MaximAlert
Technology. Transformation. Trust.

Data Privacy

What is data privacy?

Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behaviour. Just as someone may wish to exclude people from a private conversation, many online users want to control or prevent certain types of personal data collection.

As Internet usage has increased over the years, so has the importance of data privacy. Websites, applications, and social media platforms often need to collect and store personal data about users in order to provide services. However, some applications and platforms may exceed users' expectations for data collection and usage, leaving users with less privacy than they realized. Other apps and platforms may not place adequate safeguards around the data they collect, which can result in a data breach that compromises user privacy.

Why is data privacy important?

In many jurisdictions, privacy is considered a fundamental human right, and data protection laws exist to guard that right. Data privacy is also important because in order for individuals to be willing to engage online, they have to trust that their personal data will be handled with care. Organizations use data protection practices to demonstrate to their customers and users that they can be trusted with their personal data.

Personal data can be misused in a number of ways if it is not kept private or if people don’t have the ability to control how their information is used:

- Criminals can use personal data to defraud or harass users.
- Entities may sell personal data to advertisers or other outside parties without user consent, which can result in users receiving unwanted marketing or advertising.
- When a person's activities are tracked and monitored, this may restrict their ability to express themselves freely, especially under repressive governments.

For individuals, any of these outcomes can be harmful. For a business, these outcomes can irreparably harm their reputation, as well as resulting in fines, sanctions, and other legal consequences.
In addition to the real-world implications of privacy infringements, many people and countries hold that privacy has intrinsic value: that privacy is a human right fundamental to a free society, like the right to free speech.

What are the laws that govern data privacy?

As technological advances have improved data collection and surveillance capabilities, governments around the world have started passing laws regulating what kind of data can be collected about users, how that data can be used, and how data should be stored and protected. Some of the most important regulatory privacy frameworks to know include:

• THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: An Act introduced by the Indian government to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process

• Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

What are some of the challenges users face when protecting their online privacy?

• Online tracking: User behavior is regularly tracked online. Cookies often record a user's activities, and while most countries require websites to alert users of cookie usage, users may not be aware of to what degree cookies are recording their activities.

• Losing control of data: With so many online services in common use, individuals may not be aware of how their data is being shared beyond the websites with which they interact online, and they may not have a say over what happens to their data.

• Lack of transparency: To use web applications, users often have to provide personal data like their name, email, phone number, or location; meanwhile, the privacy policies associated with those applications may be dense and difficult to understand.

• Social media: It is easier than ever to find someone online using social media platforms, and social media posts may reveal more personal information than users realize. In addition, social media platforms often collect more data than users are aware of.

• Cyber crime: Many attackers try to steal user data in order to commit fraud, compromise secure systems, or sell it on underground markets to parties who will use the data for malicious purposes. Some attackers use phishing attacks to try to trick users into revealing personal information; others attempt to compromise companies' internal systems that contain personal data.

What are some of the challenges businesses face when protecting user privacy?

• Communication: Organizations sometimes struggle to communicate clearly to their users what personal data they are

such personal data for lawful purposes and for matters connected therewith or incidental thereto.

• General Data Protection Regulation (GDPR): Regulates how the personal data of European Union (EU) data subjects, meaning individuals, can be collected, stored, and processed, and gives data subjects rights to control their personal data (including a right to be forgotten).

• National data protection laws: Many countries, such as Canada, Japan, Australia, Singapore, and others, have comprehensive data protection laws in some form. Some, like Brazil's General Law for the Protection of Personal Data and the UK's Data Protection Act, are quite similar to the GDPR.

There are also industry-specific privacy guidelines in some countries: for instance, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) governs how personal healthcare data should be handled.

However, many privacy advocates argue that individuals still do not have sufficient control over what happens to their personal data. Governments around the world may pass additional data privacy laws in the future.

Key principles of the DPDPA

The DPDPA is based on six key principles:

• Lawfulness: Personal data must be processed lawfully, fairly, and transparently.

• Purpose Limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

• Data Minimization: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

• Accuracy: Personal data must be accurate and, where necessary, kept up to date.

• Storage Limitation: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

• Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

What are some of the challenges users face when protecting their online privacy?

