ransomware attack sent shock waves throughout the industry, underscoring the inherent vulnerabilities in the energy sector.

Because of electric-power and gas companies' long value chain, each stage of the chain faces distinct challenges, in addition to common threats such as ransomware attacks, supply chain attacks, and mobile device phishing attacks.

Value chain stage	Vulnerabilities	Threat vector
Generation	Outdated devices and applications deployed across legacy generation systems	DDoS and ransomware attacks
Transmission	Physical security weaknesses allow unauthorized access to grid control systems	Remote disruption of services
Distribution	Geographically distributed processes controlled by a centralized supervisory, control, and data acquisition system Third-party power distributors and remote management	Phishing or ransomware attacks could cause regional service loss
Network	The introduction of IoT devices, such as smart meters and electric vehicles, creates entry points	PII and PCI data theft and service disruptions



4.4. Education

Check Point's 2022 Mid-Year Report showed a 44% increase in cyberattacks in the education and research sector when compared with the previous year. Common attack vectors such as ransomware, phishing, and exploiting system vulnerabilities are easily exploitable for the following reasons:

- **Phishing**

  Ignorant students and overworked teachers are easy pickings for phishing attacks. When targeted with messages related to educational materials, grades, or any school-related information, students and teachers are more likely to assume they are legitimate, primarily due to the inherent trust existing in the education infrastructure.

- **Ransomware**

  Schools and colleges often exhibit a concerning inclination to pay ransoms, similar to the manufacturing sector. It may be primarily driven by the high stakes involved, as compromised data includes that of the underaged.

- **Weak credentials from multiple logins**

  The necessity for students and teachers to log in to multiple platforms as part of their curriculum forces them to create weaker and easily memorable credentials, which are susceptible to brute-force attacks.

- **Cascading compromises in online learning platforms**

  The integration of online learning platforms with third-party service providers introduces a potential domino effect in the education system. Any compromise in one section of the platform could cascade across the entire ecosystem, disrupting the seamless delivery of education.

- **Red tape and outdated systems**

  Publicly funded school systems encounter challenges in replacing outdated devices and systems due to bureaucratic red tape. The prolonged use of outdated technology introduces a host of vulnerabilities, creating an environment susceptible to cyberthreats.

Vast amount of data under a single umbrella

Students' personal information	Financial information	University research data	Patented and intellectual property

4.5. Healthcare

The fact that HIPAA was enacted in 1996, when threats to PHI were significantly lower, clearly shows how important and valuable patient confidentiality and privacy is.

Beyond the financial gain and breach of privacy, loss of patient data or disruption of medical services can also put lives at risk. The largely unknown story of a ransomware attack that led to the death of a woman in Germany in 2020 brings to light the impact of data security threats in the medical industry. Stolen records can be used to gain unauthorized access to medical programs or to get prescription medications that can be fatal. And so, hackers are highly motivated to breach healthcare institutions.

A **ransomware attack** could literally hold lives hostage in exchange for anything they want, and the institutions would have to pay.

A **supply chain attack** on any one of the hundreds of SaaS applications that healthcare organizations use could spread across systems and bring operations to a halt.

A **DDoS attack** could prevent hospital administration from accessing patients' records, their appointments, test results, or insurance information.

