EMA
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Data Security in a Multi-Cloud World

EMA Research Report

By Christopher M. Steffen, CISSP, CISA
Research Director, Information Security, Risk and Compliance Management

Table of Contents

Introduction

Securing and protecting data is at the center of the modern enterprise security plan. There are many considerations for enterprises that aim to move critical workloads and data stores to the cloud, and understanding how business-critical data will be accessed and stored is a paramount concern. In addition, GDPR and CCPA regulators are starting to issue violations, and as the various courts issue verdicts, the scope of how data privacy is regulated (and the impacts that will have on organizations big and small) will add complexity to a crowded regulatory framework.

Organizations are turning to security vendors to understand these regulations and gain control of their data estates using tools and services from the security ecosystem. The enterprise is also looking to experienced vendors with a proven track record with zero trust implementations that are able to address and assist with all aspects of a zero trust project, instead of one-off specific features.

This report addresses the importance of data security and data privacy programs, from how enterprises are evaluating and using tools for data security and the cloud, to the importance of zero trust vendors and the solutions they provide. As enterprises look to vendors to provide expertise and guidance for addressing data security and privacy regulations, they are also looking to use data privacy as a differentiator in their respective verticals.

In this exclusive research study conducted for IBM, Enterprise Management Associates polled 204 individuals from organizations of 500 employees or more from over ten different industry verticals. Nearly all (95.1%) indicated data security as a critical or very important factor in their organizations, and 74% have integrated data security and privacy as part of their organization's overall security strategy.

Key Findings

Security Trends

64% of organizations report that two or more of their tools are at least somewhat redundant

75% of organizations currently use three or more tools to secure hybrid multi-cloud environments

36% of organizations say security teams sometimes, rarely, or never work with other technical teams for problem resolution

82% of organizations are currently evaluating data privacy solutions

74% of organizations view data privacy as a major differentiator in the marketplace

94% of organizations state that data privacy is the primary driver behind their zero trust program

73% of organizations are investigating or planning a zero trust project

94% of organizations feel it is moderately or very important that they work with established zero trust leaders

96% of organizations prefer to work with a zero trust vendor that offers a comprehensive portfolio of security solutions

In this survey, we asked several open-ended questions, including how the survey respondent would describe their data security and privacy vision. Here are a few of the responses (edited for grammar, etc).

For our data security, we silo everything: only very specific people with the correct permissions and business uses are allowed to touch it. Having artificial intelligence continually verify the data integrity is also a critical component.

Data privacy is the most important thing in my organization. It is very challenging for us. Data protection is the first priority of my organization.

We are working to address compliance with privacy mandates, building trust with our stakeholders, and growing our business with a holistic, adaptive approach to data privacy based on zero trust principles and proven data privacy protection.

Data security has become a lot complicated since business embraced cloud infrastructure and increasing the volumes at which data is collected and shared across hybrid multi cloud environment. Data privacy is an important part of our business strategy that can boost our brand.

Data privacy and discreteness is the cornerstone of our industry. We need to provide our clients with the most responsive data management tools, while keeping their data safe from attack. We are constantly investigating ways to expand our data protection offerings to provide the data privacy we promise as we integrate the latest technologies and cloud offerings.

Data privacy is critical to our company as we need to maintain compliance with all the regulations, so it is of the utmost importance to have our data extremely secured and private. Up until recently, this need for privacy was restricting cloud usage in any form, but recently regulations were relaxed in that regard; for the most part non-cloud solutions is still the norm, however.

Security Trends

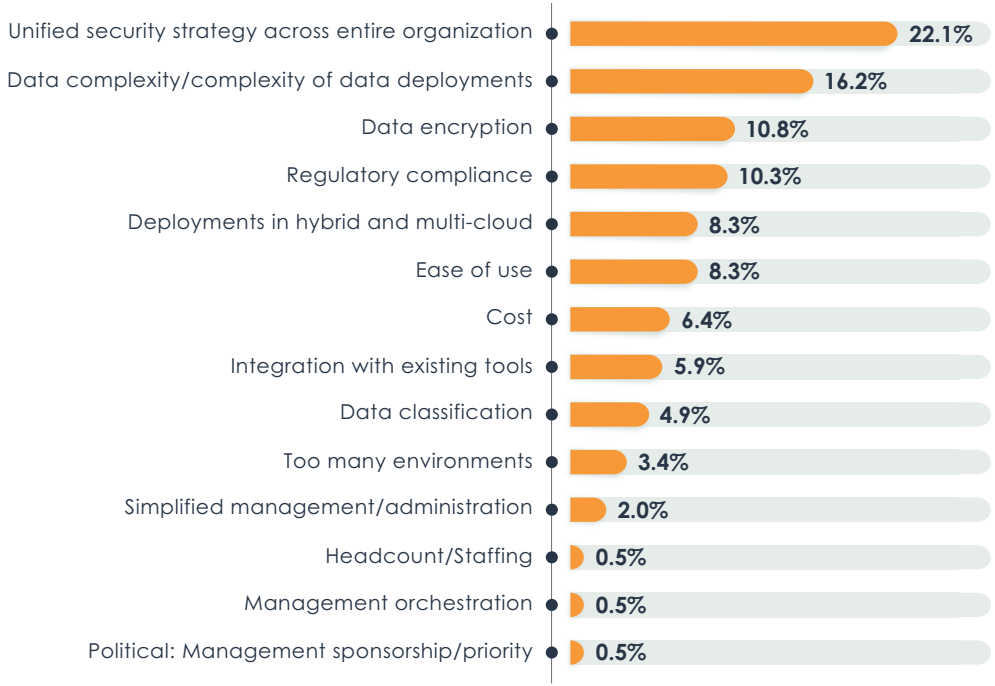
Analysis:

Data security is a factor that impacts nearly every division of an organization. The two challenges outlined in this survey showed that a unified security strategy (that encompasses data security), along with the complex nature of data and where it is deployed, ranked as the greatest challenges, followed by encryption of data, compliance requirements, and data deployed into cloud environments.

Commentary:

Integrating data security as the primary (or a major) priority in an organization's overall security strategy is critical. So many organizations have regional or divisional plans for security operations, making protecting the organization's critical data even more difficult. When combined with differing classification standards and struggles for data ownership and custody, it becomes obvious why a unified security strategy ranked as the greatest data security challenge.

What is your organization's greatest data security problem/challenge?



Analysis:

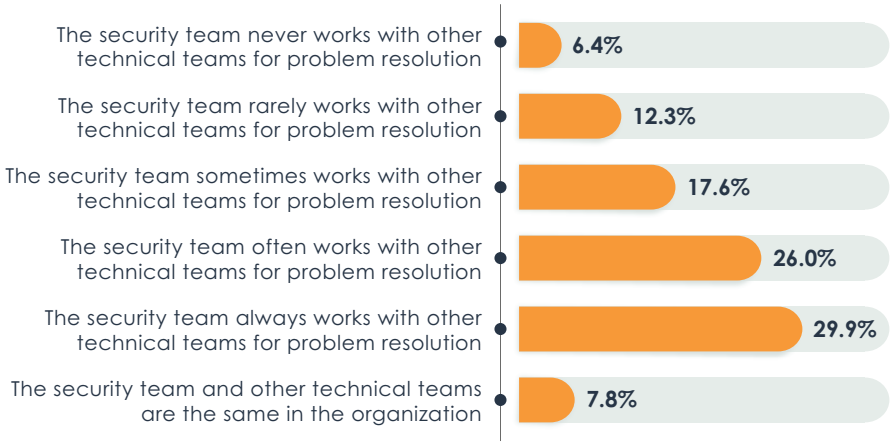
Many organizations have their security team operate as a separate entity from the rest of the technical and operations organizations, and appear to prefer that segregation. Forty-four percent indicated that they would prefer to keep the security organization siloed from other parts of the organization. Fifty-six percent responded that the security team works with the other technical teams for problem resolution, while 18% indicated that they rarely or never work with those teams when problems arise.

Commentary:

Plenty of organizations prefer the independence that a segregated security team provides for problem resolution, but over half have tried to break down the barriers that prevent their technical and operations teams from working together. When a security incident occurs, it is critical that the security team has the ability to resolve that issue as quickly as possible. More often than not, it requires working with the various divisions of the organization to understand the exposure and remediate the situation without causing additional harm or productivity loss.

Has your organization considered breaking down silos between security and technical teams?

Does your security team operate with other technical silos within your organization?



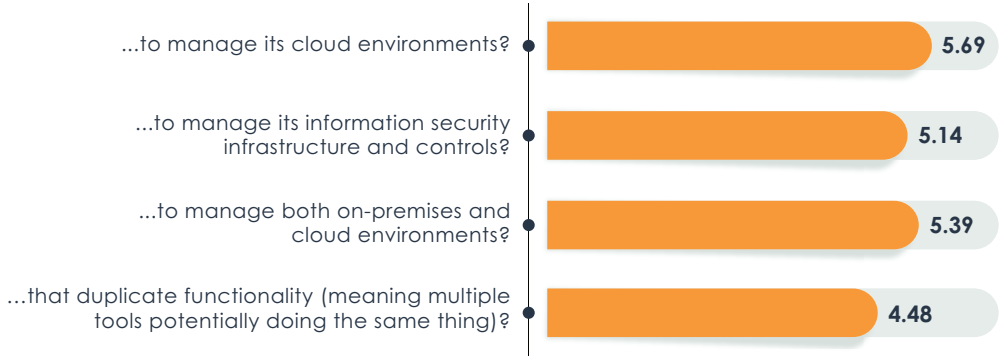
Analysis:

One of the constant concerns organizations have is the continual increases in what is often called "tool sprawl," which is the addition of management and administrative tools for every application, workload, and scenario. In this survey, organizations are using a little more than five different tools to manage security solutions and cloud environments, and over three-quarters of those surveyed (77%) indicated the importance of a tool to work in multiple environments.