• **Online tracking:** User behavior is regularly tracked online. Cookies often record a user's activities, and while most countries require websites to alert users of cookie usage, users may not be aware of to what degree cookies are recording their activities.

• **Losing control of data:** With so many online services in common use, individuals may not be aware of how their data is being shared beyond the websites with which they interact online, and they may not have a say over what happens to their data.

• **Lack of transparency:** To use web applications, users often have to provide personal data like their name, email, phone number, or location; meanwhile, the privacy policies associated with those applications may be dense and difficult to understand.

• **Social media:** It is easier than ever to find someone online using social media platforms, and social media posts may reveal more personal information than users realize. In addition, social media platforms often collect more data than users are aware of.

• **Cyber crime**: Many attackers try to steal user data in order to commit fraud, compromise secure systems, or sell it on underground markets to parties who will use the data for malicious purposes. Some attackers use phishing attacks to try to trick users into revealing personal information; others attempt to compromise companies' internal systems that contain personal data.

What are some of the challenges businesses face when protecting user privacy?

tOrganizations sometimes struggle to communicate clearly to their users what personal data they are collecting and how they use it.

• **Cyber crime:** Attackers target both individual users and organizations that collect and store data about those users. In addition, as more aspects of a business become Internet-connected, the attack surface increases.
• **Data breaches:** A data breach can lead to a massive violation of user privacy if personal details are leaked, and attackers continue to refine the techniques they use to cause these breaches.
• **Insider threats:** Internal employees or contractors might inappropriately access data if it is not adequately protected.

Our Approach:
We work with vendors who ensure that data protection is built into the system from the ground up and embedded in the design process.
Using Threat Modelling for Data privacy and technologies that enhance Privacy, they allow for the translation of abstract privacy principles into auditable, repeatable actions that can be methodically applied to data. This ensures that privacy measures are consistently implemented and are not merely theoretical.
These vendors offer automatic, mathematical methods to secure data through technologies such as differential privacy, expert determination anonymization, federated learning, secure multi-party compute etc.
Process
• Data Privacy Threat Modelling based risk assessment: Utilizing advanced privacy attack simulation techniques to analyse risk in data flows, system architectures, and potential attack vectors.
• Privacy enhancement techniques -based Mitigatory Recommendations : Implementing appropriate enhancement technologies depending upon the type of data or insight flow requirement to mitigate identified risks.
• Integration with business ecosystem: Integrate threat modelling tools with data sources and data flows, connect DPIA process with privacy threat modellimng to make it augmented DPIA, integrate the results into data pipelines to make it DevPrivacyOps, configuring

enhancement technologies in collaboration with business teams, verifying effectiveness, sharing output for teams to follow.

Privacy Controls

Cryptographic Protection: Ensures confidentiality and integrity of sensitive data through encryption techniques.

Anonymous Data Transformation: Anonymizes personally identifiable information (PII) in datasets to preserve privacy while maintaining data utility.

Access Governance: Regulates access to sensitive information based on user roles and permissions, ensuring data privacy and compliance.

Tokenization Solutions: Replaces sensitive data elements with unique tokens to minimize the risk of data exposure and unauthorized access.

Masking Techniques: Conceals sensitive information in datasets, protecting privacy during data processing, testing, and sharing.

Data Obfuscation Methods: Obscures sensitive data elements to maintain data integrity while safeguarding privacy.

Homomorphic Encryption Solutions: Enables secure computation on encrypted data, ensuring privacy-preserving data processing.

Differential Privacy Measures: Adds statistical noise to query responses to preserve individual privacy during data analysis.

De-identification Strategies: Removes direct and indirect identifiers from datasets to prevent re-identification and protect individual privacy.

Privacy Controls:

• AI-powered tool that performs dynamic assessments of privacy risks, visualizing potential threats and helping organizations mitigate risks proactively.

• Data analysis tool that scans and summarizes Personally Identifiable Information (PII) in unstructured data within a database. It helps organizations improve data security and compliance by providing insights into PII distribution across various file types.

