TITANIAM

titaniam.io

Ransomware Research Report

STATE OF DATA EXFILTRATION AND EXTORTION 2022

Titaniam's State of Data Exfiltration & Extortion Report for 2022 finds that with attackers winning over 60% of the time, enterprises seeking to defend themselves from ransomware and extortion, need to look beyond the current crop of prevention, detection, and backup solutions.

Independent Research Conducted by CENSUSWIDE

Executive Summary

With ransomware and related extortion fast becoming the biggest cybersecurity risk for both enterprises and governments, organizations are looking to actively bolster their defenses and minimize the impact from such attacks. The last eighteen months have seen hundreds of millions of dollars invested in traditional prevention, detection, and backup solutions, with the hope that these will help mitigate the impact from ransomware attacks.

A look at the news headlines over the last year and all anecdotal evidence, however, suggests otherwise. From everything we can tell by digging into the news as well as talking to impacted organizations, the majority of them have not managed even a moderate level of success against this type of attack. Time and time again, companies with major investments in ransomware detection solutions are successfully brought down. Despite fully operational backup and recovery solutions, these companies find themselves so compromised that their only option ends up being the ransom payment as demanded by attackers.

At Titaniam, we know that prevention, detection and backup are only part of the solution. We believe that the complete solution includes a strong focus on data security so that attackers are unable to gain leverage over victims through stolen data. Unless the data exfiltration vector is addressed, organizations will find themselves in a losing position despite all their other security investments. Titaniam has built a solution for this. We offer a cutting edge data security platform that combines traditional data protection techniques with high-performance encryption-in-use that effectively shuts down the large scale data exfiltration vector that is part and parcel of the modern ransomware attack.

We believe that the key to sharing our value proposition with CISOs and Boards is to base it on a strong data driven foundation. For this reason, we requested an independent research organization, CENSUSWIDE, to conduct a study. Our study aimed to gather raw data on ransomware attacks, data exfiltration, extortion, ransom payments, prior investments in security, as well as forward looking budget priorities. Respondents included 107 Security Professionals in a variety of enterprises across the United States.

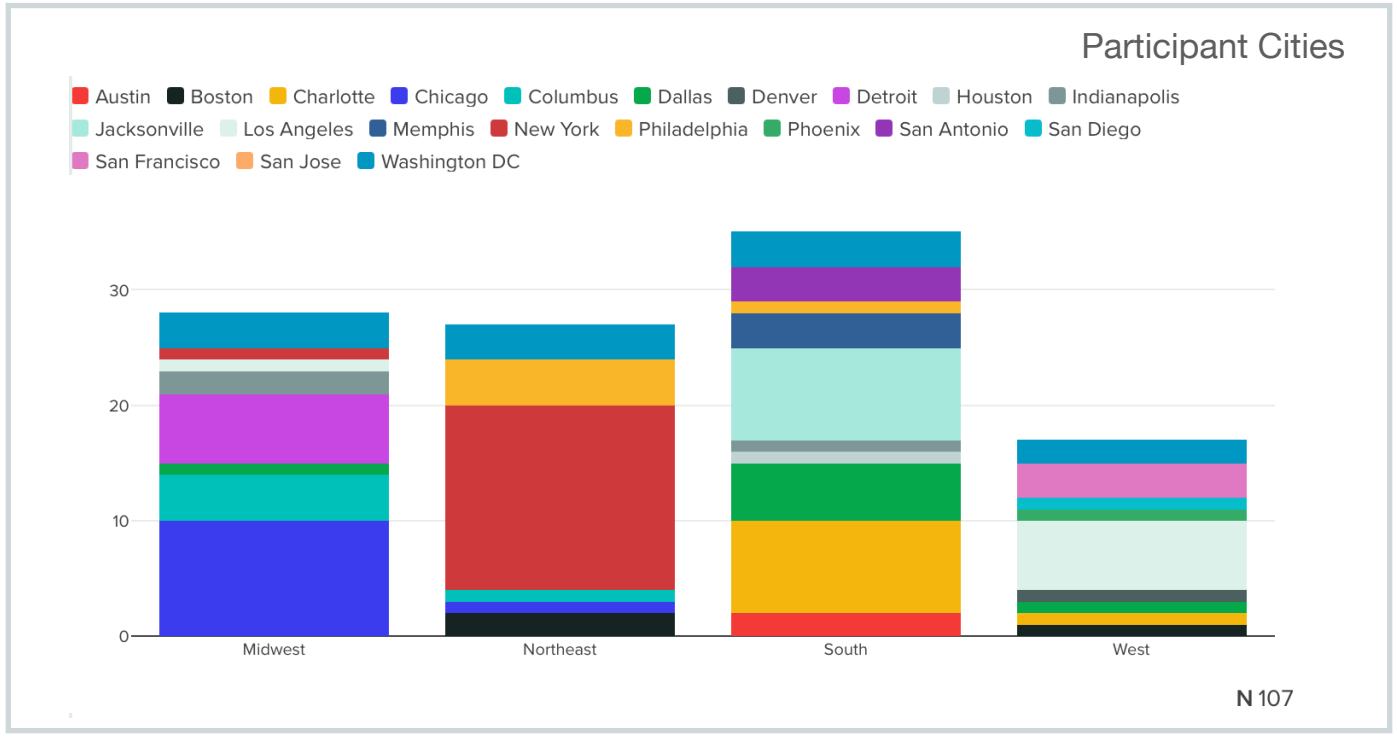
- Over 70% of organizations surveyed were attacked within the last 5 years
- 68% of those attacked had their data exfiltrated, and of those, 60% were subsequently extorted. Exfiltration rates are up 106% relative to 5 yrs ago.
- While over 75% of surveyed organizations had all three major categories of ransomware protection in place i.e. prevention/detection, backup/recovery, as well as traditional data protection, the majority of those attacked, 60%, were forced to give in to ransom demands
- Over 99% of study participants are looking for better data protection tools to overcome ransomware and extortion

