The Cost of CVEs 2025

How Much Does In-House CVE Management Cost Your Business?

Chainguard

Table of Contents

Executive Summary

In-house management of Common Vulnerabilities and Exposures (CVEs) in containerized environments is a significant, and often hidden cost for many organizations. Our analysis of customer experiences with Chainguard Containers reveals that CVE remediation, image hardening, compliance, and customer escalations impose heavy operational burdens—costing organizations millions in wasted engineering time, lost revenue opportunities, and increased risk.

Key Findings

1. **CVE Management Costs You More Than You Think:** Engineering teams are often bogged down with CVE management tasks like triaging, patching, and compliance reporting. This takes valuable time away from revenue-generating activities like feature development and product innovation. As a result, teams often face delayed **releases, reduced product quality, and missed market opportunities.**

2. **The Hidden Costs of DIY CVE Remediation:** Many organizations continue to handle CVE management internally, which often results in inefficiencies and high labor costs. On average, companies that outsource CVE remediation to Chainguard realize $2.1 million in annual savings from that specific task alone—allowing them to reallocate engineering efforts towards strategic initiatives.

3. **Outsourcing CVE Management Delivers Tangible Business Value:** Organizations that outsource CVE management experience a broad range of benefits:

    - **Cost Savings:** Reduced operational overhead from CVE remediation, image hardening, and compliance tasks.
    - **Increased Revenue:** Unlock new markets, particularly highly regulated ones, by leveraging secure and compliant container images.
    - **Faster Innovation:** Free up development teams to focus on creating new features and accelerating time-to-market.
    - **Decreased Risk:** Proactively eliminate vulnerabilities and reduce the risk of costly breaches, fines, and customer churn.

4. **ROI Across Industries:** Our analysis shows that companies in the Healthcare, Financial Services, Telecommunications & Infrastructure (Telecom), Technology, and Consumer & Commerce industries can unlock millions in cost savings and new revenue. For instance, Healthcare organizations saved $50 million annually on average, with $39 million of that coming from reduced risk.

Findings by Industry

Industry	Total Benefits	Cost Savings	Increased Revenue	Faster Innovation	Decreased Risk
Financial Services	$13,894,701	$1,427,918	$4,898,507	$3,431,333	$5,525,250
Consumer & Commerce	$32,260,238	$3,549,471	$5,526,256	$10,112,778	$13,071,733
Healthcare	$50,402,822	$2,728,874	$7,284,589	$3,652,222	$39,165,333
Technology	$9,849,190	$1,682,914	$4,597,949	$4,821,250	$2,168,889
Telecom	$48,789,216	$1,146,131	$3,009,589	$42,940,833	$18,012,667
Overall Average	**$31,039,233**	**$2,107,061**	**$5,063,378**	**$12,991,683**	**$15,588,774**

Findings by Revenue Segment

Industry	Total Benefits	Cost Savings	Increased Revenue	Faster Innovation	Decreased Risk
Tier 1: Enterprise ($10B+)	$43,653,151	$2,604,616	$4,460,630	$17,703,095	$24,801,333
Tier 2: Large ($1B–$10B)	$11,727,163	$970,323	$3,978,816	$4,065,278	$3,293,500
Tier 3: Mid-Market ($500M–$1B)	$9,600,344	$2,875,708	$2,252,920	$3,300,833	$2,821,300
Tier 4: Growth-Stage ($100M–$500M)	$14,770,032	$1,377,371	$12,618,493	$3,914,722	$1,323,667
Tier 5: Early-Stage (<$100M)	$6,808,059	$1,053,432	$3,009,589	$6,601,667	$1,898,000

How Costly is CVE Management?

Common Vulnerabilities and Exposures (CVEs) in containers are more than just a routine nuisance — they impose substantial and ongoing operational costs. If you're responsible for platform or application security, you likely already know the burden: scanning, triaging, and remediating CVEs eats up time, saps engineering cycles, and shifts focus away from delivering business value.

Over the last few years, high-profile vulnerabilities like Log4Shell (CVE-2021-44228) and recent Ingress-NGINX remote code execution CVEs have underscored the stakes. These incidents disrupted teams globally — not just because of their technical severity, but because of how difficult, time-consuming, and expensive they were to manage in containerized environments.

But how costly is CVE management, really? That's the question we set out to answer.

There has been little research on this topic. In 2022, Ponemon and Rezilion published The State of Vulnerability Management in DevSecOps. And back in 2024, we published The True Cost of CVE Management in Containers. We interviewed software professionals who handled CVE management as part of their daily responsibilities at a variety of different organizations, asking about the time they were spending managing CVEs in containers, the specific pain points, and what that time ultimately cost. The results were clear: teams are spending significant portions of their engineering time on CVE work — often at the expense of core business initiatives. And in most cases, they'd rather not be.