• Mapping, analysis, and documentation of DPIA activities by augmenting with Privacy threat modeling , ensuring GDPR compliance and promoting informed privacy decision-making.
• Advanced data anonymization including expert grade statistical anonymization with mathematical proof that ensures sensitive data can be used for analytics without compromising individual privacy
• State-of-the-art encryption and decryption capabilities, securing data at the most granular level with customizable key generation strategies, cryptographic data sharing, API based purpose centric de-identification and data minimisation for cross border transfers
• Employs advanced differential privacy techniques to protect individual data points during analysis, ensuring data confidentiality in analytics.
• Generates synthetic data that mirrors real-world datasets but contains no real personal information, allowing for safe use in testing and development environments
• Privacy Risk and Generation AI Governance specially tailored for Large Language Models (LLMs). Organizations can safeguard their data, navigate complex risks, and ensure responsible AI practices with ease, integrating user safety, AI model security and LLM governance as per various emerging AI regulatory requirements.

Web and Email Security

What Is Web Security?

Web security is a broad category of security solutions that protect your users, devices, and wider network against internet-based cyberattacks—malware, phishing, and more—that can lead to breaches and data loss. It reduces the security risk to your organization when your users accidentally access malicious files and websites through some combination of sandboxing, URL filtering, and various other security and access controls.

What's the Purpose of Web Security?

The massive importance of the internet for modern enterprises—and the accompanying growth in the sophistication, frequency, and impact of cyberattacks—has made web security critical to business continuity. It's your first line of defense against threats that can lead to the exposure of

sensitive data, costly ransoms, reputational harm, compliance violations, and a host of other consequences. Once the domain of mostly small-time hackers, internet-borne threats have evolved into a massive black market business that touches the worlds of organized crime as well as state-sponsored espionage and sabotage. Some of the latest threats are incredibly sophisticated, able to easily fool the untrained eye or bypass legacy security. Plus, with an array of ready-made tools, exploit kits, JavaScript modules, and even fully developed campaigns for sale, even a novice actor can easily launch an attack.

Cybersecurity Ventures estimates that, by 2025, global cybercrime will cost US$10.5 trillion annually—a greater profit than the entire world's major illicit drug trade—and half the world's data will live in the cloud. Given what's at stake, it's easy to see why effective web security is so important today.

What Are the Benefits of Web Security?

For a modern enterprise, effective web security has broad technical and human benefits:

- Protect your business and stay compliant by preventing loss of sensitive data
- Protect customers and employees by securing their private information
- Avoid costly service interruptions by preventing infections and exploits
- Offer a better user experience by helping your users stay safe and productive
- Maintain customer loyalty and trust by staying secure and out of the news

Great strides in cloud and mobility technology let your employees and customers connect with you with unprecedented ease and flexibility. Unfortunately, that cuts both ways, and attackers have more ways to approach your organization's wider attack surface. With the right web protections in place, you can spend more time taking advantage of the benefits, and less worrying about security threats.

What Does Web Security Protect Against?

MaximAlert
Technology. Transformation. Trust.

Web security casts a wide net to protect users and endpoints from malicious emails, encrypted threats, malicious or compromised websites and databases, malicious redirects, hijacking, and more. Let's look at a few of the most common threats in more detail:

• Ransomware: These attacks encrypt data, and then demand a ransom payment in exchange for a decryption key. In a double-extortion attack, your data is also exfiltrated.

• General malware: Countless variants of malware exist that can lead to anything from data leaks, spying, and unauthorized access to lockouts, errors, and system crashes.

• Phishing: Often carried out through email, text messages, or malicious websites, these attacks trick users into things like divulging login credentials or downloading spyware.

• SQL injection: These attacks exploit an input vulnerability in a database server, allowing an attacker to execute commands that let them retrieve, manipulate, or delete data.

• Denial of service (DoS): These attacks slow or even shut down a network device such as a server by sending it more data than it can process. In distributed DoS—that is, a DDoS attack—this is carried out by many hijacked devices at once.

• Cross-site scripting (XSS): In this type of injection attack, an attacker introduces malicious code to a trusted website by entering it in an unprotected user input field.

How can MaximAlert help?