We also gathered data on security investments and budgets. Ultimately, the data showed that strong data security that protects against exfiltration and extortion is an enormous and critical need in the fight against ransomware. 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

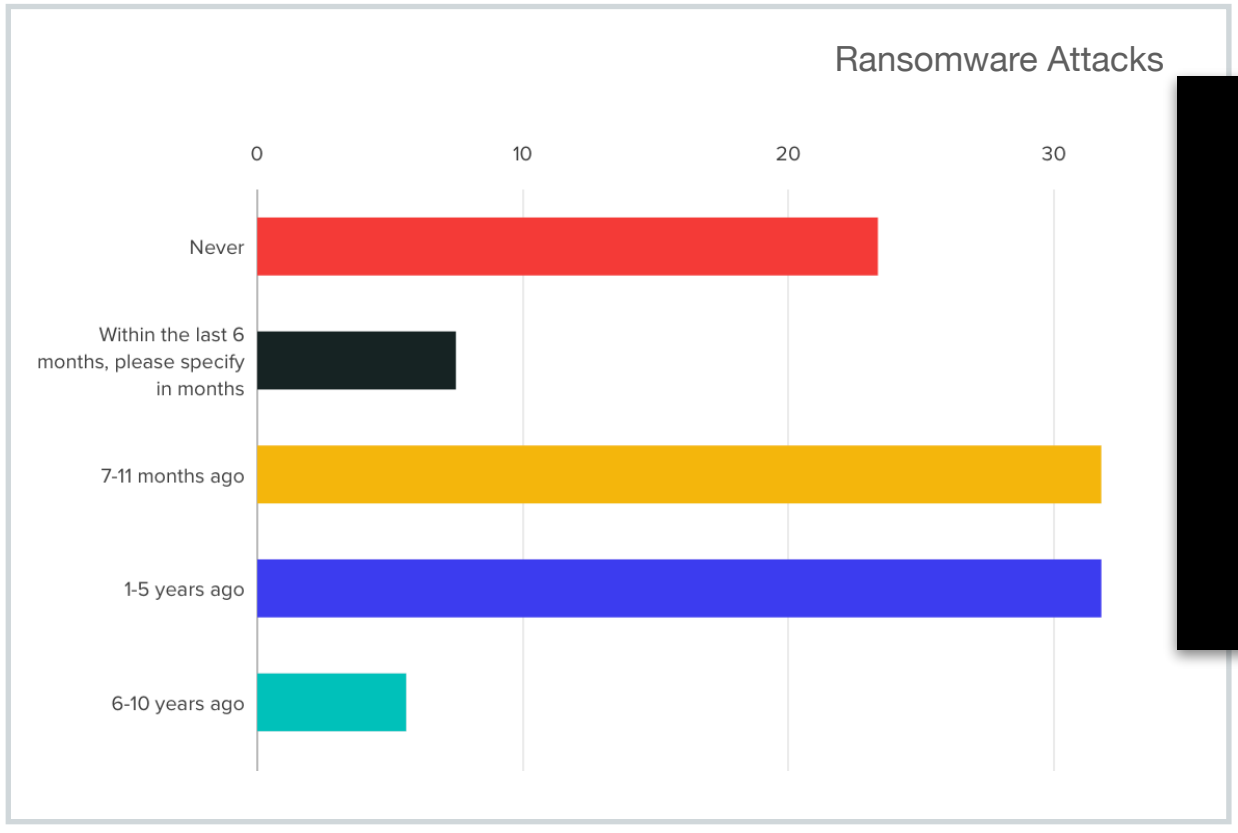
Summary of Study Participants

Titaniam's State of Data Exfiltration and Extortion Study included 107 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 geographical spread of our participants.



High Incidence of Ransomware Attacks

The study found that over 71% of respondents had experienced a ransomware attack in the last 5 years and over almost 40% in the last 12 months. This confirmed other research studies as well as our own anecdotal understanding of the extent of the ransomware problem. The chart below shows % out of a total of 107 responses.