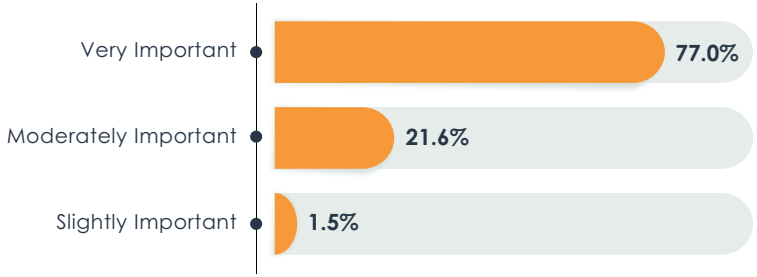
Commentary:

Many security and cloud vendors believe that their tools are differentiated and critical for a business to function. There is no question that organizations need to have tools to manage their systems and their security, but having niche tools that either provide a single function (no matter how well it works) or that do not integrate with existing infrastructure tools is not desirable. Organizations have come to realize that having more tools equates to additional expenses and misallocations of limited resources. Vendors that provide complete solutions and dashboards (with open integrations) will continue to have a significant advantage.

How many tools is your organization using…



How important is it to your organization that a data security tool can work across on-premises and cloud environments?



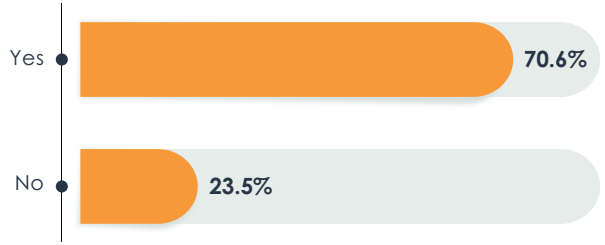
Analysis:

Nearly every organization is subject to compliance-related controls and requirements, but some have used this mandatory requirement as a method to differentiate themselves from competitors in the same vertical or space. Over 70% of those surveyed have created marketing campaigns and programs that highlight their adherence to compliance and regulatory standards as an advantage.

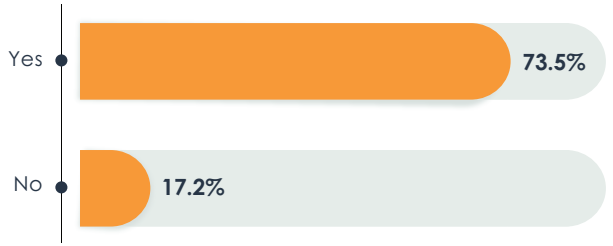
Commentary:

Compliance regulations will continue to increase, and data privacy/security is the latest to receive significant attention. Those organizations with a comprehensive data privacy program—one that can demonstrate compliance with GDPR and CCPA regulations—are using that to get a leg up on their direct competition, who may not have the maturity to enact such a program. Eventually, data privacy will be a "table stakes" requirement, much like many other regulatory frameworks have become. While the standards and requirements are new and evolving, those on the cutting edge of demonstrating compliance have an advantage over their peers.

Has your organization used or is it looking to use regulatory compliance programs as a competitive differentiator?



If your organization were to implement a significant data privacy program, do you believe that it could be a competitive differentiator in your space?



Zero Trust

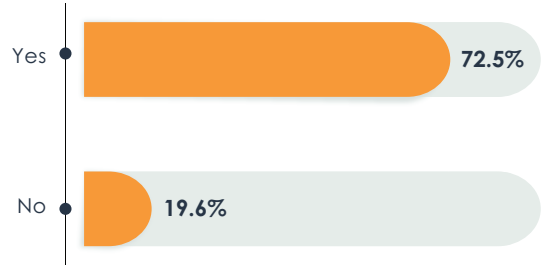
Analysis:

More than likely, most organizations have heard about the security strategy called zero trust and have looked at their organizations to determine if they would benefit from a zero trust project. In this survey, 72% have started the process of a zero trust project, and nearly all of them (94%) identify that data privacy/security is a primary motivation to implement zero trust in their organization.

Commentary:

Zero trust is not a product or a single solution. It's an approach. Successfully completing a zero trust project takes time and thoughtful investment of company resources and priorities. Organizations are right to examine zero trust. Data privacy should be a primary— if not THE primary—motivation of a zero trust infrastructure, since protecting the organization's critical data is paramount.

Is your organization investigating/planning a zero trust project?



Is data privacy a primary driver for your zero trust project?

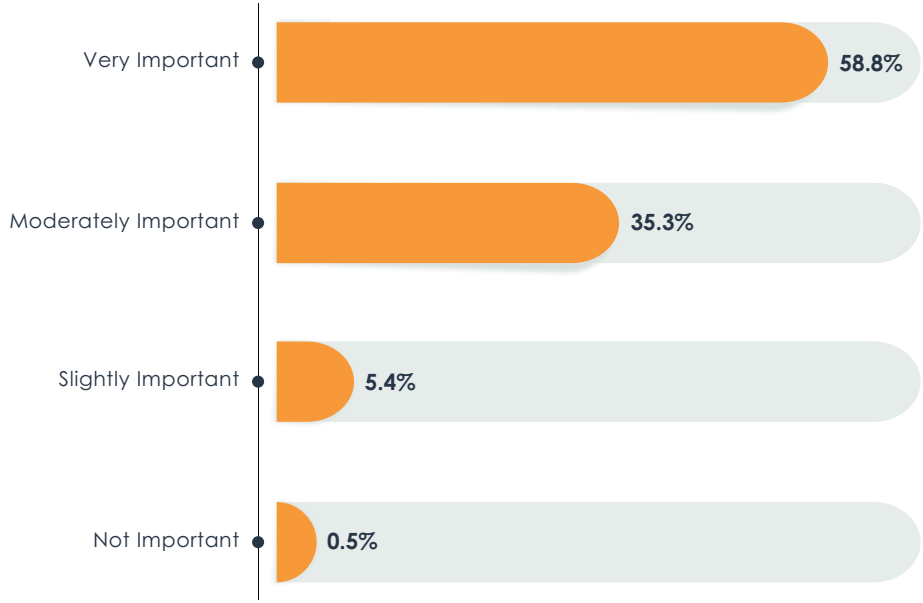
Analysis:

Organizations are hoping to start a zero trust project, and they do not just want to go with the first vendor that comes along. Organizations looking to start a zero trust project are seeking leaders in the zero trust space to guide them on their zero trust journey. Ninety-four percent ranked zero trust experience and leadership as very or moderately important.

Commentary:

The industry is filled with vendors claiming to be able to provide the best-in-class zero trust solution. However, that can hardly be the case—the technology is too new, there are many components to a zero trust infrastructure, and the number of best-in-class leaders must be finite. Not all vendors are created equal, and organizations would do well to understand the solutions from the vendors that they want to work with and their experience (and success) in implementing zero trust.

When considering a zero trust project, how important is it to your organization to work with established leaders and vendors in the zero trust space?



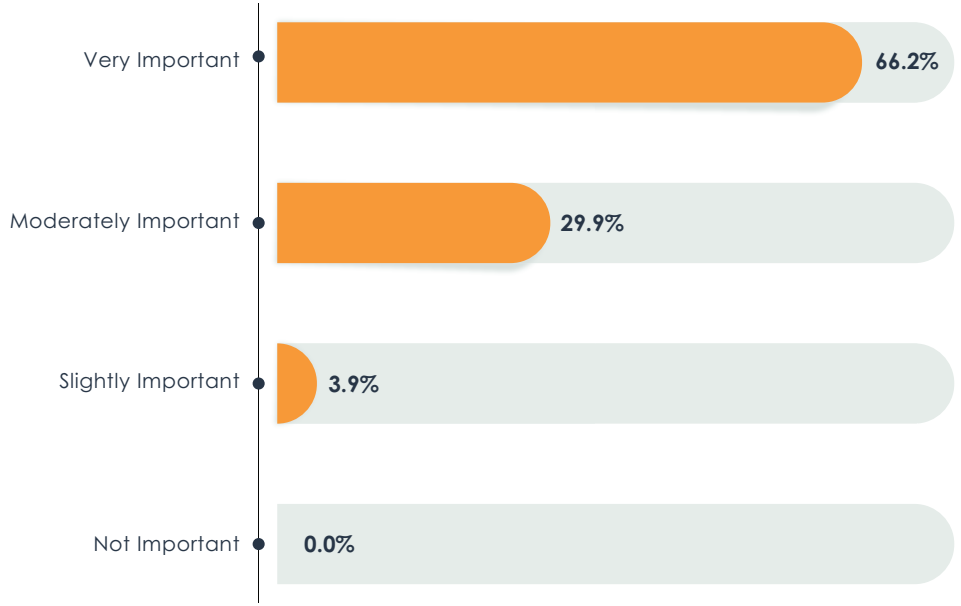
Analysis:

Zero trust is not a product or a single solution. It's an approach. To be successful with this approach requires a vendor that understands all of the various parts that make a zero trust infrastructure work. One way of accomplishing this is by finding a vendor that offers all of the components that make up a zero trust solution. Organizations believe that it is very important to moderately important over 95% of the time that their zero trust vendor has a comprehensive suite of zero trust-related security solutions.

Commentary:

Keeping in mind that zero trust is compromised of many different parts, it is important to consider a vendor that has a "full stack" solution. They are likely to succeed and offer advice for the entire project compared to individual point solutions. Organizations realize that their likelihood of success is exponentially greater if they use the solutions and advice from a single vendor instead of multiple point solutions with integration challenges and management considerations.

When considering a zero trust project, how important is it to your organization to work with vendors that have a comprehensive security solutions portfolio?