• We work with leading secure web gateway vendors that provide on-premise as well as cloud-delivered solutions, so it enforces security policies consistently, no matter where users connect, what endpoint devices they're using, or where applications are hosted.

• Our partner vendor solutions are built on a global multitenant cloud architecture for massive scalability, so it can inspect all encrypted traffic without degrading performance.

• Additionally, our partner vendors provide an integrated, cloud native platform that greatly reduces your operational complexity and costs.

Email Security

What is Email Security?

Email security is the practice of protecting email accounts and communications from unauthorized access, loss, or compromise. Organizations can enhance their email security posture by establishing policies and using tools to protect against malicious threats such as malware, spam, and phishing attacks. Cybercriminals target email because it is an easy entry point to other accounts and devices—and it relies in large part on human error. All it takes is one misguided click to cause a security crisis for an entire organization.

Why is email security important?

Email has been a primary communication tool in the workplace for more than two decades. More than 333 billion emails are sent and received daily worldwide—and employees get an average of 120 emails a day. This spells opportunity for cybercriminals who use business email compromise attacks, malware, phishing campaigns, and a host of other methods to steal valuable information from businesses. Most cyberattacks—94 percent—begin with a malicious email. Cybercrime cost more than USD$4.1 billion in 2020, with business email compromise causing the most damage, according to the FBI's Internet Crime Complaint Center (IC3). The consequences can be severe, leading to significant financial, data, and reputational losses.

The benefits of email security

Businesses of all sizes are realizing the importance of prioritizing email security. An email security solution that safeguards employee communication and reduces cyberthreats is important because it helps to:

• Protect a company's brand, reputation, and bottom line. Email threats can lead to devastating costs, operational disruption, and other severe consequences.

• Enhance productivity. With a robust email security solution in place, businesses can reduce potential disruptions to operations and downtime because of a cyberattack. An effective solution helps

security teams streamline response and stay ahead of increasingly sophisticated threats.
• Ensure compliance with data protection laws such as the General Data Protection Regulation (GDPR) and help circumvent the many intangible costs of a cyberattack such as business disruption, legal fees, regulatory fines.

t

In response to the fast-changing email threat landscape, enterprises have established email security best practices to support communication and guard against threats. Top email security best practices include:
• Educate employees with periodic training to minimize the risk of human error and ensure that employees—often considered a company's first line of defense—understand the importance of email security.
• Invest in user awareness training so users can learn how to recognize the signs of a phishing attack and other indicators of malicious intent.
• Upgrade to an email security solution that provides advanced threat protection.
• Implement multifactor authentication (MFA) to prevent account compromise. Asking users to provide more than one way to sign into accounts is an easy way to help secure organizational data.
• Review protections against business email compromise attacks through methods like spoofing and impersonation.
• Move high-risk processes and transactions to more authenticated systems.

Types of email threats

• Data exfiltration: Data exfiltration is the unauthorized transfer of data from an organization either manually or through malicious programming. Email gateways help make sure businesses avoid sending sensitive data without authorization, which could lead to a costly data breach

• Malware: Malware is short for malicious software, and its primary aim is to damage or disrupt computers and computer systems. Common types of malware include viruses, worms, ransomware, and spyware.
• Spam: Spam is an unsolicited message sent in bulk and without the recipient's consent. Businesses use spam email for commercial purposes. Scammers use spam to spread malware, trick recipients into divulging sensitive information, or extort money.
• Impersonation: Impersonation occurs when cyber criminals pretend to be a trusted person or organization to secure money or data via email. Business email compromise is one example in which a scammer impersonates an employee to steal from the company or its customers and partners.
• Phishing: Phishing is the practice of pretending to be a trusted person or organization to trick victims into disclosing valuable information such login credentials and other types of sensitive data. Different types of phishing include spear phishing, vishing, and whaling.

How can MaximAlert help with email security services

Email security services help companies protect email accounts and communication from cyberthreats. The best way for companies to implement email security is to create and maintain a policy for using email and share that with employees so they are aware of email security best practices, Common email security services available for individuals, schools, communities, and organizations include:
• Detonation capabilities that scan incoming, outgoing, and internal email for malicious links and attachments.
• Data encryption to secure mail communications from being intercepted by cybercriminals.
• Image and content control capabilities to scan attached or embedded images and content for malware and blocks them from being downloaded.
• Spam filters that filter unwanted email like bulk and spam messages.
• Authentication systems to evaluate the validity of senders

MaximAlert
Technology. Transformation. Trust.