Since the initial study, Chainguard has grown to serve over 160 organizations, many of whom have echoed those frustrations. Whether large or small, no matter the vertical, these teams consistently report that CVE management remains a major drag on developer time — especially when specialized expertise is required for triage and remediation. And that ends up costing organizations money.

Many of our customers have worked with Chainguard to quantify the cost of not addressing the CVE management problem in their container images. In this report, we share findings from our analysis, broken down by industry segment (Healthcare, Telecommunications & Infrastructure, Consumer & Commerce, Financial Services and Technology) and organization size — to expose just how costly unmanaged CVEs can be.

Measuring the cost of CVE management and the return on investment organizations can expect when using a solution like Chainguard Containers requires a structured, consistent framework, especially given the range of variables across organizations. To enable meaningful comparison and actionable insight, Chainguard developed a standardized methodology to quantify both the direct costs and return on investment of outsourcing CVE management efforts. Each participating customer provided data specific to their environment, enabling individualized savings calculations across four distinct dimensions, encompassing both internal operational efficiencies and outward-facing market entry dynamics. All data is anonymized to protect customer privacy and confidentiality.

When working with customers to assess the total return on investment for outsourcing CVE management, we begin by understanding the cost savings organizations can expect:

Cost Savings: The cost avoided by eliminating time spent on tasks such as building hardened images, remediating CVEs, achieving compliance (e.g., FIPS, STIGs, etc.), and handling CVE-related customer escalations. This was calculated using inputs like engineering team size, time allocation, and average engineer salary.

After assessing the cost savings, we look at the overall value unlocked, in the form of revenue (by unlocking new markets and freeing up developers) and decreased risk:

Increased Revenue: The new revenue opportunities unlocked through outsourcing image hardening and CVE remediation to Chainguard, by adopting Chainguard Containers. This includes access to highly-regulated and security-conscious markets (e.g., federal contracts), customer deals dependent on vulnerability remediation, and faster release cycles unblocked by security clearance.

Faster Innovation: The revenue generated from reallocating engineering time (previously spent on CVE remediation) toward product development. This includes reducing time-to-market for new features and products, driving higher win rates in B2B and B2C offerings, and expanding addressable markets.

Decreased Risk: The potential loss avoided by preventing a container-based breach. This is modeled using historical breach data, breach likelihood, incident response costs, and estimated reputational damage and customer churn impacting revenue.

Before getting into the details, it’s important to understand more about the methodology.

Methodology

During the qualification process, we worked with a selection of participating customers to generate a monetary value attached to each of the four categories. Some opted out of areas that were not relevant to their business model or maturity. As a result, the number of data points varies by the key area under consideration. This variation means that the summation of average benefits across customers does not equal the average of the total summed benefits. To accurately reflect aggregate outcomes, we use the average of the summation for each category rather than simply adding the average benefit for each of the key areas per segment. This approach ensures integrity and avoids misleading inflation or dilution of impact estimates

After collecting each of these numbers, we divided the data for the participating organizations into five groups based on their industry:

1. Healthcare
2. Telecom & Infrastructure
3. Consumer & Commerce
4. Financial Services
5. Technology

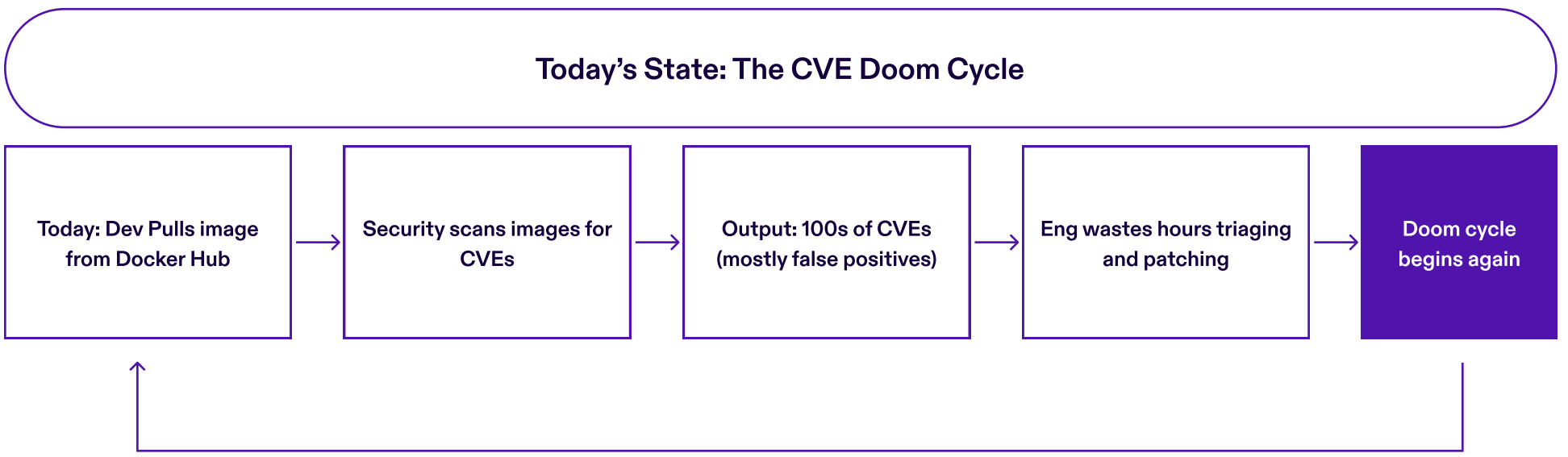
We also split the findings into five different revenue segments based on the organization's annual revenue:

1. Enterprise: $10 billion+
2. Large: $1 billion–$10 billion
3. Mid-Market: $500 million–$1 billion
4. Growth-Stage: $100 million–$500 million
5. Early-Stage: <$100 million

The report is organized into two sections: First, we'll do a deep dive into the cost savings data for each industry and revenue segment. Next, we'll look at the value organizations unlock across increased revenue, faster innovation, and decreased risk, again for each industry and revenue segment, looking at the overall totals alongside any segment-specific trends.

The Costs of DIY CVE Management

When we began assessing the data our customers shared, we were particularly interested in the key area of cost savings. Engineering teams building CVE management programs in-house often dedicate enormous time and effort to areas outside of the core business functions. This time and effort is costly, and pulls engineers away from innovation and revenue-generating activities. These numbers capture the savings that organizations experience across CVE remediation, image hardening, compliance, and customer escalations. Saving in these areas enables customers to boost revenue and accelerate innovation by empowering developers to focus on building products and solutions instead of being stuck in the CVE doom cycle.

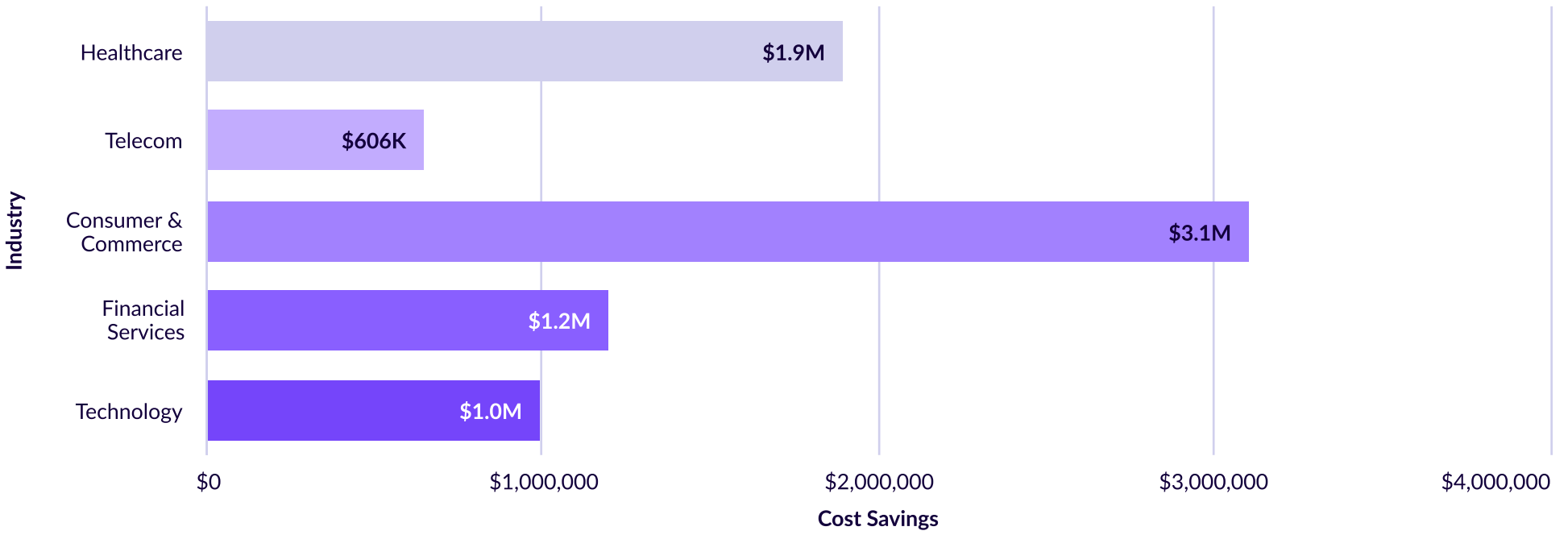


Not every customer participated in every section of the value assessment. As a result, some industries and revenue segments will not have numbers for all four of the above cost savings areas. This doesn't mean that organizations don't experience cost savings in a particular area — it just means that the organization chose not to focus on it when quantifying the value of outsourcing vulnerability management. As we'll see throughout the report, every organization is different, and the value of outsourcing CVE management manifests itself in different ways depending on an organization's unique needs.