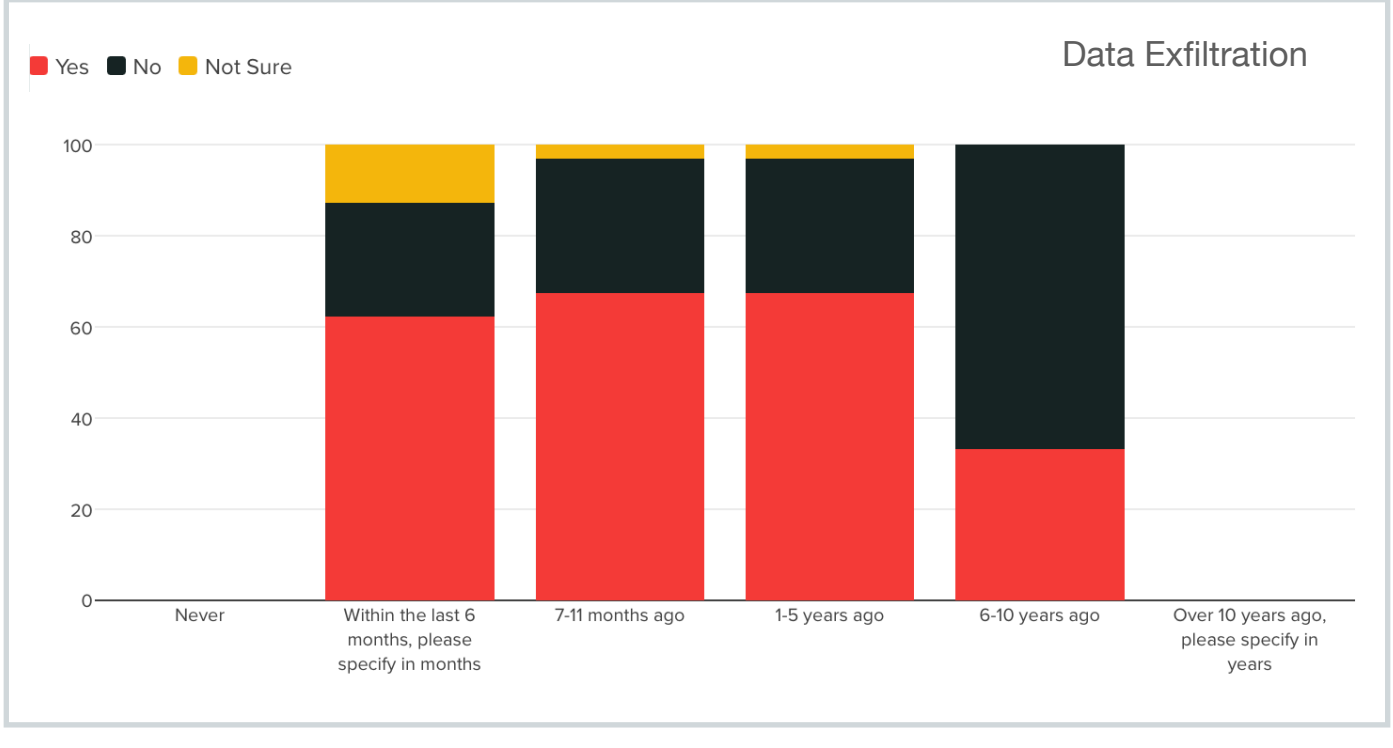


Orgs attacked in the last 12 months

40%

Majority of Attacks Involve Data Exfiltration

With the red bars in the chart below depicting the percentage of companies that had their data exfiltrated as part of the ransomware attack, it is clear that the nature of attacks has changed to include data exfiltration in a majority of the attacks. The data shows that while prior to 5 years ago, only 33% of attacks included data exfiltration, in recent years this number has grown to 68%.



Ransomware Attacks Have Evolved From 2-Stage to 3-Stage Attacks

This data above shows very clearly that ransomware attacks have gone from primarily two-stage attacks to primarily three-stage attacks. The original two stage attacks involved:

Stage 1: Infiltration and lateral movement to identify high value services, resources/ data
Stage 2: Encryption of valuable services, resources, and data with the intent to extort

The original two-stage attack was well addressed by a combination of prevention/ detection solutions and backup/recovery tools. If attackers were successful with Stage 2, organizations could recover from backup and ignore ransom demands.

Modern ransomware attacks are three-stage attacks with data exfiltration being the middle stage that provides unbeatable leverage for attackers. Data stolen in Stage 2 is used to extort victims even if they stand up impacted services and data from backup.

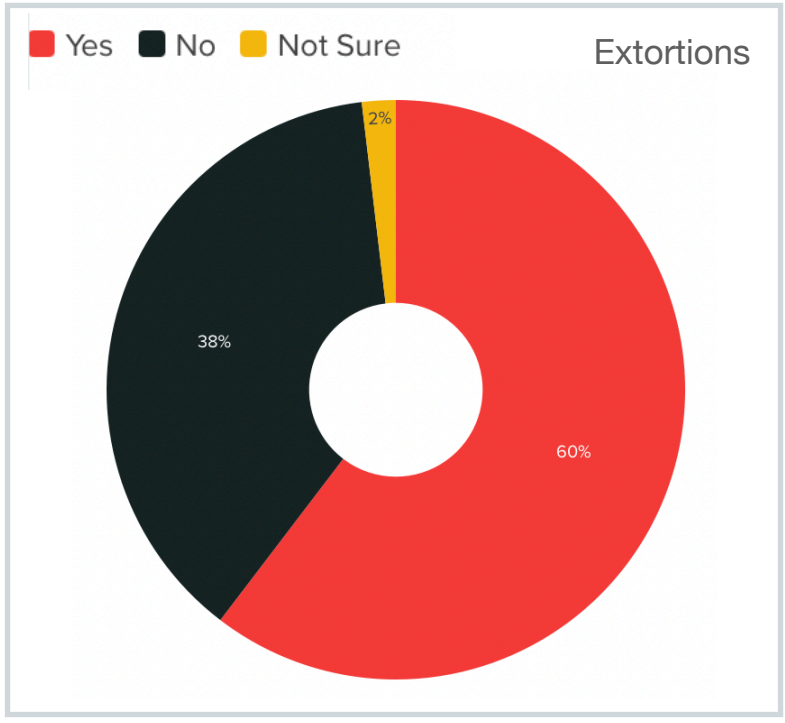
Stage 1: Infiltration and lateral movement to identify high value services, resources/ data
Stage 2: Exfiltration of data with the intent to extort victims, customers, and partners
Stage 3: Encryption of valuable services, resources, and data with the intent to extort

