TITANIAM

titaniam.io

Titaniam
Research Report
STATE OF ENTERPRISE TOKENIZATION 2022

Titaniam's State of Enterprise Tokenization Report for 2022 finds that with 40% of enterprises spending jaw dropping sums of over 1M per year on tokenization, 70% of them complain of inadequate coverage and compromised data resulting in a whopping 98% of enterprises ready to embrace a more modern solution provides strong security with better coverage and without usability tradeoffs.

Independent Research Conducted by CENSUSWIDE

Executive Summary

Ever since its introduction in 2001, Tokenization has remained and indispensable tool in the enterprise security toolbox. When sensitive data is tokenized, the original data is replaced with an unrelated and randomly generated token (in the case of Vaulted tokenization), or a cryptographically generated one (in the case of Vaultless tokenization). With the original data not being present in applications and databases, attackers breaking into these systems are unable to access anything of value. Tokenization serves not just a security purpose, but also speaks to privacy and compliance use cases.

It is no surprise then that enterprises are willing to go to great lengths to implement tokenization solutions, despite the extremely disruptive and resource intensive nature of traditional tokenization solutions. Beyond just the time and effort to deploy, tokenization also presents an extremely high cost in terms of business data use, essentially eliminating all rich data usage options. In its tokenized form data cannot be searched or analyzed for insight. For it to be used in an insightful way, the data must be detokenized and released right back into its original vulnerable clear text state. Some traditional tokenization solutions detokenize in memory while others release clear text into downstream analytical processes, thus limiting the overall security benefit.

However, despite having been around for over 20 years, the real impact of tokenization has been limited to payment card data and select few fields beyond that. Anytime enterprises deal in data that is truly required for insight, analytics, or rich search, tokenization fails to provide coverage. As a result we continue to see large scale breaches and sensitive data compromises in enterprises that invest millions annually into traditional tokenization solutions.

At Titaniam, we understand that what enterprises really need is the strength of tokenization without the tough tradeoffs of the past. Our product suite delivers this and we invite you discover the power of a modern data security platform that speaks to both strong security as well as data centric decision making at near real-time speeds.

In order to get first hand data on enterprise sentiment regarding current tokenization solutions as well as their asks of modern solutions, Titaniam commissioned an independent third-party to conduct a study on this topic. In this original research study covering 104 enterprises, we uncovered the true state of tokenization in enterprises. We present our findings in this report.

- Over 40% of organizations spend over $1M each year on tokenization, 99% are unsatisfied with it and are looking for modern alternatives.
- 70% of tokenization users still had sensitive data stolen and 98.6% of them believe a modern solution with better coverage would have prevented this.
- 47% cited lack of insight as the reason for minimal coverage, 44% cited poor performance, and 41% cited lack of context, all three of which represent a lack of data usability in real business use cases
- Nearly 85% detokenize protected data to use it, this negating the security benefit altogether and finally a whopping 75% complain that tokenization is cost-prohibitive.

Users unsatisfied with traditional tokenization

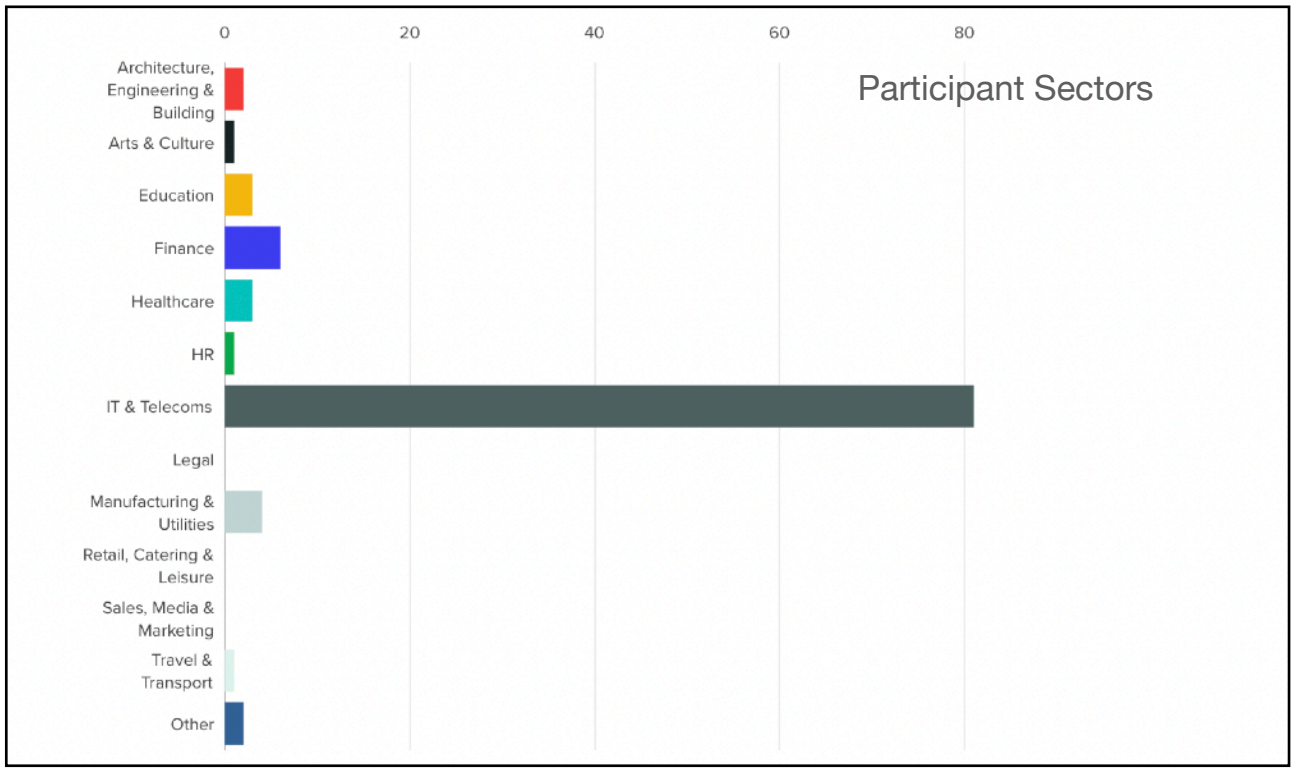
99%

Ultimately, the data showed that enterprises are tired of spending enormous amounts to protect a small portion of sensitive data and are ready for a better answer! We offer this data to you, our readers, so that you have the information you need to make a strong case for improving data security in your organization. As always, please feel free to write with questions or comments.