Data Privacy

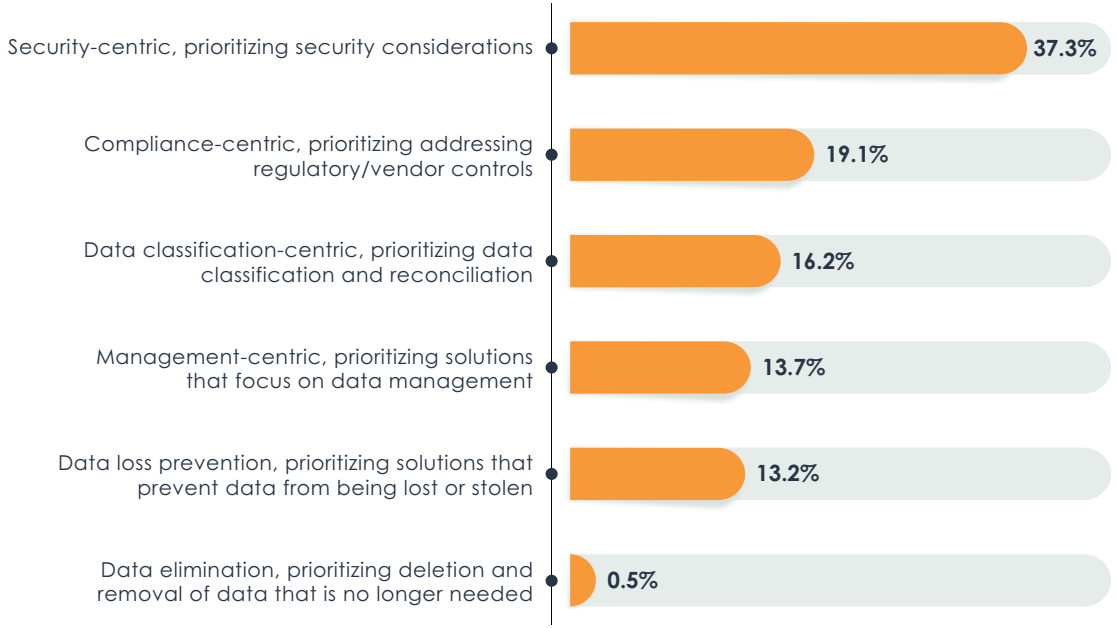
Analysis:

Data privacy is a major driver for organizations trying to implement a data security project. Many organizations (37%) have decided to take a security-centric approach to data privacy, prioritizing the security considerations first. Compliance (19%) and data classification (16%) round out the top three approaches to address data privacy.

Commentary:

As organizations embark on their data privacy projects, the key stakeholders need to determine the priority and approach to addressing data privacy concerns. In this survey, security was determined to be the primary motivator, but that answer could have just as easily focused on compliance if the survey respondent pool had been different. Both are valid approaches, and it is critical to agree on an approach before starting the project. There is no reason that the project cannot accomplish both, since the tools and vendors are designed with these approaches in mind.

When considering the methods used by your organization to address data privacy, which of the following best describes the approach?



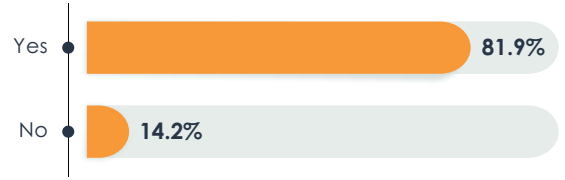
Analysis:

Most organizations intend to use their existing security tools to address data privacy concerns (82%). However, 72% of them are also willing to look at a specific tool to address data privacy considerations, provided that tool can address other security priorities. Ninety-five percent indicated that their data privacy tools need to also be used to address other security priorities in their environments.

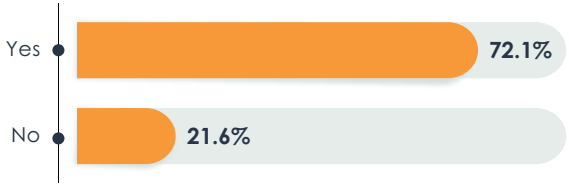
Commentary:

Very few organizations want point solution tools because the expense (both from cost and management/resource perspectives) often outweigh the benefits. While organizations are willing to evaluate a new tool to address specific data privacy considerations, it is critical that the tool can be used to augment other security priorities. While there are some specific tools around privacy searches and notifications, these one-off tools may also have other uses (like breach notification and incident alerting).

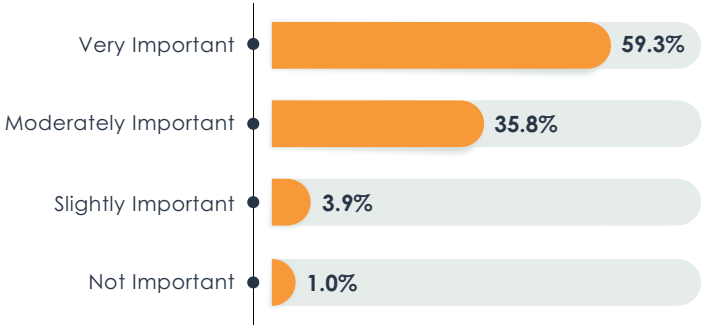
Is your organization evaluating tools/using existing security tools to address data privacy considerations?



Is your organization considering separate security tools to address data privacy?



How important is it to your organization that the tools used to address data privacy also be used to address other security considerations?