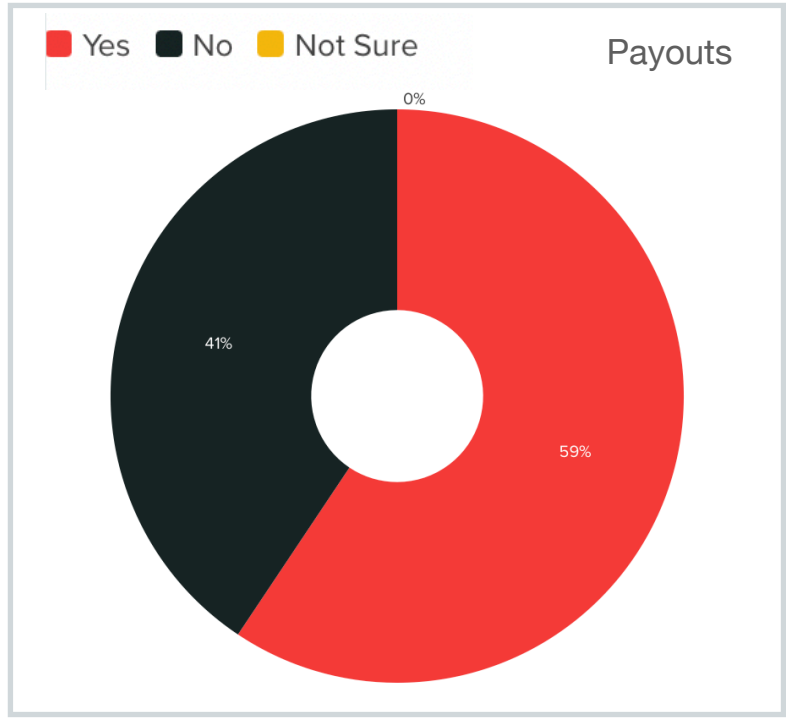
Increase in Data Exfiltration relative to 5 years ago

106%

Stolen Data is used to Extort Victims Who are Forced to Pay

The study found that in the majority of cases where data was exfiltrated as part of the ransomware attack (60%), attackers then proceeded to extort the victims. This is consistent with what we learned from other studies as well as anecdotal conversations from ransomware victims. The data also shows that there are simply not enough protections in place from a data security point of view. A majority of those extorted (59%) found that the stolen data gave attackers unbeatable leverage and they ended up giving in to the ransomware demands presented to them.

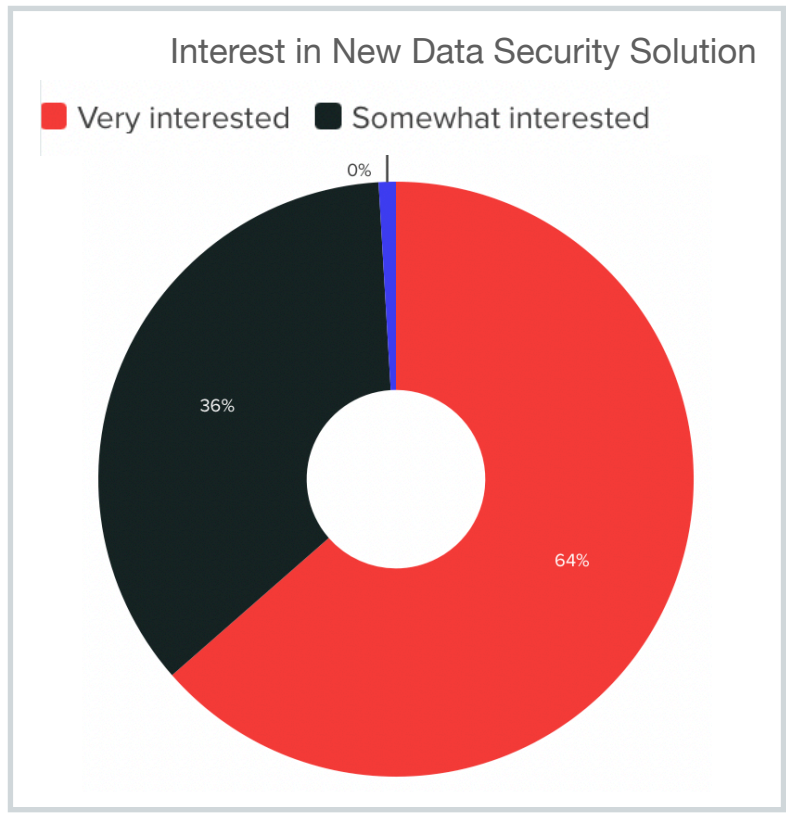




Demand for a Platform that Secures Data from Ransomware is Very High

The study also found that data was exposed and lost by means other than ransomware related data exfiltration. 47% of respondents across the board reported data exposure via other means.

Regardless of how data was lost, over 99% of all participants expressed an interest in a data security platform that eliminates the loss of valuable data with 64% being very interested.