Best Regards,
Titaniam
info@titaniam.io

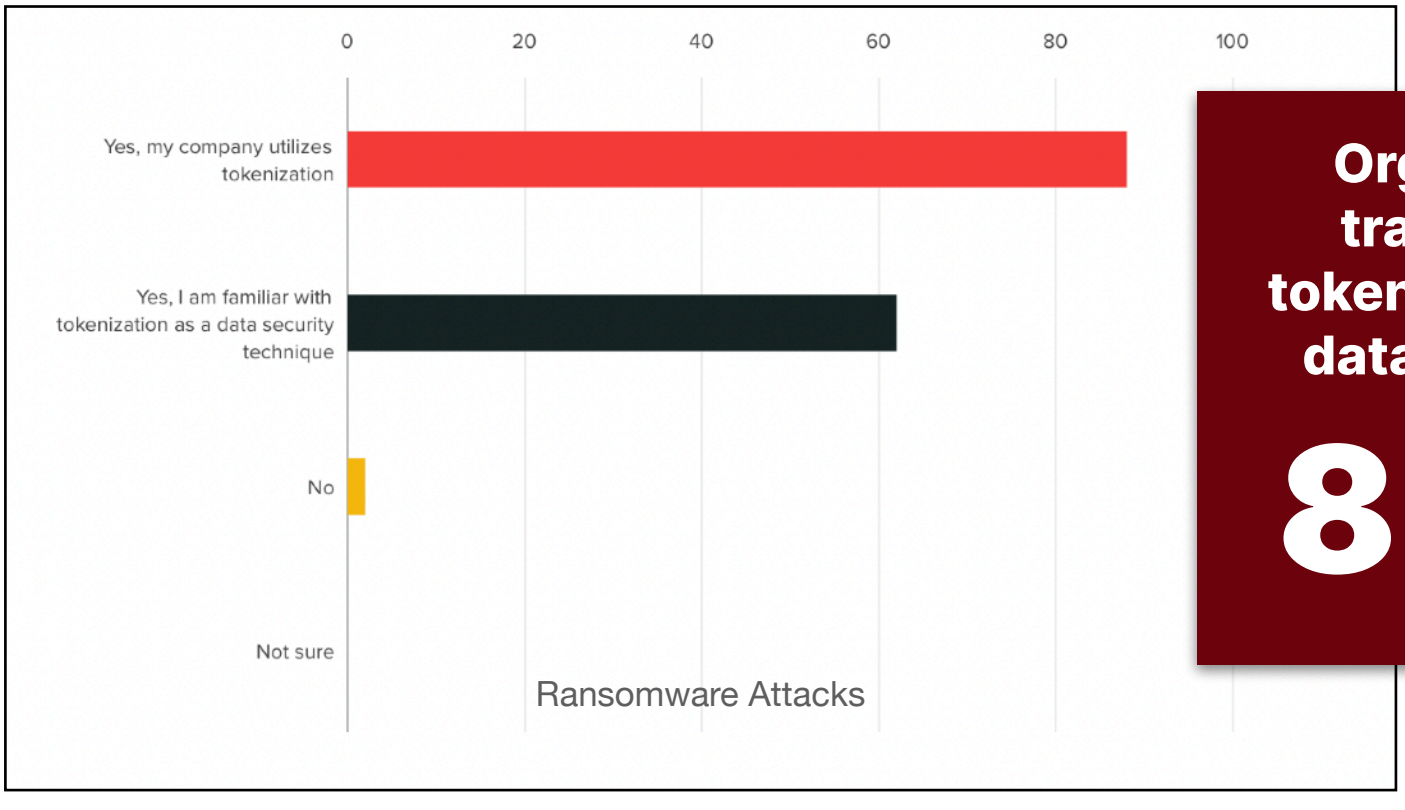
Summary of Study Participants

Titaniam's State of Tokenization Study included 104 participants across the United States from a variety of industries. Participants were all Security professionals. We requested a wide distribution cross regions and cities and participation definitely reflected this. See chart below for a breakdown of industries covered.



Tokenization is Widely Used and Well Understood

The study found that over 80% of surveyed companies utilize tokenization confirming our understanding of the prevalence of tokenization in a large majority of security conscious enterprises. The study also confirmed that there is a widespread understanding one how tokenization works with over 60% being familiar with how it works.

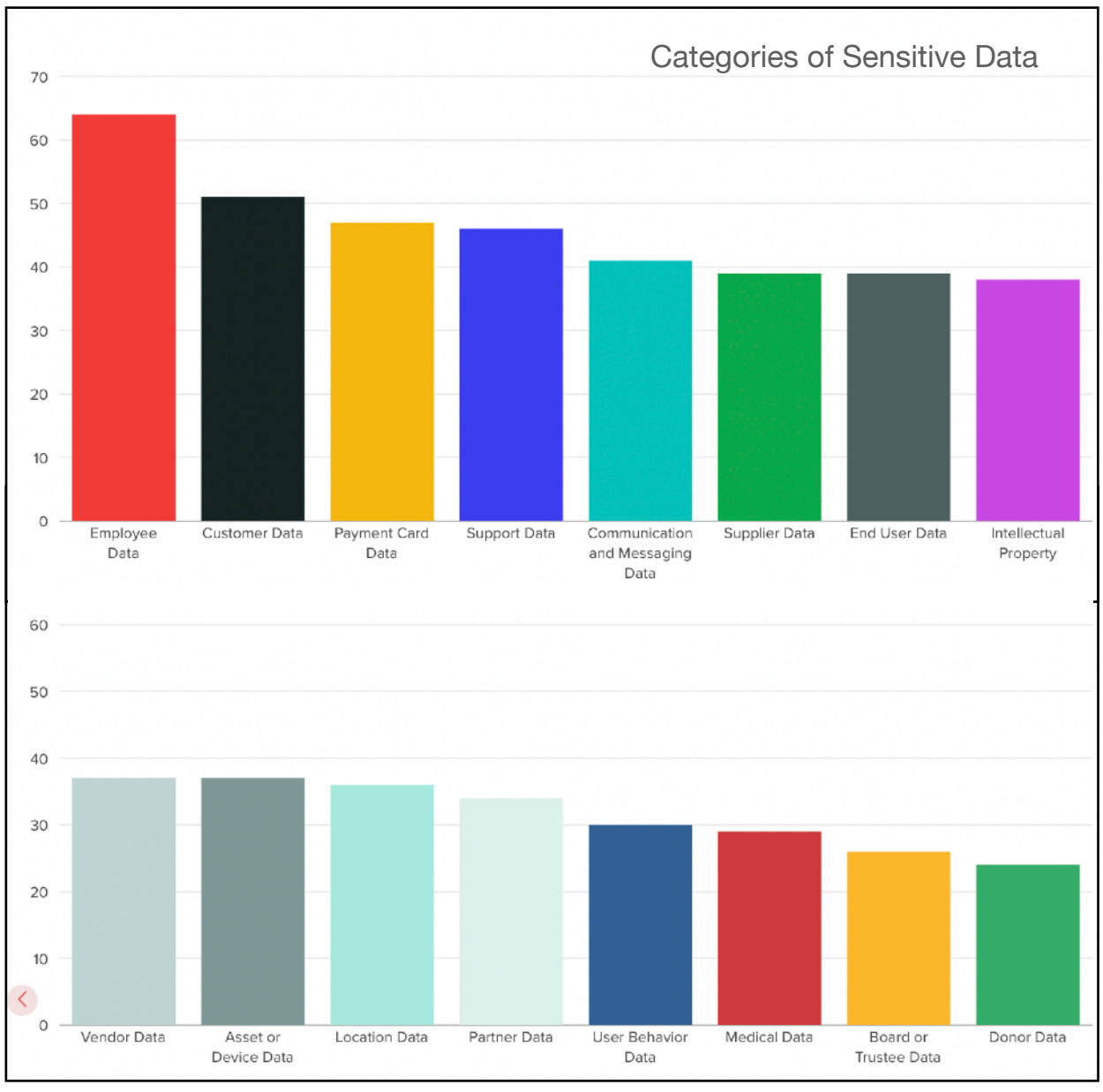


Orgs using traditional tokenization for data security

88%

Enterprises House a Wide Spectrum of Sensitive Data

With the chart below depicting all the categories of sensitive data that participating enterprises would like to protect, it is easy to see why tokenization might fall short in its ability to provide adequate coverage. For a modern data security strategy to be effective, it would need to account for the variety of data and all the business process around this sensitive data. The Y- Axis represents the number of companies out of a total of 104 participants.