Database Security

What is database security?

Database security refers to the range of tools, controls and measures designed to establish and preserve database confidentiality, integrity and availability. Confidentiality is the element that's compromised in most data breaches.

Database security must address and protect the following:

• The data in the database.
• The database management system (DBMS).
• Any associated applications.
• The physical database server or the virtual database server and the underlying hardware.
• The computing or network infrastructure that is used to access the database.

Database security is a complex and challenging endeavor that involves all aspects of information security technologies and practices. It's also naturally at odds with database usability. The more accessible and usable the database, the more vulnerable it is to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use.

Why is it important?

By definition, a data breach is a failure to maintain the confidentiality of data in a database. How much harm a data breach inflicts on your enterprise depends on various consequences or factors:

• Compromised intellectual property: Your intellectual property—trade secrets, inventions, proprietary practices—can be critical to your ability to maintain a competitive advantage in your market. If that intellectual property is stolen or exposed, your competitive advantage can be difficult or impossible to maintain or recover.
• Damage to brand reputation: Customers or partners might be unwilling to buy your products or services (or do business with your company) if they don't feel they can trust you to protect your data or theirs.

• Business continuity (or lack thereof): Some businesses cannot continue to operate until a breach is resolved.
• Fines or penalties for non-compliance: The financial impact for failing to comply with global regulations such as the Sarbannes-Oxley Act (SAO) or Payment Card Industry Data Security Standard (PCI DSS), industry-specific data privacy regulations such as HIPAA, or regional data privacy regulations, such as Europe's General Data Protection Regulation (GDPR) can be devastating, with fines in the worst cases exceeding several million dollars per violation.
• Costs of repairing breaches and notifying customers: In addition to the cost of communicating a breach to customer, a breached organization must pay for forensic and investigative activities, crisis management, triage, repair of the affected systems and more.

Common threats and challenges

Many software misconfigurations, vulnerabilities or patterns of carelessness or misuse can result in breaches. The following are among the most common types or causes of database security attacks.

Insider threats

An insider threat is a security threat from any one of three sources with privileged access to the database:
• A malicious insider who intends to do harm.
• A negligent insider who makes errors that make the database vulnerable to attack.
• An infiltrator, an outsider who somehow obtains credentials via a scheme, such as phishing or by gaining access to the credential database itself.

Insider threats are among the most common causes of database security breaches and are often the result of allowing too many employees to hold privileged user access credentials.

Human error

Accidents, weak passwords, password sharing and other unwise or uninformed user behaviors continue to be the cause of nearly half (49%) of all reported data breaches.

Exploitation of database software vulnerabilities

Hackers make their living by finding and targeting vulnerabilities in all kinds of software, including database management software. All major commercial database software vendors and open source database management platforms issue regular security patches to address these vulnerabilities, but failure to apply these patches in a timely fashion can increase your exposure.

SQL or NoSQL injection attacks

A database-specific threat, these involve the insertion of arbitrary SQL or non-SQL attack strings into database queries that are served by web applications or HTTP headers. Organizations that don't follow secure web application coding practices and perform regular vulnerability testing are open to these attacks.

Buffer overflow exploitation

Buffer overflow occurs when a process attempts to write more data to a fixed-length block of memory than it is allowed to hold. Attackers can use the excess data, which is stored in adjacent memory addresses, as a foundation from which to start attacks.

Malware

Malware is software that is written specifically to take advantage of vulnerabilities or otherwise cause damage to the database. Malware can arrive via any endpoint device connecting to the database's network.

Attacks on backups

Organizations that fail to protect backup data with the same stringent controls that are used to protect the database itself can be vulnerable to attacks on backups.

These threats are exacerbated by the following:

• Growing data volumes: Data capture, storage and processing continues to grow exponentially across nearly all organizations. Any data security tools or practices need to be highly scalable to meet near and distant future needs.