DIY CVE Remediation

For many organizations, doing CVE remediation in-house was incredibly costly. The customers participating in this analysis saved an **average of $2.1 million** annually by outsourcing CVE remediation. For this cost savings area, and others throughout the report, the higher savings amounts tend to correlate with the breadth of the organizations' current efforts in the area. In this case, organizations with higher amounts of container images saved more, as a wider scope requires more headcount to effectively manage CVEs in-house.

CVE Remediation Savings by Industry



Consumer & Commerce companies saw the largest CVE remediation savings, averaging $3 million annually, due to the intense burden of managing vulnerabilities across fast-moving, microservice-heavy environments. Manual patching, testing, and redeployment consume vast engineering hours and hinder velocity. By adopting zero-CVE container images, these organizations drastically reduce rework and protect customer-facing systems while freeing up developers to focus on feature delivery.

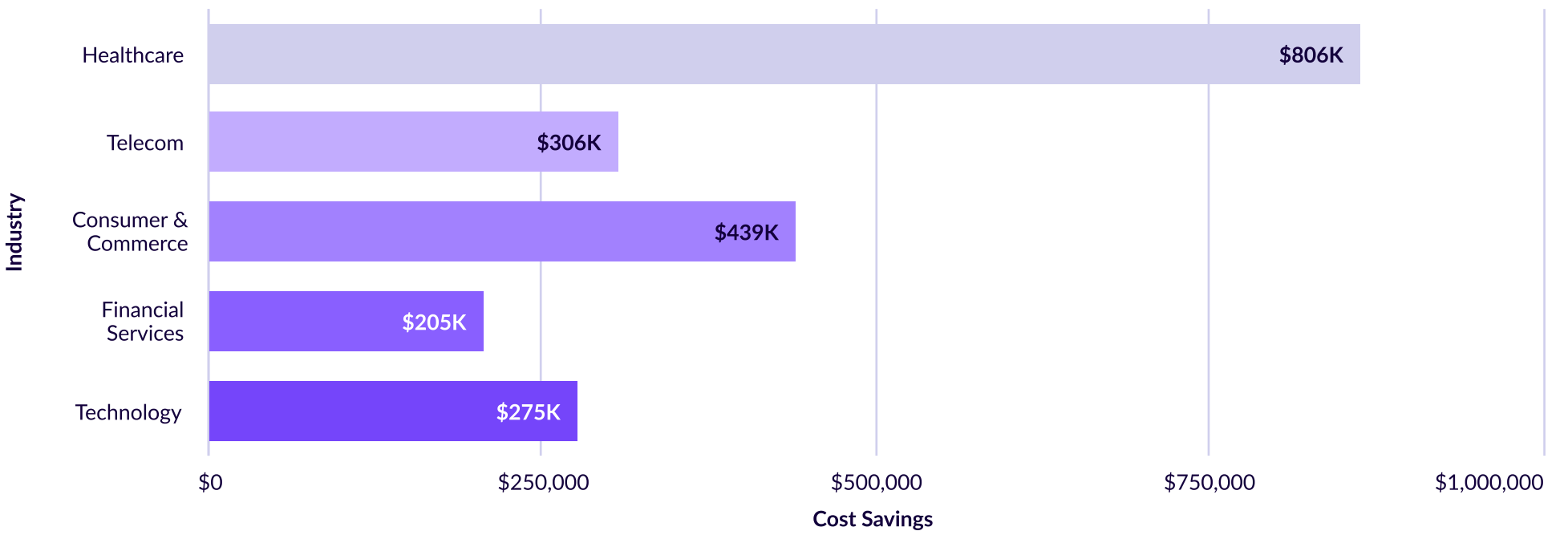
Other industries reported similarly significant savings from eliminating manual CVE triage. Healthcare organizations saved an annual average of $1.8 million by simplifying remediation across legacy and high-risk systems under regulatory pressure like HIPAA. Financial Services saved $1.16 million on average annually, where CVEs carry audit and compliance risk requiring meticulous documentation and cross-team coordination. Tech companies saved $1 million annually by automating CVE workflows, preserving SLAs, and accelerating product delivery. Even in Telecommunications & Infrastructure, with fewer but higher-stakes vulnerabilities, teams saved an average of $600,000 annually by minimizing the coordination burden of large-scale vulnerability patching across critical systems.

When filtering the data by revenue segment, mid-market organizations saw the highest average savings at $2.13 million annually, followed by enterprise organizations at an annual average of just below $2 million. Enterprise organizations can see large amounts of savings in this category due to the presence of golden image programs, which often require many hours of platform engineering time to maintain. For mid-market organizations, a golden image program is rare, and engineers must spend time manually remediating CVEs to meet security requirements. These organizations typically don't have the same level of CVE remediation infrastructure in place that large or enterprise organizations have, making the task more laborious and expensive. Large, growth-stage, and early-stage organizations all saw similar average annual savings in this category, at $665,000, $706,000, and $581,000, respectively.