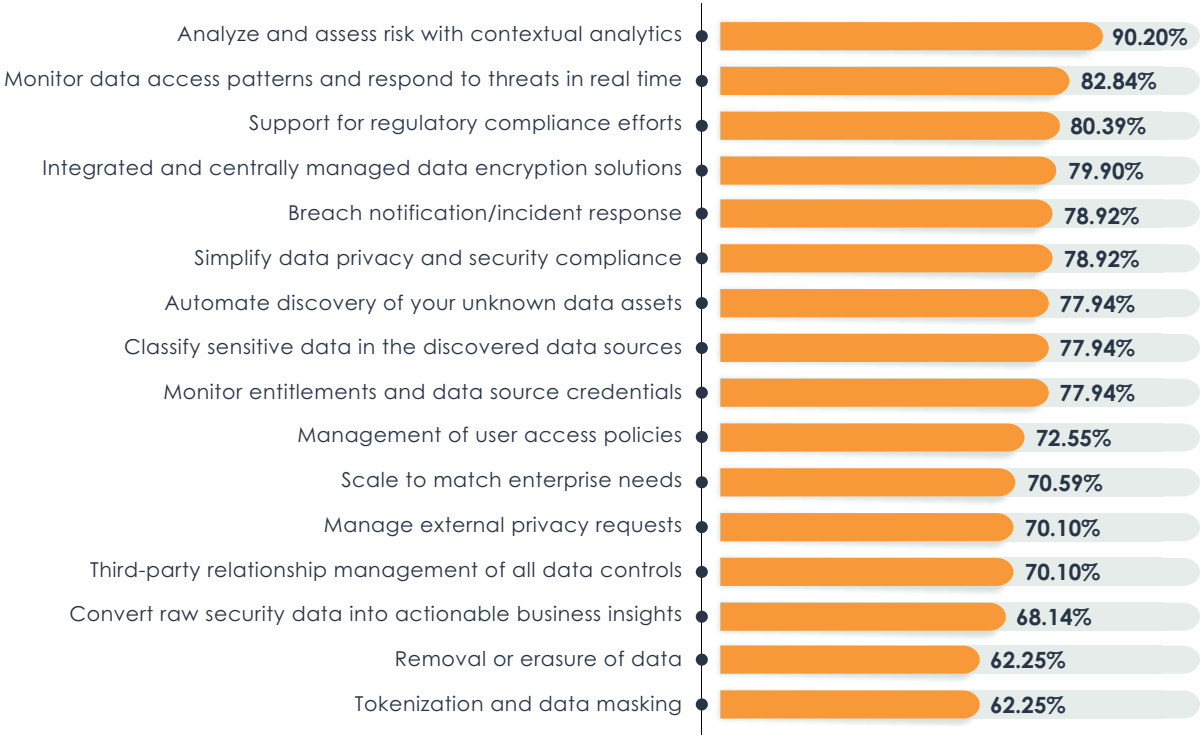
Analysis:

When investing in a data privacy solution, organizations are searching for numerous capabilities. First among these priorities was the ability for the solution to analyze and assess risk (90%). Monitoring data access (83%) and addressing compliance-related controls (80%) were also highly rated.

Commentary:

Data privacy solutions/tools must be able to address a variety of considerations. Some of these are expected and considered basic criteria for selecting any potential solution. A data privacy vendor that has a solution that addresses as many of the 16 capabilities that are listed here will have an advantage. Every one of the capabilities listed was considered important by a majority of those polled, meaning that any data privacy solution will likely need to provide some method of addressing all of them. A "full stack" solution provider will likely not have an issue addressing all of these considerations, while a point solution may be lacking in several of these key features.

What capabilities is your organization interested in investing/evaluating to address data privacy?



EMA Perspective

Data privacy and security are hot topics in the security industry right now, second only to the buzz around zero trust. Luckily, this survey was able to collect data on all three topics, and the responses were illuminating. Many organizations just recently started to integrate data security as part of their overall security strategy, and vendors are catching up with how best to address the needs of their customers. Among the most important results were that most organizations are interested in starting a zero trust project, and data security/privacy will be at the center of that engagement. Still, they don't want just any vendor. They are looking for leaders in the zero trust space, and preferably a leader with a complete zero trust and data security solution.