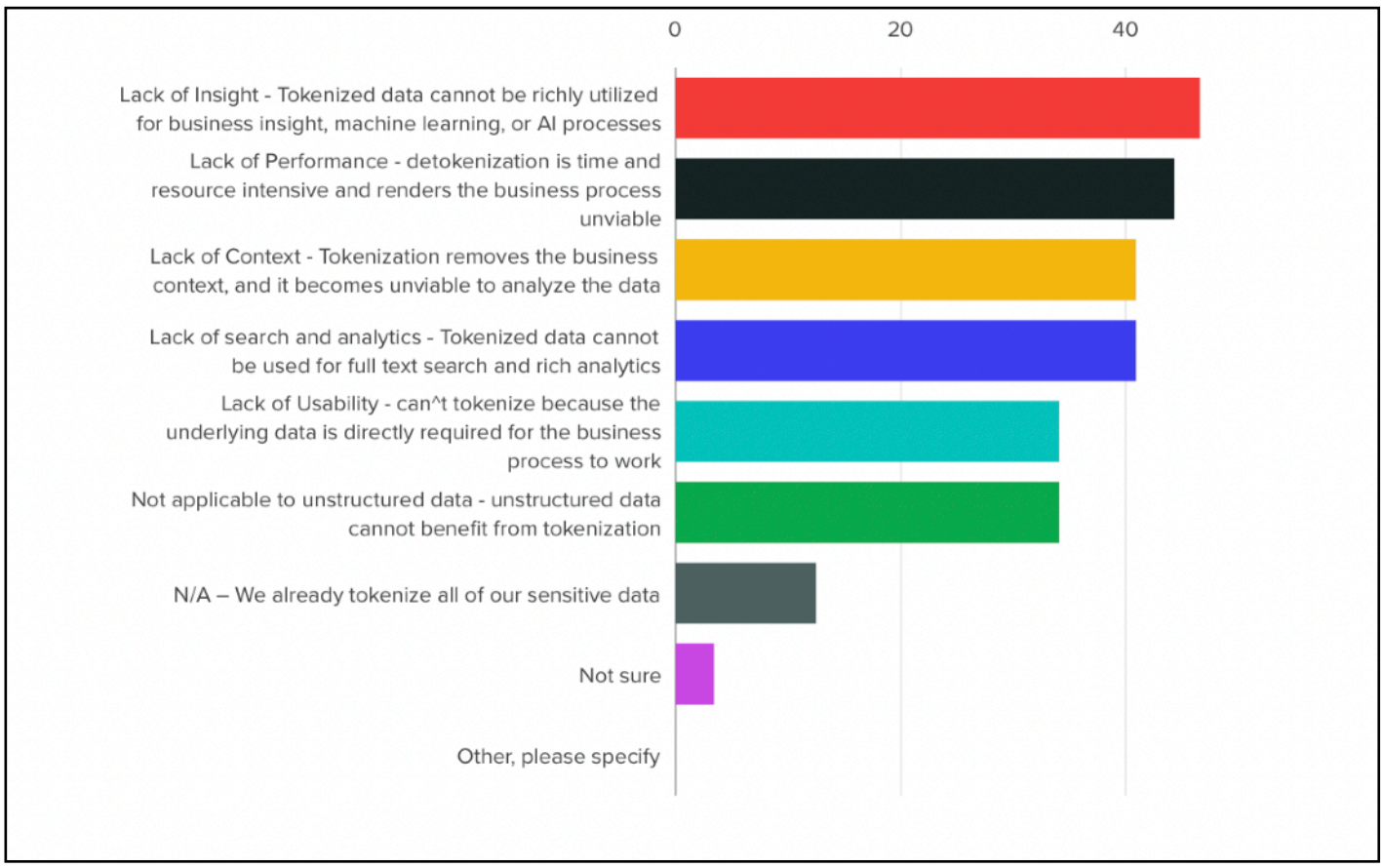
Seeing the large variety of data that needs to be protected, we were curious about how companies went about protecting this data. In particular, as it relates to tokenization, we were interested in whether it was a helpful technique to protect these categories and if not, what prevented enterprises from utilizing tokenization as a data security tool in this regard.

Separately we were also interested in learning what happens to data that is tokenized but eventually required for analytics or other type of in-depth business usage.