DIY Image Hardening

Image hardening — the process of securing container base images through proactive vulnerability prevention by building minimal images that include only necessary packages, applying secure configurations, and enforcing security policies — also delivered significant savings for organizations who outsourced the task. An effective in-house hardened image program requires a special combination of platform-specific knowledge to build and dedicated headcount to maintain. These organizations saved an **average of over $400,000 annually** by outsourcing image hardening.

Image Hardening Savings by Industry



Healthcare institutions achieved the highest average annual image hardening savings—over $800,000—by adopting zero-CVE containers that ease regulatory compliance. Managing a mix of legacy and modern systems, these organizations face strict audit requirements that make in-house hardening resource-intensive. Zero-CVE containers reduce both the compliance burden and engineering toil, enabling teams to focus on patient-centric development without sacrificing security.

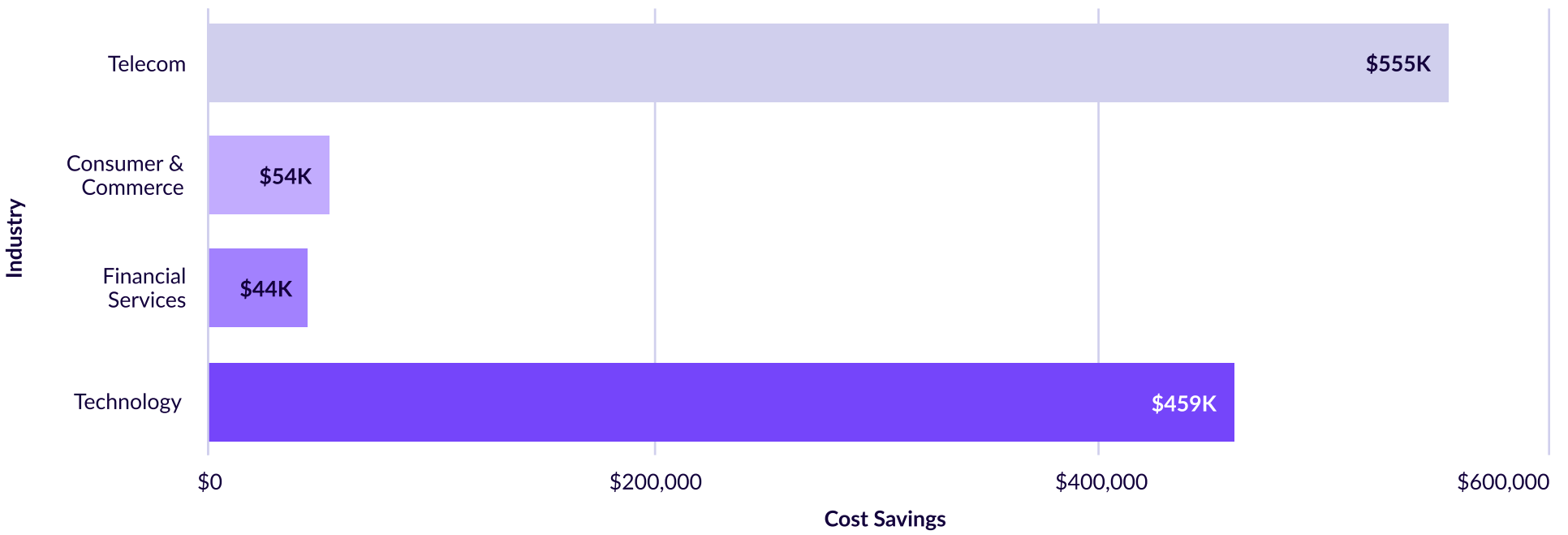
There were considerable savings across industries. Consumer & Commerce companies saved an average of $439,000 annually by eliminating the need to harden thousands of frequently updated container builds, a task complicated by diverse dependencies and rapid release cycles. Telecommunications & Infrastructure firms saved an annual average of $300,000, where FedRAMP-level compliance across distributed environments demands rigorous image control. Technology companies, though often staffed with capable infrastructure teams, still saw $275,000 in average annual savings by outsourcing the heavy lift of securing and maintaining base images. Financial Services organizations saved $205,000 on average annually by meeting stringent security and compliance standards, like PCI-DSS, without slowing their development pace, thanks to zero-CVE hardened containers.

Across the different revenue segments, enterprise organizations saw the highest average annual savings at $484,000. Enterprise organizations typically have the highest total number of container images running in their organization. Interestingly, growth stage organizations came in second here, with an average annual savings of nearly $388,000. For many growth-stage organizations, it is important to begin hardening images early in the organization's maturity, as hardening an increasing number of images only becomes more expensive and difficult as the company grows. By spending time and effort on this problem early, many growth-stage organizations hope to avoid trouble around fulfilling customer requirements of using images with lower attack surface down the road.