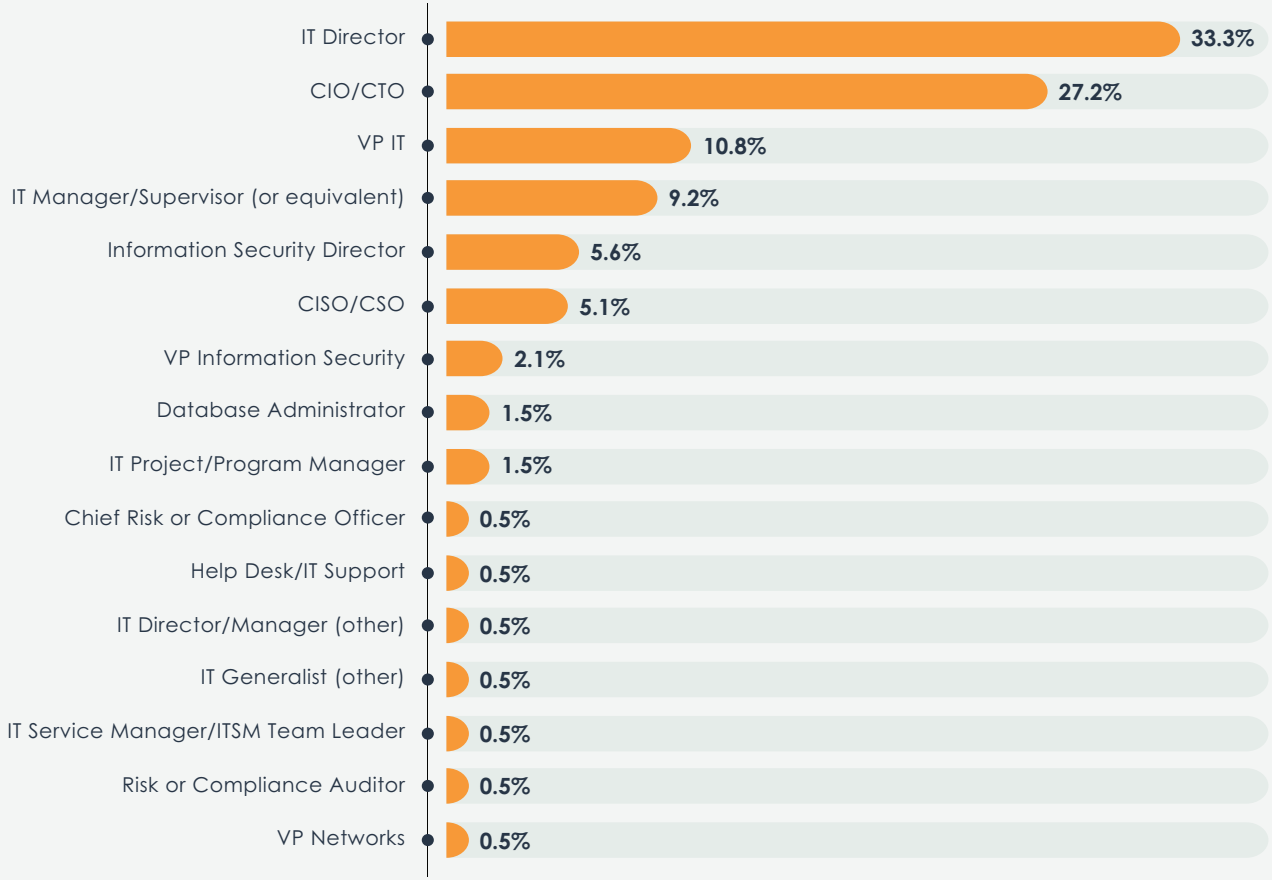
Organizations are ready to start their zero trust and data privacy journey, and they are investigating some key differentiators when selecting a vendor to guide them on their journey.

- **Ease of use.** Organizations want a complete solution: one that is easy to integrate into their existing environment, with robust and customizable reporting capabilities and is relatively easy to use and manage. They do not want to integrate a half dozen point solutions, nor are they interested in adding another battery of security tools, each designed to solve a specific problem (regardless of how well the tool may solve). Compliance and risk teams need a solution that will organize and classify data, while security teams are looking toward data encryption and access solutions. As basic as these criteria seem to be, they are anything but basic, since very few vendors have the ability to meet or exceed these requirements.
- **Security leadership.** It is not enough for the zero trust or data security solution to have the basic functionality that they advertise: organizations want industry leaders to help guide them through their project and help define their processes. MSPs and services integrators need to understand that their clients recognize that these sorts of projects are not short-term. They have multiple steps for implementation and often last years. Customers are looking for solutions and vendors that have a proven track record of success when it comes to managing their data estates and will be able to support them in the long term as the regulatory requirements change and technology is updated.
- **Zero trust is not a buzzword.** There are always emerging trends in the security industry, with plenty of vendors jumping on the bandwagon to ride the publicity around the current buzzword or phrase. Without question, there is a lot of buzz about zero trust, but unlike other fly by night trends, zero trust will be a philosophy that will drive security innovation for the foreseeable future. Organizations are excited to start their zero trust implementations, but require guidance to make all the pieces work. Also, organizations can smell a fraud—they know that the organization that sold them sprockets yesterday and wants to ride the zero trust wave is not likely the zero trust leader that they need today.
- **Compliance drives security spending.** The trend of the past several years continues with zero trust and data security—that regulatory compliance and vendor due diligence requirements drive security spending. Compliance requirements, such as GDPR and CCPA, are pushing organizations to evaluate their data security, and tools that can address those requirements will drive spending. Security professionals should work with the other divisions of their organizations to procure security tools that address the business requirements while furthering the security strategy. Breaking down communication barriers and getting a complete picture of the business priorities will not only help the security team with their goals, but integrate and align with business priorities.

Data security and zero trust will continue to be the top priorities of the business, and vendors that have a more complete understanding of the challenges that their clients face will be able to more completely guide their customers in these security projects.