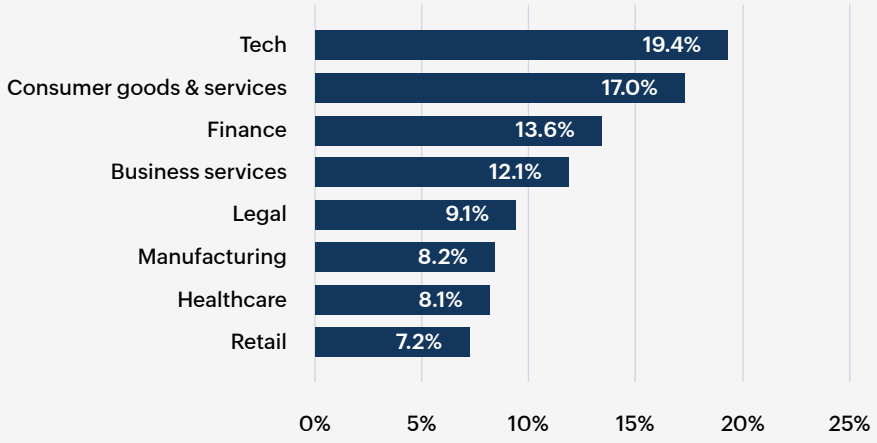
Exploiting the vulnerabilities in increasingly interconnected medical equipment could directly disrupt the timely delivery of critical healthcare services.

5. Choosing a data security solution that's right for you

In 2004, the global cybersecurity market was a mere $3.5 billion. Fast-forward to 2025, and forecasts predict astounding growth to $450 billion, highlighting the escalating awareness about the paramount importance of IT security across industries. According to IANS Research's 2023 Security Budget Benchmark Summary Report, on average, 11% of a company's annual IT spending is allocated to IT security, reflecting a notable 4% increase from 2020.

% of annual IT budget spent on cybersecurity

Source: IANS & Artico, 2023 Security Budget Benchmark Summary



% budget share of cybersecurity

As industries worldwide are swiftly ramping up their cybersecurity spending, the challenge lies in judiciously investing these funds. The reality of choice fatigue is undeniable, given the plethora of available options. On top of that, many companies don't clearly know what kind of security measures to invest in. Even companies at the forefront of cybersecurity often find themselves burdened with redundant and unnecessarily expensive security measures. This redundancy may stem from the challenges associated with migration, industry connections, or simply a lack of awareness regarding superior solutions.

Therefore, it is imperative to pause and periodically assess the specific security needs of your company. Ideally, your chosen solution or combinations thereof should comprehensively address security requirements, provide regular updates through periodic reports, ensure compliance with industry-specific regulatory mandates, and be cost-effective.

Although most solutions have overlapping features, your comprehensive data security platform should cover the following aspects of data security:

5.1. Automated data visibility

Data discovery and classification form the cornerstone of any effort to secure sensitive and critical data. The process involves systematically identifying, categorizing, and labeling data based on its sensitivity and importance within an organization. This includes understanding where the data resides, what types of data need to be protected, and what format the data is stored in. Your data visibility software should have the following abilities:

- **Data sources and storage environments**: The ability to discover and classify data across a diverse storage environment that can include databases, file servers, cloud repositories, and endpoints.
- **Types of sensitive data**: The ability to discover and classify sensitive data, such as PII, health records, financial records, and intellectual property.
- **Structured and unstructured data**: The ability to address both structured data—residing in databases and organized formats—and unstructured data, found in documents, emails, and multimedia files. The solution you choose should effectively analyze both types, employing techniques like pattern recognition and content analysis.
- **Regulatory standards**: The ability to facilitate adherence to compliance requirements such as the GDPR, HIPAA, and the PCI DSS by providing a systematic approach to data discovery and classification with comprehensive audit trails and reports.

5.2. Accelerated auditing and reporting

File auditing involves the meticulous examination of data activities across all data sources and storage environments within an organization, providing a detailed log of who accessed what data, when, and how. An ideal auditing and reporting solution should:

- **Capture detailed activity records**: Event logging is foundational to auditing and captures detailed records of data activities, such as file accesses, modifications, deletions, and permission changes, providing a chronological trail for thorough analysis.

Ensure accessibility of logged data

Ease of accessibility to audit data allows authorized personnel to review data activities promptly. It also provides transparency and oversight.

Deliver real-time alerts about anomalies

Real-time alerting is a critical feature, allowing organizations to receive immediate notifications about suspicious or unauthorized file activities.