Compliance

Another popular use case for outsourcing CVE management is to make it easier for organizations to meet compliance requirements around CVEs and continuous monitoring. This drives not only cost savings, but also, for many organizations, increased revenue by tapping into new regulated markets. These organizations saved an **average of over $278,000 annually.**

Compliance Savings by Industry



The compliance requirements around CVEs across different compliance frameworks often manifest as a daunting, sometimes confusing problem for organizations across industries. In industries like Healthcare or Financial Services, CVE remediation and image hardening contribute to the safety of the business and the overall goal of reducing risk. These goals contribute to an overall “compliance” need. But in some cases, getting to zero CVEs is just the beginning of a potential compliance journey.

Many compliance frameworks require additional image hardening standards like FIPS (Federal Information Processing Standards) cryptography and STIGs (Security Technical Implementation Guides). Some frameworks, like FedRAMP, also require POA&Ms (Plan of Action and Milestones) for remediation of every CVE that has not already been addressed in an organization’s containerized environment. These standards must be maintained in the event of an audit by regulators, so compliance isn’t just achieved; it must be continuously maintained. When an organization has hundreds of container images, and potentially even more CVEs, creating FIPS images, STIGs, and POA&Ms in-house becomes a tall order.

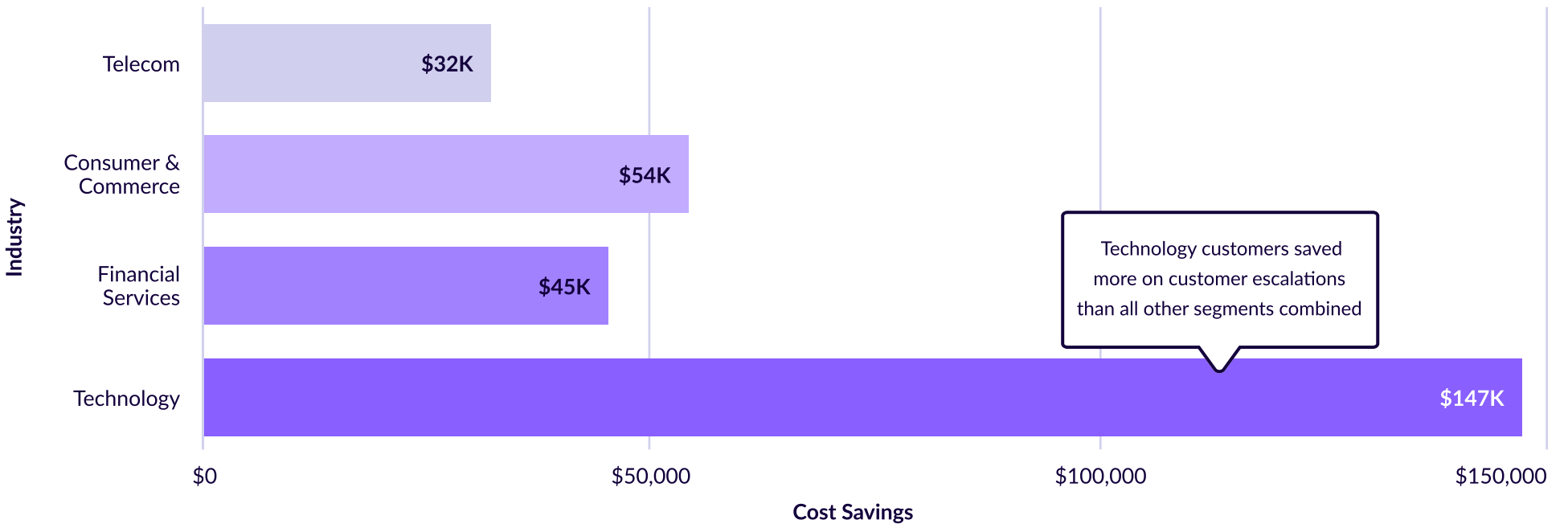
Organizations quickly see savings by simplifying this problem. Telecommunications & Infrastructure companies reported the highest average annual savings at $555,000, followed by Technology companies, which saved an average of $459,000 annually. Consumer & Commerce firms saw $54,600 in annual savings. And Financial Services companies, subject to stringent rules like PCI-DSS and FFIEC, saved $44,600 annually.

Similar to CVE remediation, enterprises and mid-market organizations saw the highest average annual savings in compliance ($555,000 and $481,000, respectively). As mentioned above, for many Chainguard customers, CVE remediation and compliance go hand-in-hand. Remediating CVEs allows organizations to meet rigorous compliance standards. Achieving compliance goals like FedRAMP or PCI-DSS help organizations reduce risk and unlock new market opportunities, ultimately driving increased revenue.