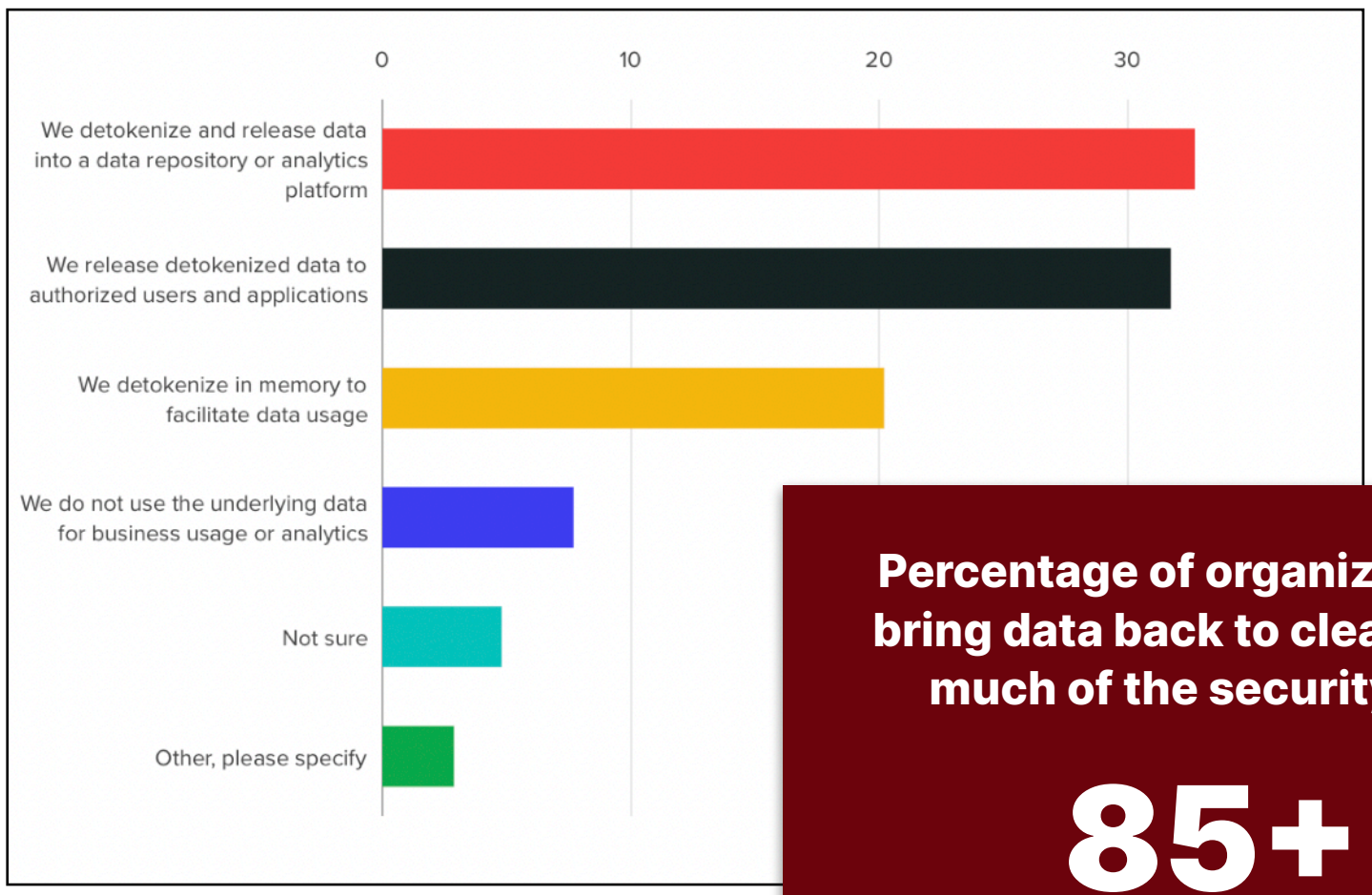
For these reasons, we set up the survey to ask a series of questions about this data that would shed light on both actual coverage as well as effectiveness of tokenization as a data security control in the enterprise. The next few questions address this area.

Even Though it is Widely Used, Tokenization Fails to Provide Coverage

The study found that even though over 80% of participants use tokenization, they are unable to use it to protect all the data that truly needs protection. When asked about what specific limitations they face, 47% cited lack of insight as the reason for minimal coverage, 44% cited poor performance, and 41% cited lack of context, all three of which represent a lack of data usability in real business use cases. The chart represents % responses.



Data that is Tokenized Still Ends up in the Clear

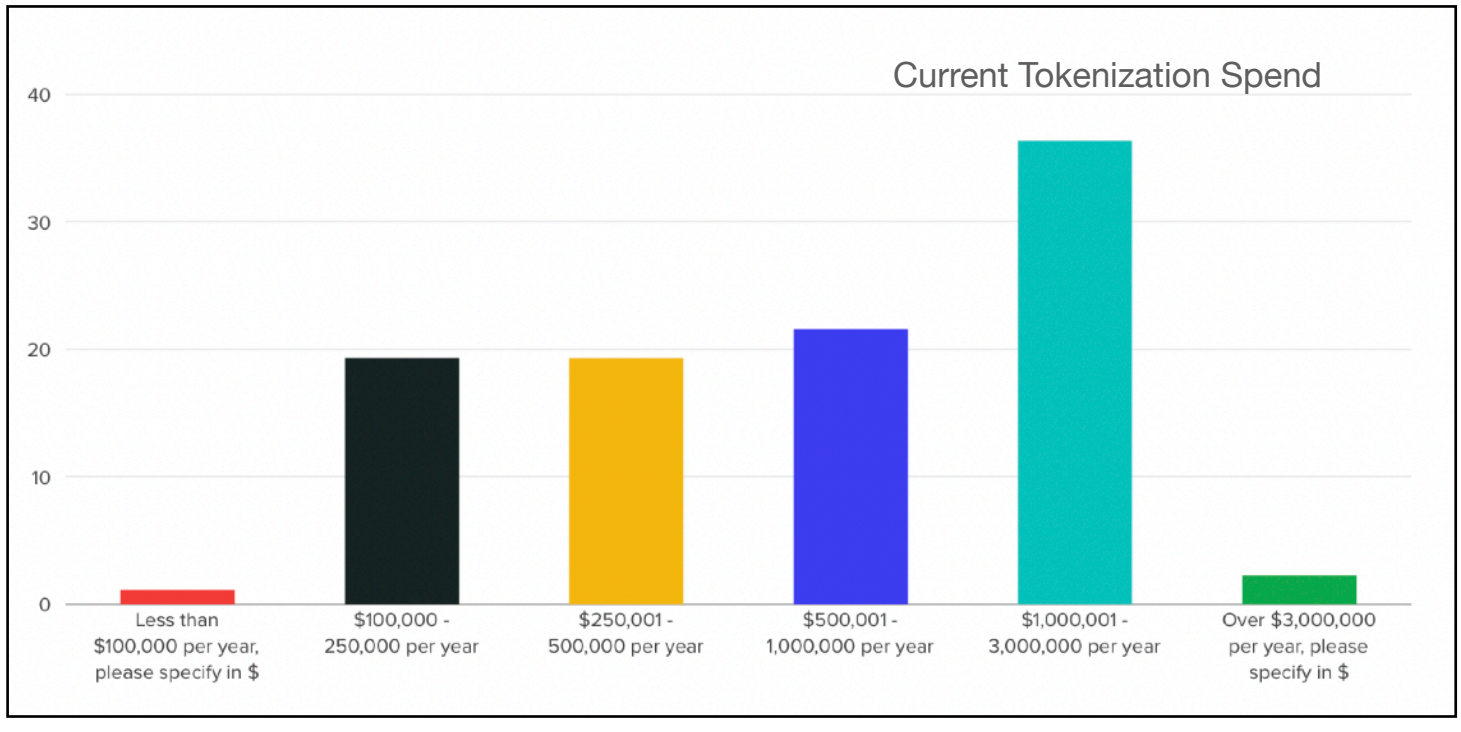


Percentage of organizations that bring data back to clear, negating much of the security benefit