• Infrastructure sprawl: Network environments are becoming increasingly complex, particularly as businesses move workloads

to multicloud or hybrid cloud architectures, making the choice, deployment and management of security solutions ever more challenging.

• Increasingly stringent regulatory requirements: The worldwide regulatory compliance landscape continues to grow in complexity, making adhering to all mandates more difficult.

• Cybersecurity skills shortage: Experts predict there might be as many as 8 million unfilled cybersecurity positions by 2025.

Denial of service (DoS and DDoS) attacks

In a denial of service (DoS) attack, the attacker deluges the target server—in this case the database server—with so many requests that the server can no longer fulfill legitimate requests from actual users, and, often, the server becomes unstable or crashes.

In a distributed denial of service attack (DDoS), the deluge comes from multiple servers, making it more difficult to stop the attack.

Best practices

When evaluating database security in your environment to decide on your team's top priorities, consider each of the following areas:

• Physical security: Whether your database server is on-premises or in a cloud data center, it must be located within a secure, climate-controlled environment. If your database server is in a cloud data center, your cloud provider takes care of this for you.

• Administrative and network access controls: The practical minimum number of users should have access to the database, and their permissions should be restricted to the minimum levels necessary for them to do their jobs. Likewise, network access should be limited to the minimum level of permissions necessary.

• User account and device security: Always be aware of who is accessing the database and when and how the data is being used. Data monitoring solutions can alert you if data activities are unusual or appear risky. All user devices connecting to the network housing the database should be physically secure (in the hands of the right user only) and subject to security controls at all times.

• Encryption: All data, including data in the database and credential data, should be protected with best-in-class encryption while at rest and in transit. All encryption keys should be handled in accordance with best practice guidelines.
• Database software security: Always use the latest version of your database management software, and apply all patches when they are issued.
• Application and web server security: Any application or web server that interacts with the database can be a channel for attack and should be subject to ongoing security testing and best practice management.
• Backup security: All backups, copies or images of the database must be subject to the same (or equally stringent) security controls as the database itself.
• Auditing: Record all logins to the database server and operating system, and log all operations that are performed on sensitive data as well. Database security standard audits should be performed regularly.

Controls and policies

In addition to implementing layered security controls across your entire network environment, database security requires you to establish the correct controls and policies for access to the database itself. These include:
• Administrative controls to govern installation, change and configuration management for the database.
• Preventive controls to govern access, encryption, tokenization and masking.
•Detective controls to monitor database activity monitoring and data loss prevention tools. These solutions make it possible to identify and alert on anomalous or suspicious activities.

• Database security policies should be integrated with and support your overall business goals, such as protection of critical intellectual property and your cybersecurity policies and cloud security policies.

Data protection tools and platforms

Today, a wide array of vendors offer data protection tools and platforms. A full-scale solution should include all of the following capabilities:

• Discovery: Look for a tool that can scan for and classify vulnerabilities across all your databases—whether they're hosted in the cloud or on-premises—and offer recommendations for remediating any vulnerabilities that are identified.

• Data activity monitoring: The solution should be able to monitor and audit all data activities across all databases, regardless of whether your deployment is on-premises, in the cloud, or in a container. It should alert you to suspicious activities in real-time so that you can respond to threats more quickly. You'll also want a solution that can enforce rules, policies and separation of duties and that offers visibility into the status of your data through a comprehensive and unified user interface.

• Encryption and tokenization capabilities: Upon a breach, encryption offers a final line of defense against compromise. Any tool that you choose should include flexible encryption capabilities that can safeguard data in on-premises, cloud, hybrid or multicloud environments. Look for a tool with file, volume and application encryption capabilities that conform to your industry's compliance requirements, which might demand tokenization (data masking) or advanced security key management capabilities.

• Data security optimization and risk analysis: A tool that can generate contextual insights by combining data security information with advanced analytics will enable you to accomplish optimization, risk analysis and reporting with ease. Choose a solution that can retain and synthesize large quantities of historical and recent data about the status and security of your databases, and look for one that offers data exploration, auditing and reporting capabilities through a comprehensive but user-friendly self-service dashboard.