Customer Escalations

An often overlooked area of savings for organizations that outsource CVE management is a reduction in customer escalations. If CVEs are already taken care of, many organizations offering products and services that require a high degree of security will see fewer escalations and spend fewer staff hours handling said escalations. Many organizations saw tangible savings in this area, with an **annual average of $70,000** across all organizations.

Customer Escalation Savings by Industry



Technology companies reported the highest average annual savings—$150,000—by proactively preventing CVE-related customer escalations. Serving enterprise clients and regulated industries, these firms face intense scrutiny, where even a single vulnerability can trigger procurement delays or breach contractual SLAs. Escalations consume time from high-cost teams across security, engineering, and customer success. Eliminating CVEs before deployment helps reduce these costly, trust-impacting events.

Other industries saw meaningful but lower savings. Healthcare organizations saved an average of $54,700 annually by avoiding disruptions to sensitive clinical systems and the documentation demands of compliance-triggered escalations. Financial Services firms saved $45,000 by heading off escalations tied to client audits and vendor assessments, protecting high-value relationships and ensuring regulatory alignment. Telecommunications & Infrastructure companies reported $32,900 in savings; while less frequent, their escalations carry high coordination and reputational costs, making upstream prevention a critical efficiency gain.

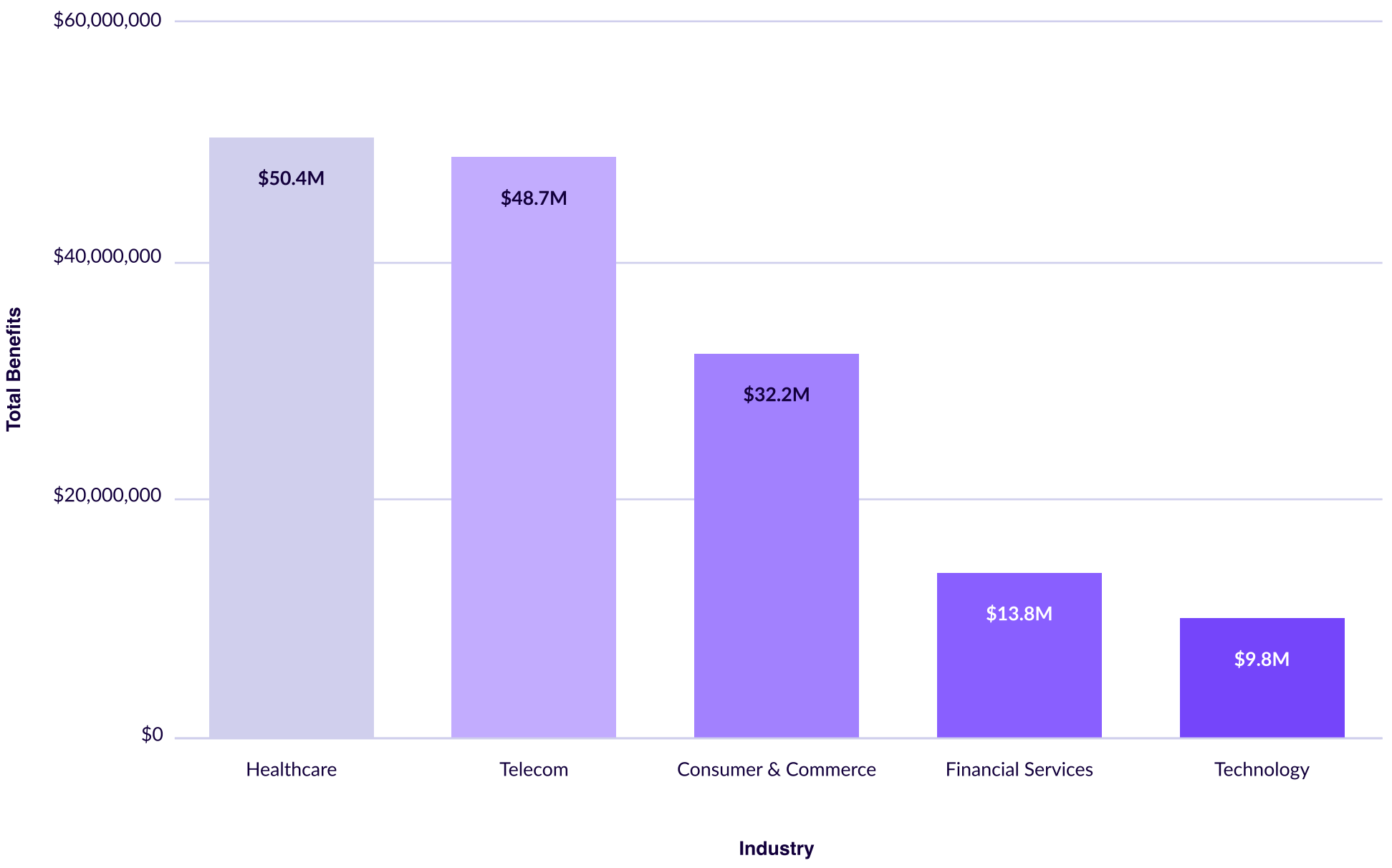
Interestingly, mid-market and growth-stage organizations reported the highest average annual savings in the customer escalations category. Mid-market organizations, with over $327,000 in average savings, saved more in customer escalations than all the other revenue segments combined. Many organizations in this market segment have customers with highly regulated environments, and these organizations must deal with CVEs or face the consequences. With a typically large footprint of container images relative to company size, mid-market organizations can see massive savings in decreasing the number of customer escalations they need to deal with.