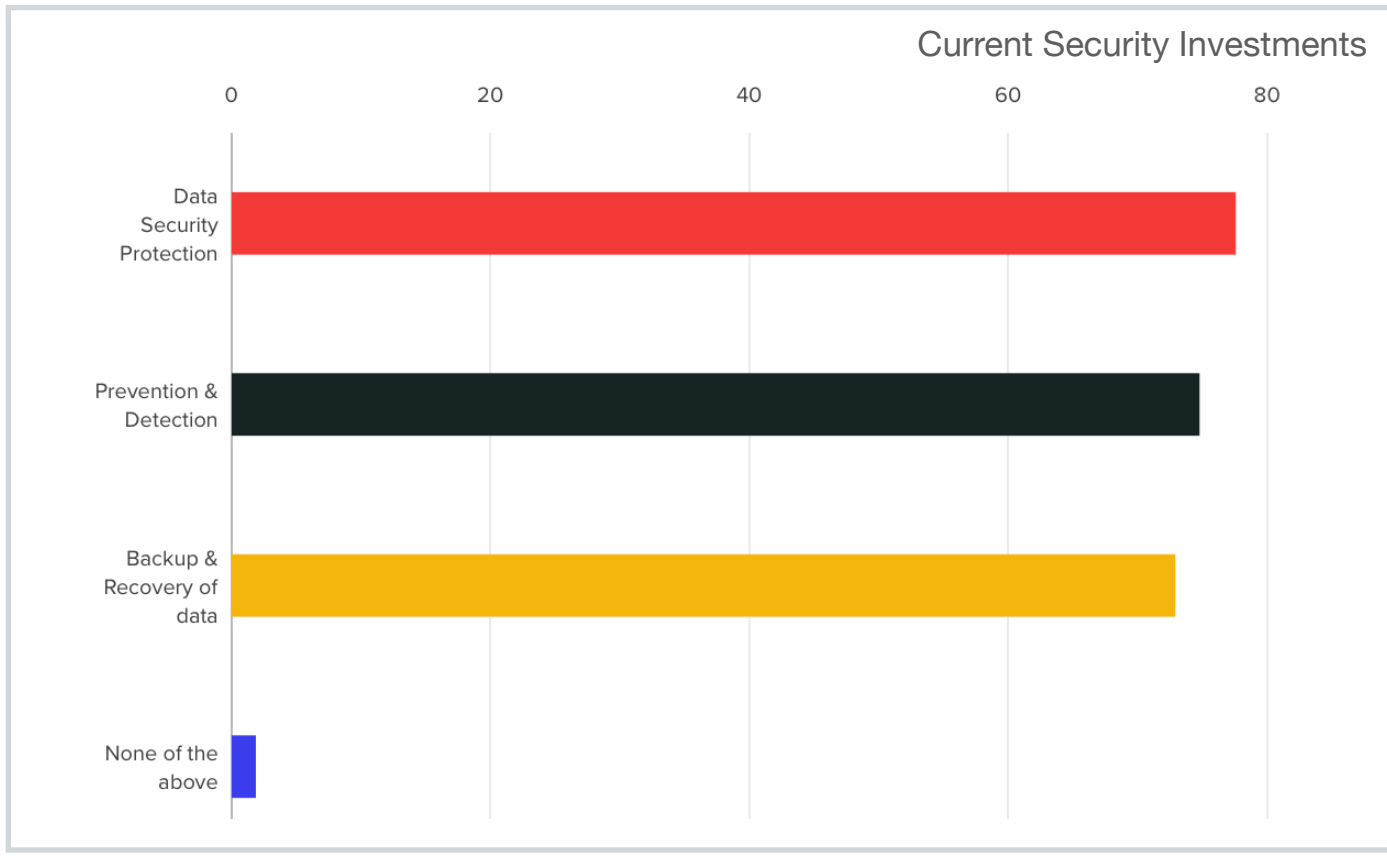


Percentage of organizations looking for data security that address the ransomware challenge