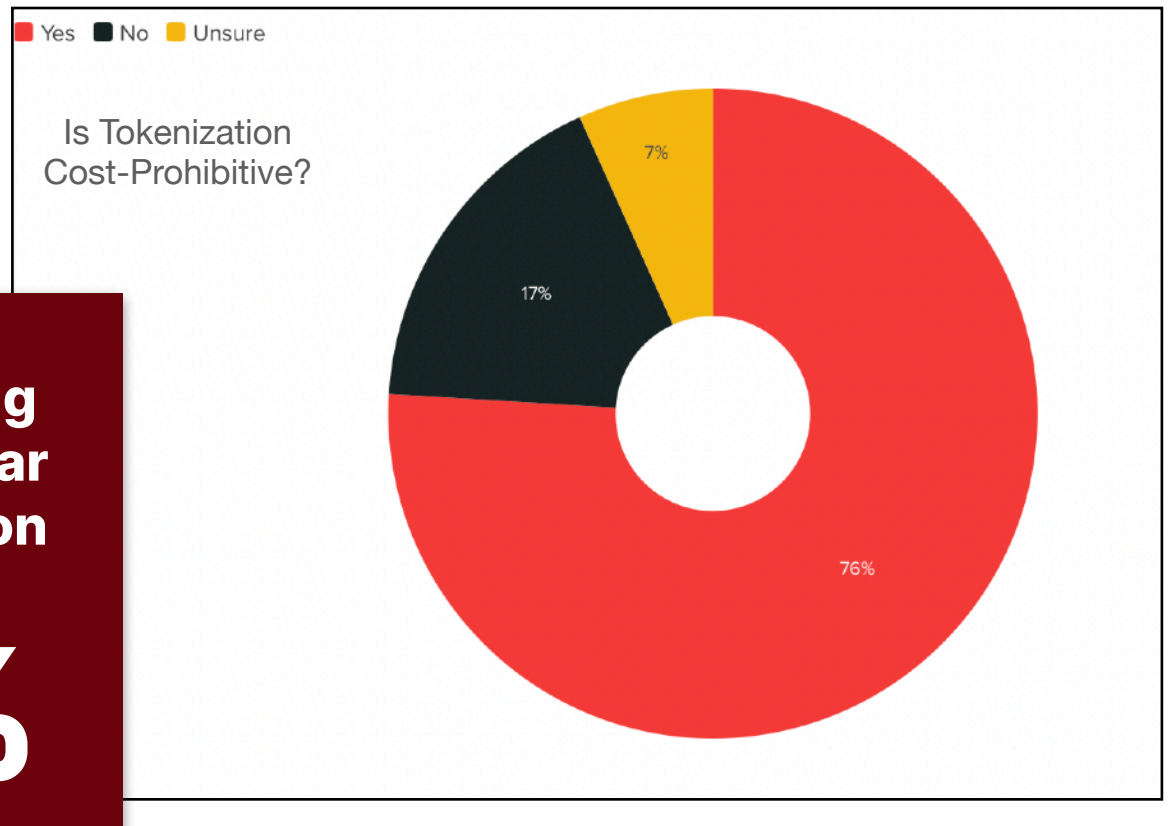
85+%

Enterprises Spend Millions Despite Dismal Data Coverage

Study participants revealed that a majority pay millions for traditional tokenization while still not gaining meaningful data protection coverage. With 36% spending between $1M and $3M and an additional 2% spending over $3M each year, it is no surprise that enterprises are ready for better ROI. The chart below represents % data.



When asked the same question another way, enterprises responded by saying tokenization is cost-prohibitive. This confirmed our anecdotal understanding that while tokenization works well by simply removing data, it fails when the underlying data is truly required, it becomes less and less useful as sensitive data categories increase, and in light of all that, enterprises find the cost of tokenization to be a heavy burden.

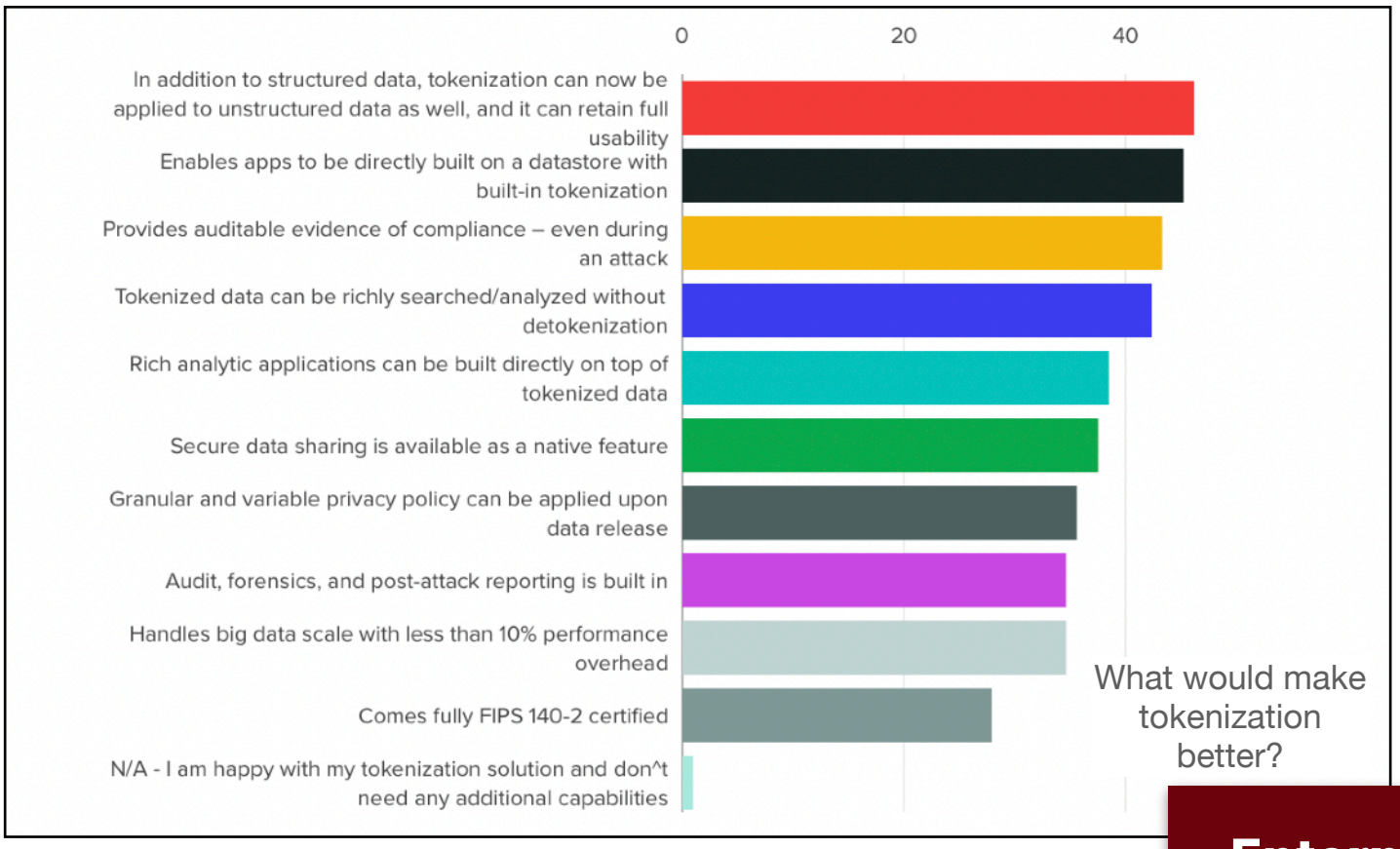


Orgs spending over $1M a year on tokenization

38%

Enterprises Want Better Features and Fewer Tradeoffs

The Study polled participants on what features would improve their tokenization experience. The survey presented modern data protection capabilities that make “Next Gen Tokenization” dramatically different in its coverage, usability and performance. Examine the chart below for features that received the most votes. Notice that only 1% of participants are happy with their current tokenization solution.