Generate comprehensive reports

Another critical feature is customizable reports that cover key metrics to achieve compliance and provide management insights to aid in strategic decision-making.

5.3. Access management

Strong access management should involve a comprehensive strategy for managing user identities and monitoring user accesses to sensitive data, i.e., authentication and authorization.

5.3.1. Authentication

User authentication is the process of verifying and validating the identity of users before granting them access to sensitive data, systems, or digital resources. The core components of user authentication are:

- **Credential management:**
  Issuing, storing, and organizing large volumes of credentials, which can be something the user knows (passwords or PINs), something they have (smart cards or security tokens), or something they are (biometric data like fingerprints or facial recognition).

- **Password policies:**
  Requiring strong and unique passwords, implementing regular password changes, and educating users on the dangers of weak or compromised passwords.

- **Zero Trust model:**
  Embracing a Zero Trust model involves continuously verifying user identity and access, regardless of their location or network.

- **Session management:**
  Managing session timeouts, secure cookie handling, and protection against session hijacking helps maintain user authentication throughout an active session.

5.3.2. Authorization

User authorization is the process of granting or restricting users' access to sensitive data, systems, or digital resources. The core components of user authorization are:

- **Roles and permissions management:**
  Defining what responsibilities or tasks are associated with a specific job function and what actions that users with a particular job function are allowed to perform.

- **Principle of least privilege:**
  Granting users only the minimum level of access necessary to perform their job functions.

- **Enforcing access control policies:**
  Monitoring access, location, device used, and user attributes.

- **Audit trails and continuous monitoring:**
  Generating detailed reports on user access and modifications, and getting notified about potential issues like permission inconsistencies or overexposed files.

5.4. Endpoint security

Enterprise endpoint security involves protecting the myriad of devices an organization uses, including desktop computers, laptops, servers, smartphones, tablets, and IoT devices. While antivirus software protects individual endpoints from malware intrusions, a comprehensive endpoint security solution monitors and prevents data loss on an enterprise level.

Capabilities of an endpoint data loss prevention solution: Defines and enforces data loss prevention policies across all endpoints to control and monitor various user activities, like:

- **File activity and integrity control:** Monitors and manages file interactions to prevent unauthorized access or transfers.

- **Network activity control:** Ensures secure sharing of data across networks.

- **USB device control:** Manages and restricts the use of USB devices.

- **Web control:** Monitors web activities to prevent access to malicious or unauthorized sites.

- **Application control:** Manages and controls the usage of suspicious and shadow applications.

5.5. Cloud data security

Cloud security refers to the implementation of security measures to protect data stored, processed, and transmitted within cloud computing environments. With the introduction of a shared responsibility model, security responsibilities are now split between the cloud service provider and the customer (an individual or a company). The provider is required to ensure the security of the cloud infrastructure, and the customer is responsible for securing their data, applications, and configurations within the cloud environment. This collaborative approach refocuses enterprises' cloud security towards data protection. So, a good cloud data security solution should:

- Discover and classify data across all cloud environments.
- Implement robust authentication and access controls on cloud data.
- Encrypt data at rest, in transit, and in use.
- Continuously monitor cloud applications.
- Address shadow IT challenges by preventing unauthorized use of cloud services.
- Possess threat detection mechanisms to identify and respond to security threats.

5.6. Encryption

Data encryption software uses algorithms and cryptographic keys to convert plaintext data into a coded or unreadable format, known as ciphertext. When choosing encryption software, it should:

- Adhere to recognized encryption standards, such as the Advanced Encryption Standard.
- Encrypt data in all states, i.e., at rest, in transit, and in use.
- Selectively encrypt specific files, folders, or data elements, allowing you to apply encryption based on sensitivity levels.
- Provide effective key management practices to generate, store, and distribute encryption keys securely. This includes key rotation, backup, and access control.
- Establish and enforce encryption policies that dictate when and how encryption should be applied.