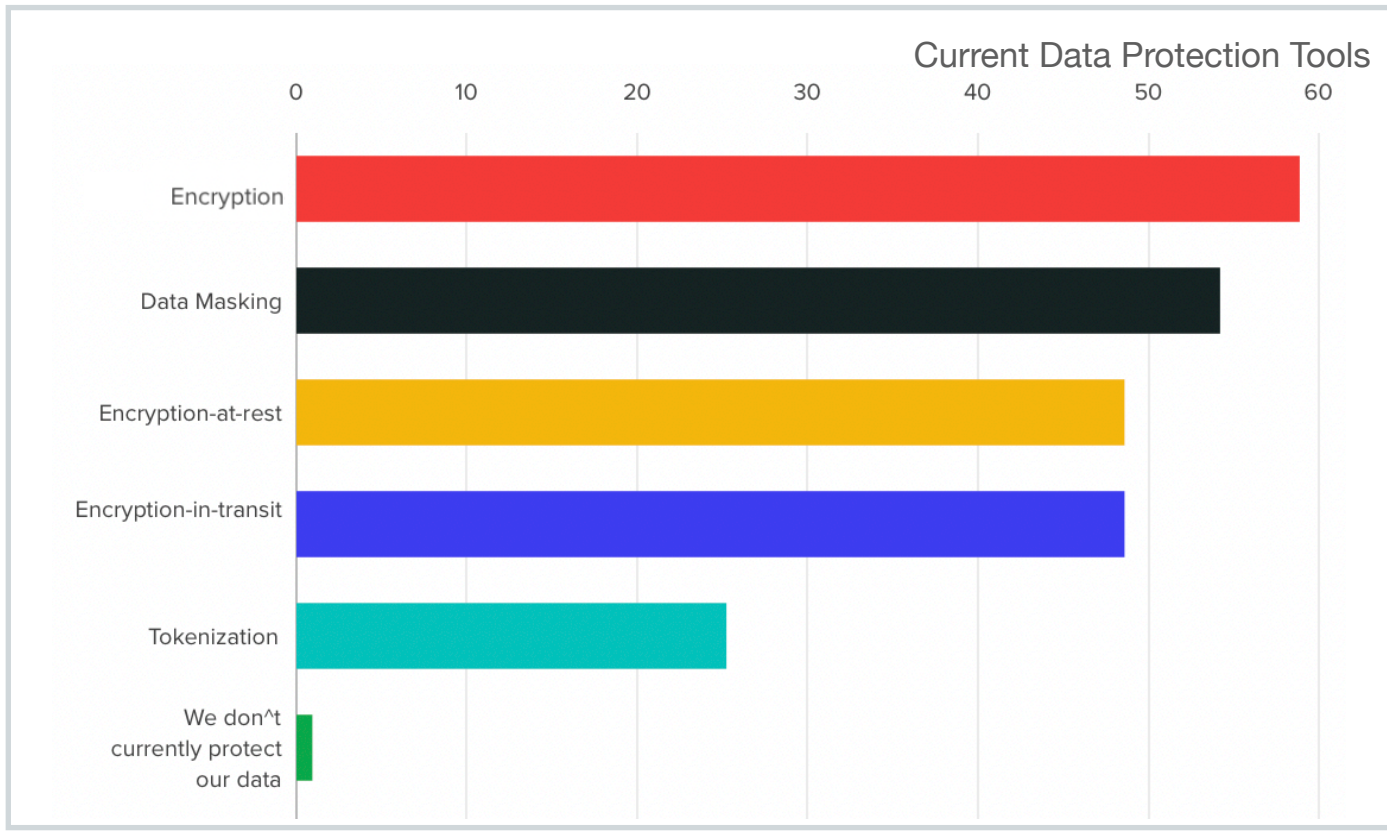
99+%

Current Security Solutions in Use

Study participants revealed strong investments in traditional technologies and we found an even spread between solution categories such as Prevention/Detection Solutions, Backup/Recovery Solutions, and Traditional Data Protection Solutions. See the chart below for the data that was gathered.

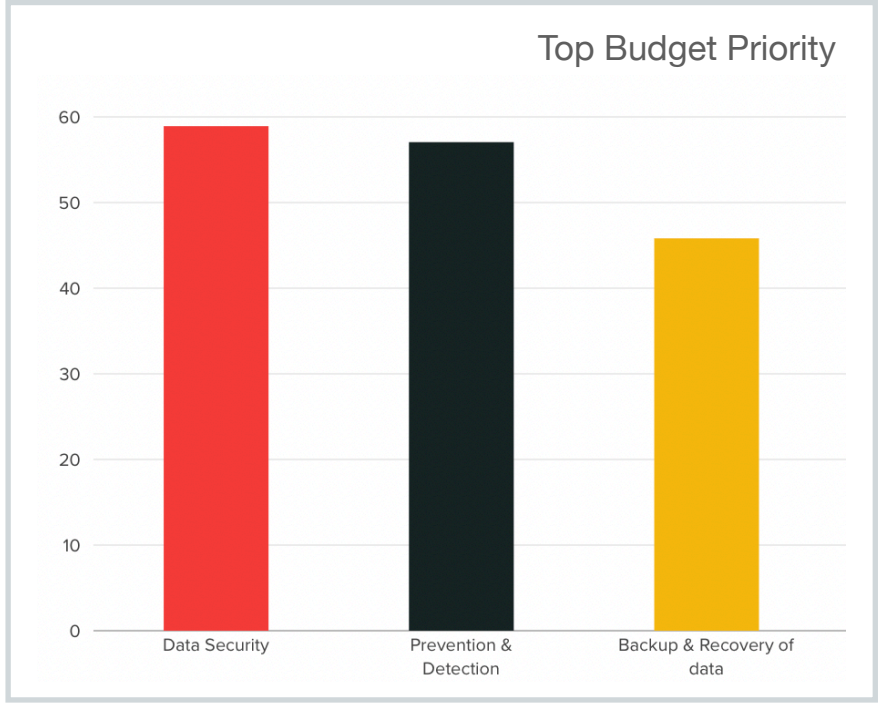


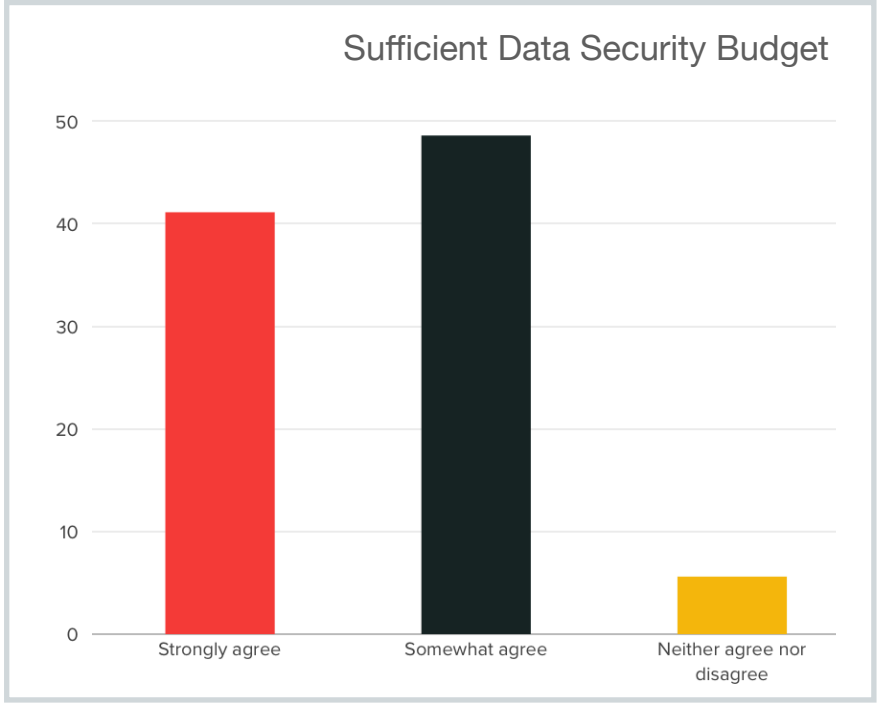
Within Data Protection, the study found that participants were utilizing all popular traditional data protection techniques. While their presence did not result in a good success rate against ransomware and data related extortion, having this data leads us to conclude that enterprises continue to make strong efforts to protect themselves and as they are introduced and adopt more effective solutions, they will see improved defense.