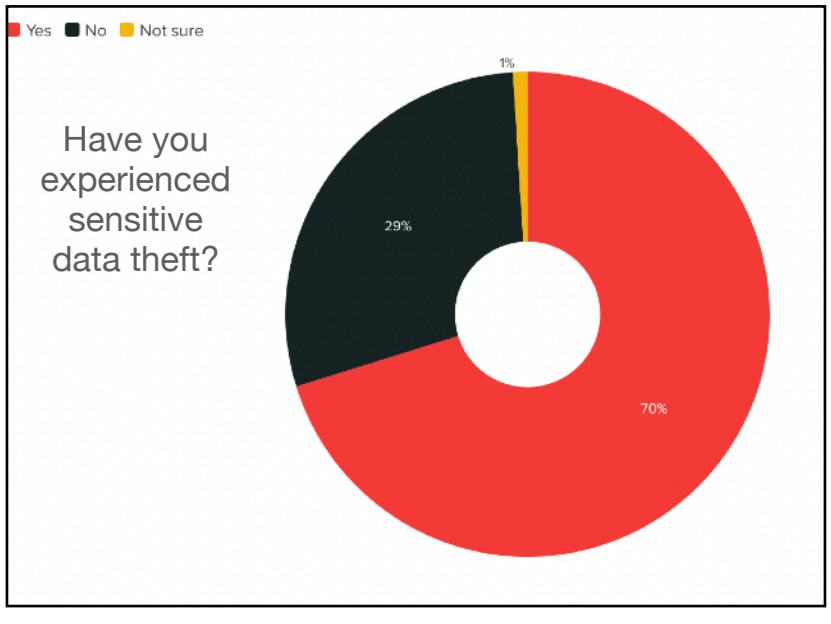


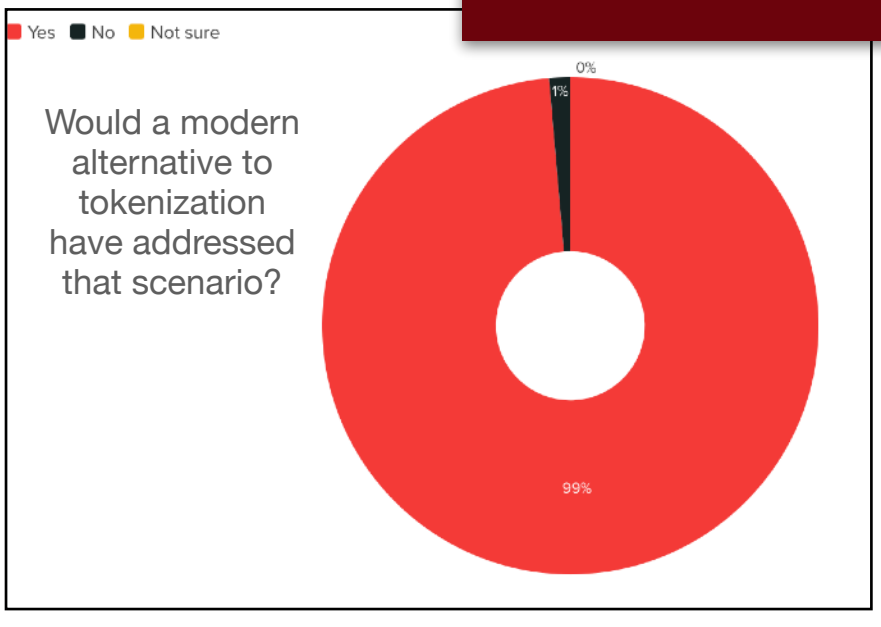
Our final question asked users if they experienced loss of sensitive data despite their investment in tokenization. We also asked whether they believe a more modern solution such as one with features described above would, in their opinion, prevent such compromises in the future.

Answers confirmed our suspicion that as data usage explodes and enterprises move into the era of data driven decision making, we need data protection solutions that deliver strong security without getting in the way of business. Traditional tokenization is not the right answer. Enterprises need to look to “Next Gen” solutions that address traditional limitations and provide superior alternatives. Titaniam offers an answer and we invite you to explore our solution.

Enterprises who believe that a modern solution wold have prevented data compromise

99%

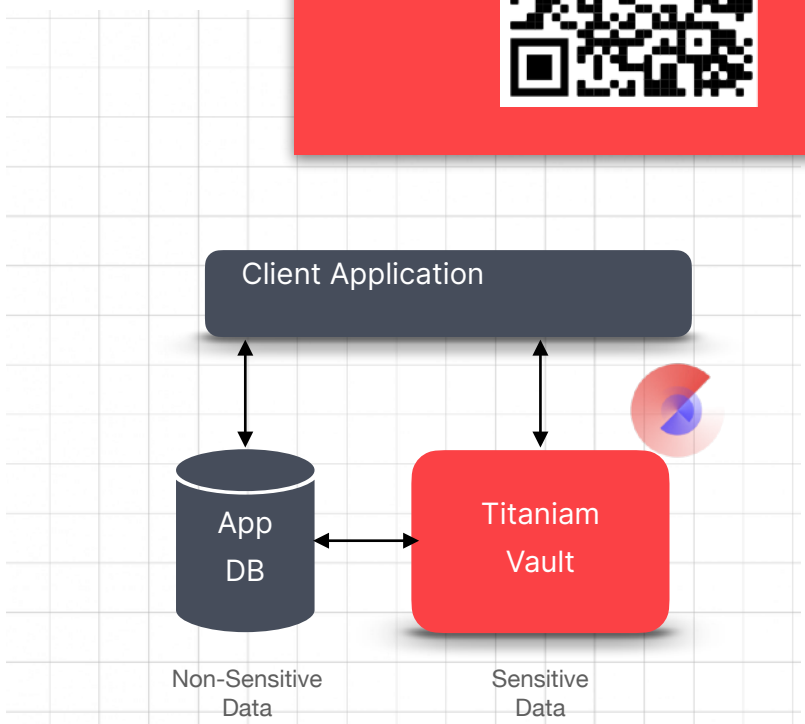




Learn more about Next Gen Tokenization from Titaniam here

Titaniam Secure Analytic Vault

Next Gen Tokenization for Data Intensive Organizations



Gartner
COOL
VENDOR
2022

"Titaniam Provides substantial reduction in risk from ransomware and other data related attacks."

- Gartner

Titaniam Vault is the industry's most advanced vaulted and vaultless tokenization solution delivering all the benefits of tokenization without the severe data usability and performance restrictions that organizations have had to live with in the past. Built for high-performance, petabyte scale, analytic use cases, Titaniam Vault enables full featured search and analytics without any decryption or detokenization. This makes our Vault immune to insider threats as well as all data related cyberattacks including ransomware. In addition to high-performance encryption-in-use, Titaniam Vault includes all nine privacy preserving technologies eliminating the need for separate investments in vaulted and vaultless tokenization, data masking, anonymization, whole and partial redaction, traditional and format-preserving encryption, secure data sharing, and data supply chain security solutions.