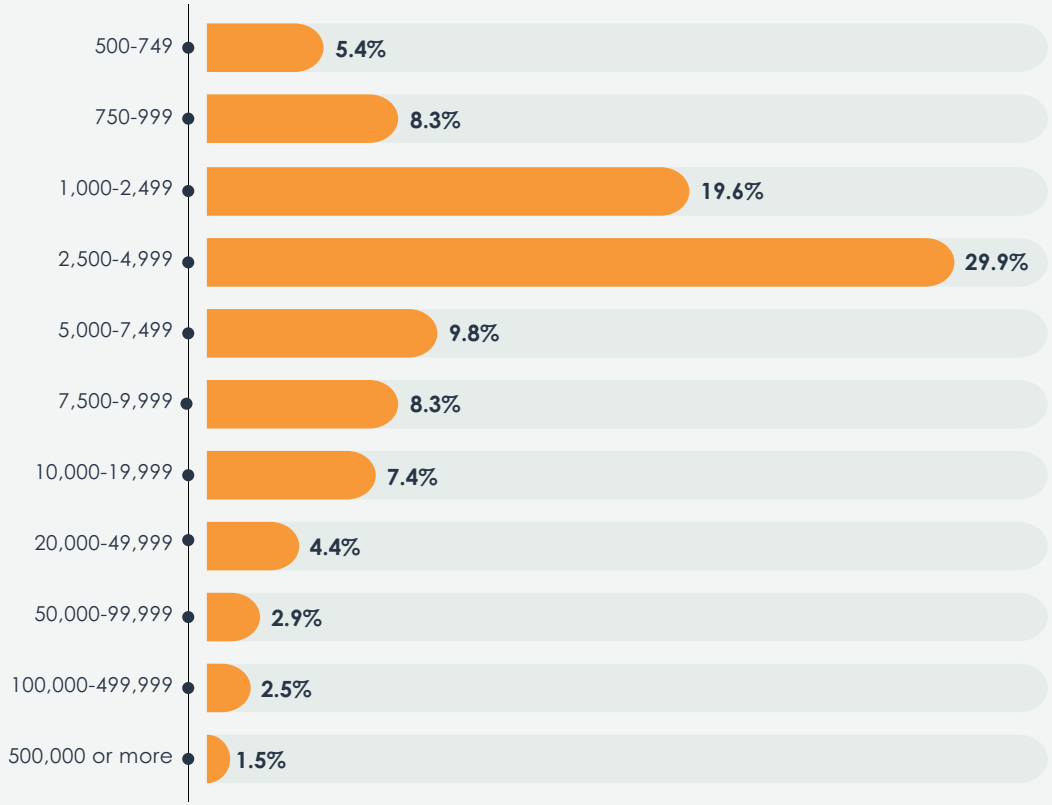
Demographics

You indicated that your department is IT-related.
Which of the following BEST describes your specific role?



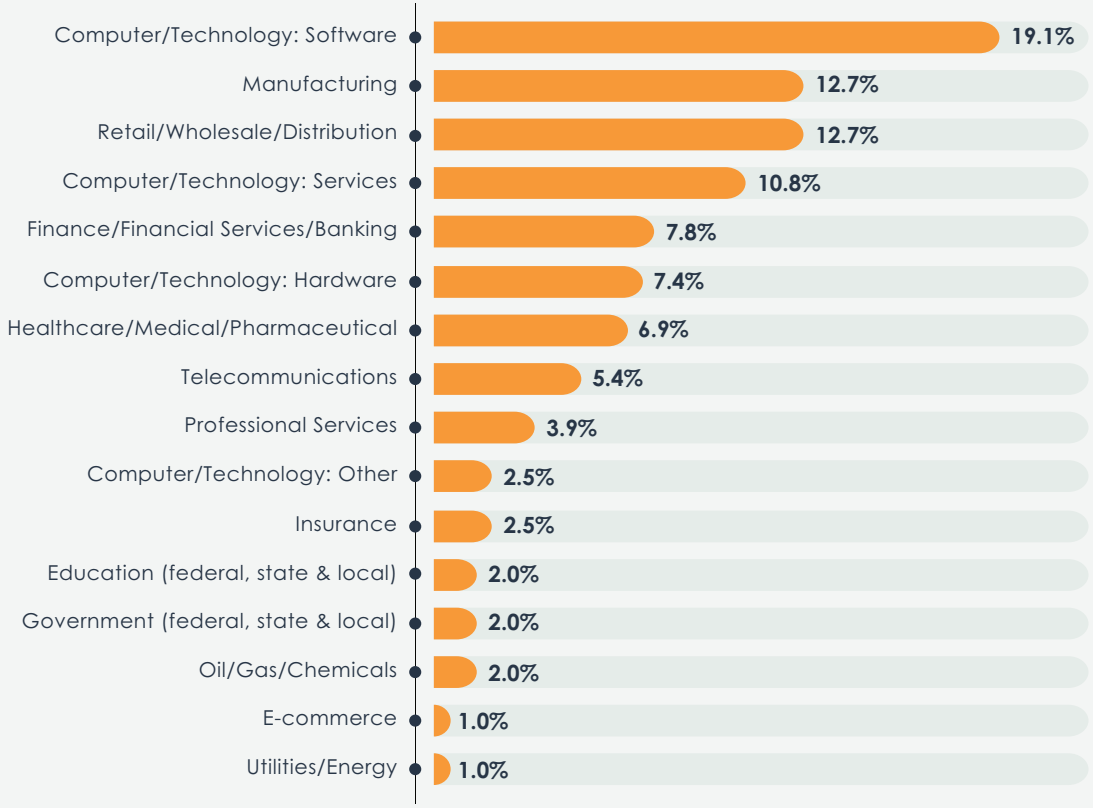
Sample Size = 195

In total, how many employees are currently working in your organization?



Sample Size = 204

Which of the following best describes your organization's primary industry?



Sample Size = 204

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4106.070621