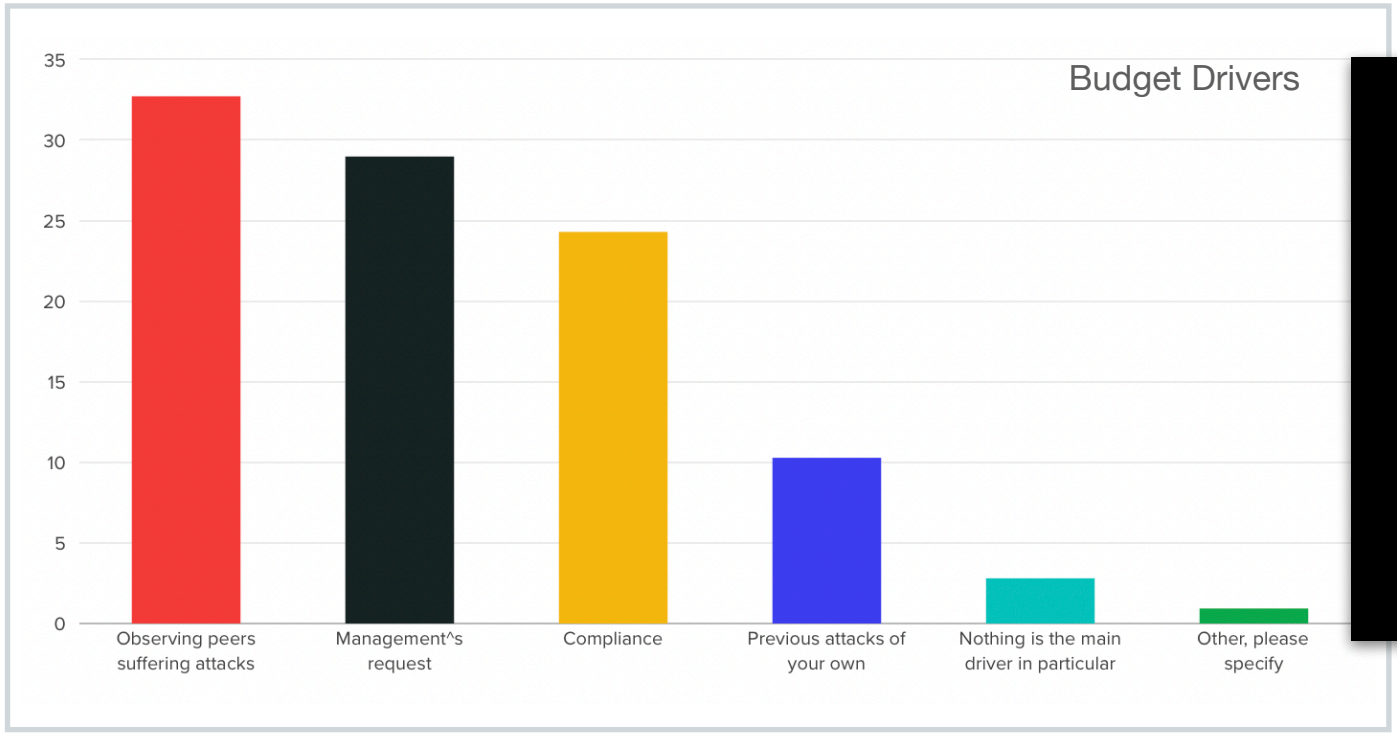
Data Security Budgets

The Study found very strong budgets for data security. Data Security was ranked as the top budget priority for 59% of responders compared to Prevention/Detection (56%) and Backup/Recovery tools at (47%). When asked whether they believed they had sufficient Data Security budget, a majority of respondents (90%) answered in the affirmative with 41% agreeing very strongly and 49% somewhat agreeing.





Our final question in the study asked participants to share what their primary data security budget drivers were and the answers were in line with our anecdotal experiences. The biggest factor driving purchase appears to be witnessing peers suffer ransomware and extortion attacks. This is followed by management requests, compliance considerations, and past ransomware attacks within their own organizations. Based on this data we should expect to see a lot more investment in Data Security Platforms that address the specific exfiltration and extortion challenges presented by modern ransomware attacks.