Unlike traditional tokenization solutions, Titaniam Vault supports both structured and unstructured data. This means it can enable the traditional structured data use cases but also enable brand new capabilities such as full text search on sensitive documents, confidential tagging and search on images and media, the ability to manipulate encrypted voice and chat logs while ensuring their privacy, and much more. Another key advancement that Titaniam brings is the ability to intake full document context along with individual data items. This allows the Vault to be schema aware and be richly queried directly by client applications. This also allows brand new application development to take place directly on the Vault, thus giving birth to applications that are natively immune to modern cyberattacks and automatically compliant with a myriad of security and privacy regulations.

Titaniam Vault also includes the industry's most advanced key orchestration capabilities with a built-in BYOK/HYOK platform that allows commingled vault data to be encrypted using separate encryption keys controlled by individual data owners inside or outside the organization. In addition. Titaniam Vault interoperates with the rest of TItaniam's suite (Proxy, Plugin, Developer API service, and Studio), allowing it to exchange encrypted data with other Titaniam protected datastores and applications across the enterprise. In this way Titaniam offers unprecedented data security that stands up to the most challenging attacks such as full admin compromise of high value systems and ransomware.

All Titaniam algorithms are NIST CAVP certified and our underlying engine is NIST FIPS 140-2 validated. This allows our customers to enjoy immediate compliance, efficiently apply data privacy controls across the enterprise, and most importantly, it allows Titaniam to provide granular field-level evidence of encryption in the event of an attack. CISOs can rely on Titaniam for visibility on what attackers observed, accessed, and exfiltrated and reporting that can be provided to auditors, regulators, and boards of directors.

Until now Tokenization has been both a symbol of strong security, and at the same time, it has also been one of the most invasive, inconvenient, slow, and expensive security controls in the enterprise. Titaniam is here with a formidable set of capabilities that eliminates all those challenges and provides enterprises with the strength of tokenization without the ugly tradeoffs of the past.

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

Gartner COOL VENDOR 2022

FIPS CERTIFIED 140-2

TAG CYBER 2022 DISTINGUISHED VENDOR

Intellyx DIGITAL INNOVATOR 2022

2022 SINET 16 INNOVATOR

Key Capabilities

Titaniam Vault takes data security and usability to a whole new level compared to traditional tokenization. The table below provides traditional tokenization features in the first few rows of column one. These are highlighted in gray. The rest of the table covers additional capabilities included in Titaniam's Vault. In addition the Vault interoperates with the rest of Titaniam's Suite to keep data protected as it flows through the enterprise.

Data Types & Context

In addition to tokenizing individual data items, Titaniam Vault supports full data context via documents and collections; structured and unstructured data; binaries and tags; and field, index, collections, file, and schema-level security.

Search & Analytics

Supports full-featured search and analytics without detokenization; search through unstructured data; and fuzzy search such as Soundex. It includes full-text search, including prefix, suffix, wildcard, etc.

Data Privacy

Releases data in all nine privacy-preserving formats and enables secure data sharing with partners and suppliers. It supports granular field-level privacy policies and private data sharing across vaults or applications.

Encryption Keys / HYOK

Integrates with industry-leading key vaults for key materials and supports Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) at scale and zero downtime key rotation and re-keying. It is also resilient against compromised master keys

Integration & App Development

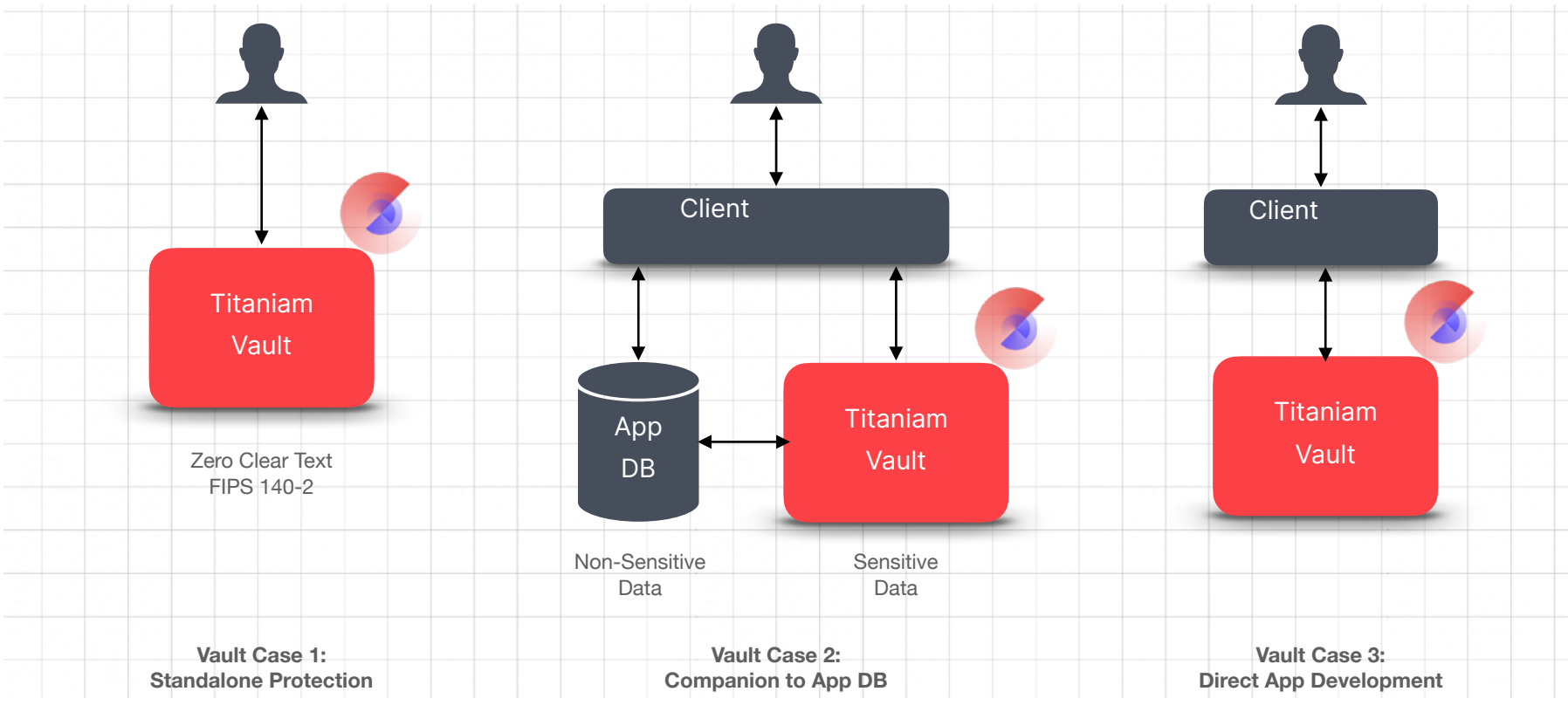
Integrates with existing application role-based access control (RBAC), seamlessly interoperates with other Titaniam models to expand coverage and supports developer-led security with the direct development of new applications on top of the vault.