5.7. Backup and recovery

Backup and recovery is an integral component of data security, and in most cases, it's the final resort. When a system is breached and data is lost, all isn't lost. There's still one more trick up your sleeve when you have backups of your data ready to be restored. A good data backup and recovery solution should have the following capabilities:

- **Scalability:** The ability to handle the growing volume of data and the subsequent storage needs.
- **Simplicity:** User-friendly and straightforward implementation and operation to reduce risk of errors.
- **Speed of recovery:** Rapid restoration is necessary for minimizing downtime and ensuring business continuity.
- **Customizable policies:** Select the frequency and retention policies of your backups. Decide how many copies you want, on how many storage types, and whether you want an additional offsite backup.

5.8. In short... DSPM

Data security posture management (DSPM) combines all the key aspects of data security into a holistic approach towards continuously assessing and managing an organization's security posture. Starting from data visibility, auditing, and risk assessment to vulnerability management, compliance monitoring, and incident response, DSPM provides a comprehensive view of an organization's data security health.

As data becomes more valuable and the regulatory environment more stringent, the adoption of DSPM is not just a security best practice but a strategic imperative for any modern organization aiming to safeguard its digital assets and maintain the trust of its stakeholders.

6. How DataSecurity Plus can help you address data security threats

With five dedicated solutions bundled together to address distinct aspects of DSPM, ManageEngine DataSecurity Plus can simplify your data protection strategy. With an easy-to-use interface and insightful dashboards and reports, DataSecurity Plus automates monitoring and reporting to a much higher degree.

Explore **DataSecurity Plus' capabilities**

File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

LEARN MORE

File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

LEARN MORE

Data risk assessment

Discover and classify files containing sensitive data, such as PII, PCI, and ePHI, by combining content inspection and contextual analysis.

LEARN MORE

Data leak prevention

Monitor endpoint file activities, and detect and disrupt data leaks via USBs, email, web applications, and printers.

LEARN MORE

Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

LEARN MORE

Our Products

AD360 | Log360 | ADAudit Plus | EventLog Analyzer

Exchange Reporter Plus | SharePoint Manager Plus

7. Wrapping up

The landscape of data security is on the brink of transformative shifts, fueled by emerging trends that organizations must navigate adeptly. The advent of technologies like AI and quantum computing presents both opportunities and challenges, requiring organizations to strike a delicate balance in their adoption of robust data security. The regulatory landscape is also becoming increasingly intricate, demanding a proactive and adaptive approach to compliance.

Amidst the digital revolution and widespread remote work, the human factor emerges as a pivotal element in data security. Elevating employee awareness and education becomes imperative for comprehensive data protection.

The battle for data security is continuous and multifaceted, necessitating holistic strategies like DSPM that incorporate proactive measures, dynamic threat intelligence, and adaptive technologies.

In the face of exponential cybersecurity market growth, judicious investment becomes paramount. Organizations must focus on building a resilient security framework tailored to their needs, integrating emerging technologies efficiently, and staying abreast of the ever-shifting regulatory landscape. This strategic approach fortifies defenses against evolving threats and maintains data integrity in our interconnected and data-centric world.

References

https://www.winzip.com/en/resources/reports/data-security/report/

https://thehackernews.com/2023/09/new-survey-uncovers-how-companies-are.html

https://www.statista.com/statistics/871513/worldwide-data-created/

https://explodingtopics.com/blog/data-generated-per-day

https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023

https://www.devry.edu/blog/cyber-security-facts.html

https://www.exabeam.com/explainers/insider-threat/insider-threat-examples/

https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches

https://www.ibm.com/reports/threat-intelligence

https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2022.pdf

https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

https://www.wired.co.uk/article/job-security-cybersecurity-alec-ross

https://cdn.iansresearch.com/Files/Marketing/2023SurveyContent/IANS+ArticoSearch-2023SecurityBudgetBenchmarkSummaryReport.pdf