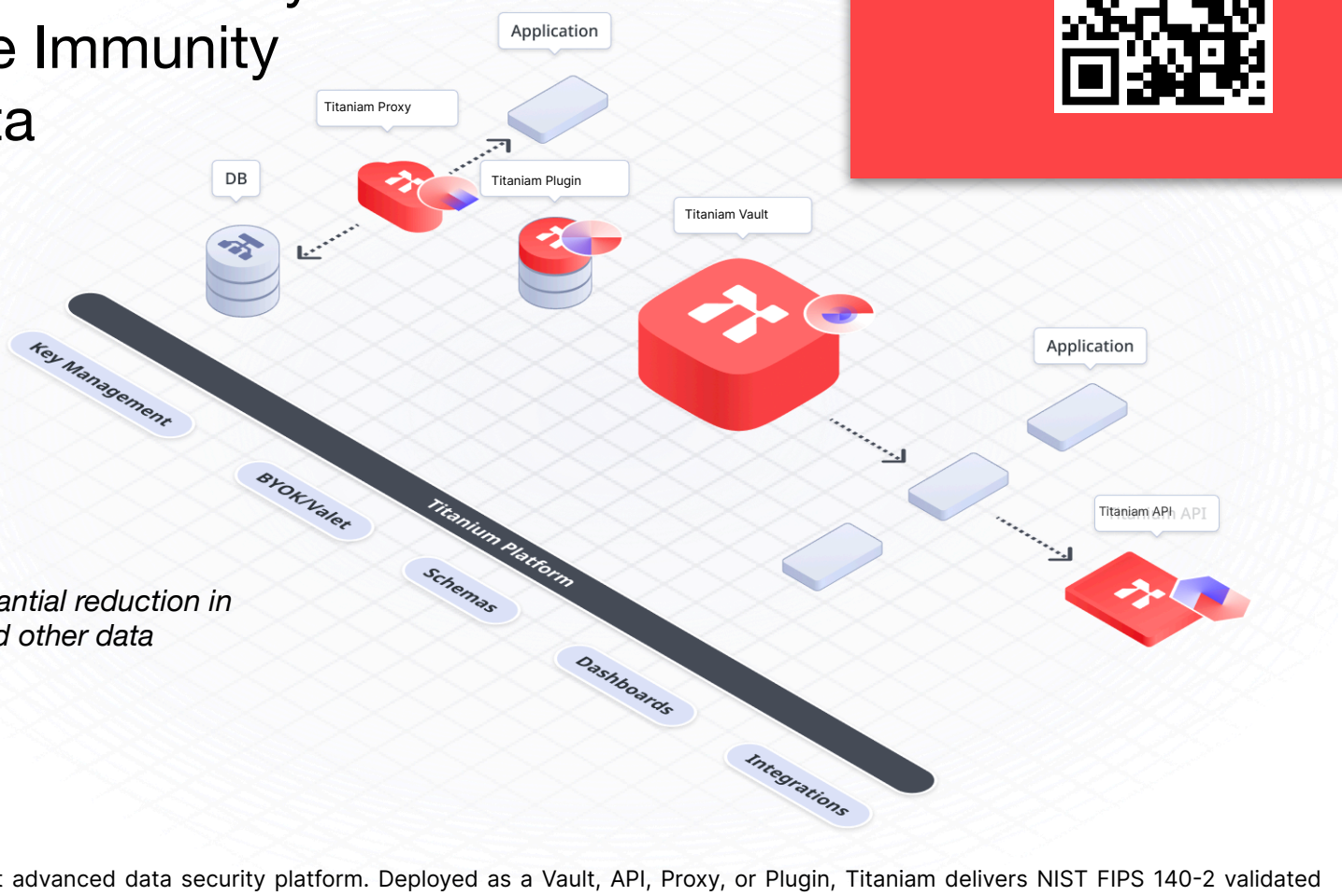
How Often Does a Peer Attack Result in New Security Budget

33%

Learn more about Titaniam here

About Titaniam

Titaniam's Data Security Platform Builds Ransomware Immunity into your data



Gartner
COOL VENDOR 2022

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

- Gartner

Titaniam is the industry's most advanced data security platform. Deployed as a Vault, API, Proxy, or Plugin, Titaniam delivers NIST FIPS 140-2 validated encryption-in-use at all times, without loss of functionality. In addition to high-performance encryption-in-use, Titaniam provides all nine privacy-preserving formats thus eliminating the need for additional solutions for tokenization, masking, anonymization, and traditional encryption. Enterprises rely on Titaniam for day-to-day privacy and compliance as well as strong data security during ransomware or insider attacks.

Top Use Cases

SaaS Data Security
For SaaS providers who do not want to risk compromising valuable customer data

Regulated Enterprise
For enterprises who need to tokenize without losing the ability to analyze protected data

Enterprise Search Data
For encrypting Elasticsearch or OpenSearch data while retaining full featured search

Product Data Security
For enterprises who want to build products that are natively immune to data compromise

Object Store Data
For protecting valuable structured or substructures data in S3, AzureBlob, or GCS

BYOK/HYOK for SaaS
For SaaS companies to let customers hold their own keys to limit data exposure and liability

Titaniam Product Suite

Select the building blocks i.e. products 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.

Protected Systems	Titaniam Studio	Titaniam Vault	Titaniam Plugin	Titaniam Proxy	Translation Service
Cloud/On-Prem/Hybrid	O	O	O	O	O
Search Engines	O		O		O
Object Stores	O			O	
SQL and NoSQL Databases (both OLTP & DWH usages)	O	O			
Cloud Datawarehouse	O	O			
File Systems and Distributed File Systems	O				O
Other File Stores	O				O
Applications with Extensibility	O		O		O
Applications with Object Store Backend	O			O	
Applications with Elasticsearch/ Opensearch Backend	O		O		O

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 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 provide 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.

Next Gen Cybersecurity Startup of the Year

Most Innovative Ransomware Data Security Solution

Hot Company Zero Trust Application Protection

Best Product Encryption

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

TITANIAM

titaniam.io