Certification, Compliance & Post-attack Support

Provides visibility into data observed, accessed, or exfiltrated in an attack and post-attack evidence of compliance and certification. NIST FIPS 140-2 validated with all individual algorithms and key derivation, NIST CAVP certified.

Titaniam Vault Deployment Architectures

Customers can use Titaniam's Vault as a standalone solution to store and analyze valuable data without decryption. The Vault can also be used as a companion data store for existing applications where sensitive data is transparently isolated into the Vault while retaining the primary DB for other types of data. The third and most powerful use of Titaniam's Vault is to build ground up systems that are natively immune to data compromise.



Vault Case 1: Standalone Protection

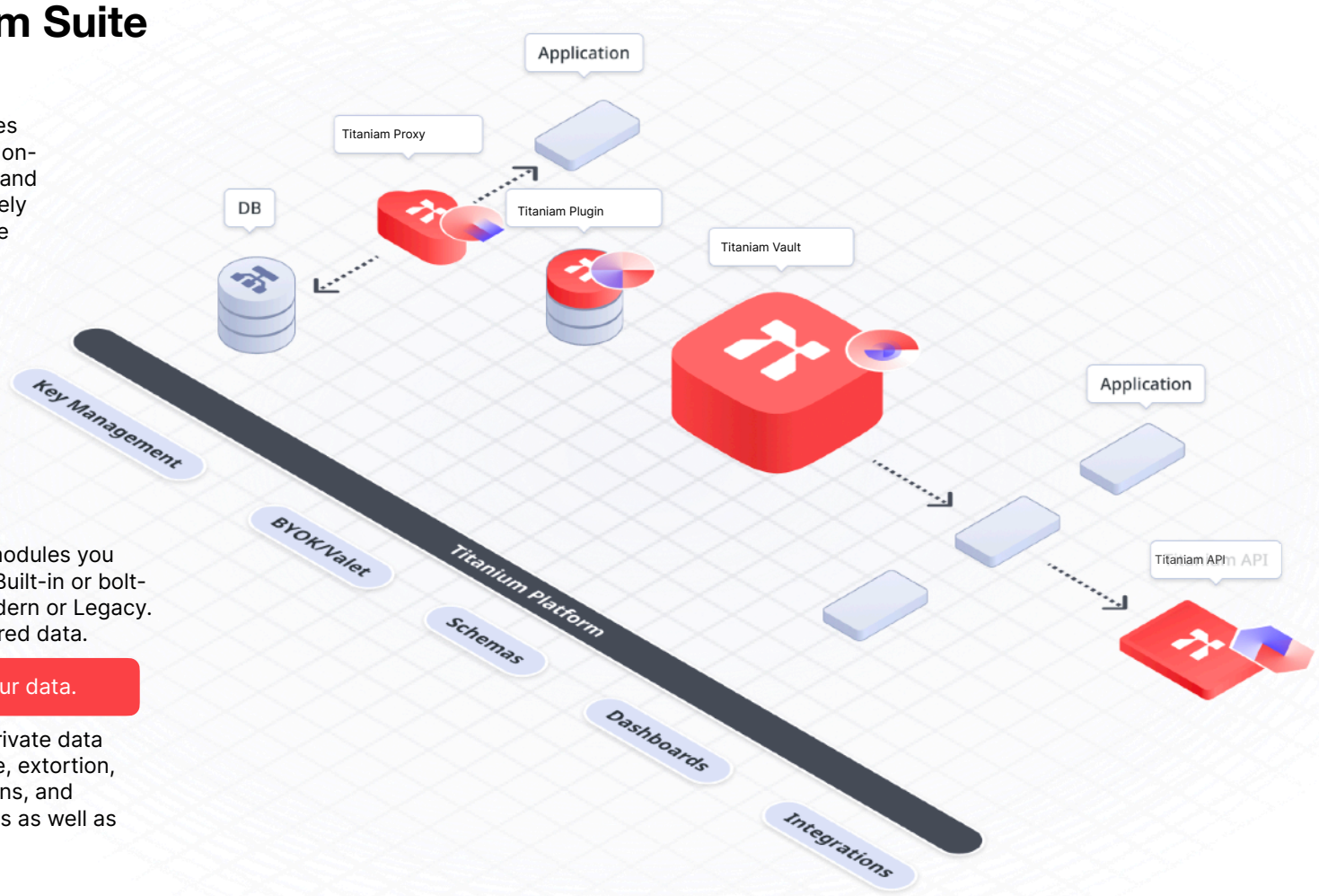
Vault Case 2: Companion to App DB

Vault Case 3: Direct App Development

The Full Titaniam Suite

The overall Titaniam Platform offers five interoperable modules that support a variety of cloud, on-prem, and hybrid architectures and enable secure data to move freely and be safely utilized across the organization.

1. Titaniam Vault
2. Titaniam Plugin
3. Titaniam Proxy
4. Titaniam Translation Service (Developer APIs)
5. Titaniam Studio



Select the building blocks i.e. modules you need to suit your architecture. Built-in or bolt-on. Cloud, Prem, or Hybrid. Modern or Legacy. Protect structured or unstructured data.

Your systems. Your schema. Your data.

Encrypted data processing + private data release. Immune to ransomware, extortion, insider attacks, misconfigurations, and compliant with major regulations as well as frameworks.

Top 5 Reasons to add Titaniam to your Toolbox

#5: Compliance is easier than ever

Titaniam provides FIPS 140-2 validated encryption to sensitive data at all times, including while it is in active use. Titaniam encryption meets with the most strict data protection standards included in all major regulations and frameworks. Titaniam provides granular field-level NIST certificates for all protected data.

#4: Privacy enforcement is a breeze

Titaniam releases data in all nine privacy preserving formats including traditional and format preserving encrypted, partially or fully masked, vaulted or vaultless tokenized, redacted, hashed, and in a searchable encrypted format. Data release can be individually configured, at a granular level, for downstream systems and users.

#3: Cost goes down while coverage goes up

Compared to traditional solutions like tokenization where enterprises pay millions each year to protect a handful of fields while struggling to utilize the data downstream, Titaniam secures as much data as needed while retaining usability. Typical coverage increases are from 5% to 95% while costs come in at 25% relative to tokenization.

#2: Time to value is unbelievably fast

The Titaniam plugin can be fully operationalized within half a day. The Proxy takes a few days. Our translation service and tokenization require integration into the environment but do not require complex de-tokenization and analytics workflows. All products offer standard REST interfaces.

#1: If attacked, Titaniam makes life much easier

In the attack scenario, Titaniam provides visibility into any data that was observed, accessed, or exfiltrated. Further, Titaniam provides granular field-level NIST certificates to show that sensitive data retained encryption during the attack. These can be cross correlated with log data to proceed evidence that can be presented to auditors, regulators, and boards of directors.

This reduces compliance and notification obligations as well as risk of penalty. Most importantly, in this day and age of ransomware, Titaniam minimizes the possibility that victims of ransomware would be extorted by threatening exposure of stolen data.

For more information please contact Titaniam at info@titaniam.io, visit us at titaniam.io, or scan the QR code below

TITANIAM

titaniam.io