Value Unlocked by Industry

The cost savings organizations experience by outsourcing CVE management is measurable. However, those cost savings are really just the beginning of the value organizations unlock when investing in a CVE management solution. In the following sections, we'll break down the value Chainguard customers unlocked in three key areas: increased revenue, faster innovation, and decreased risk.

We'll examine the data first by looking at each of the five major industries in the report, beginning with the total amounts that the organizations in each industry shared with our team:

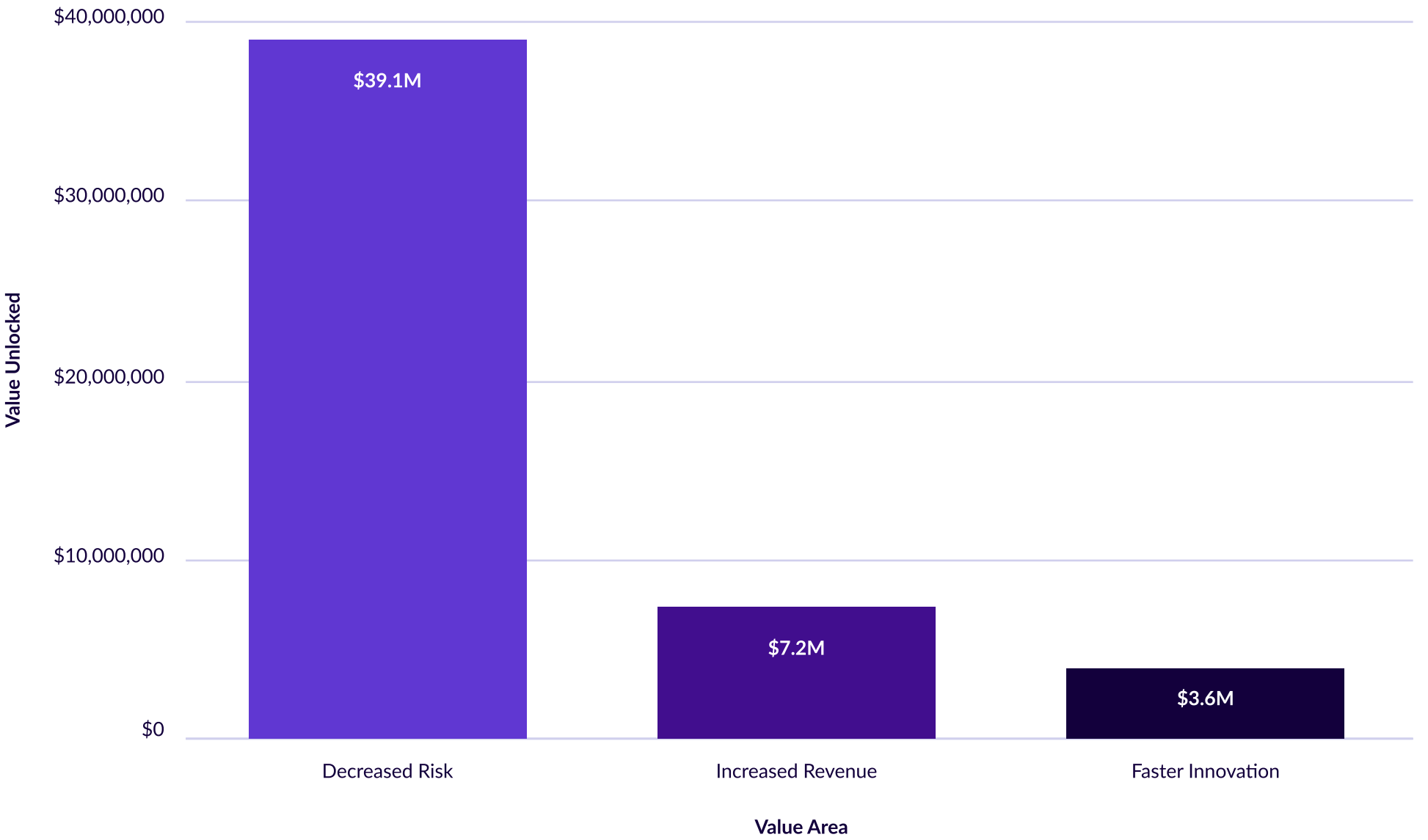
Average Overall Value Unlocked by Industry



Healthcare

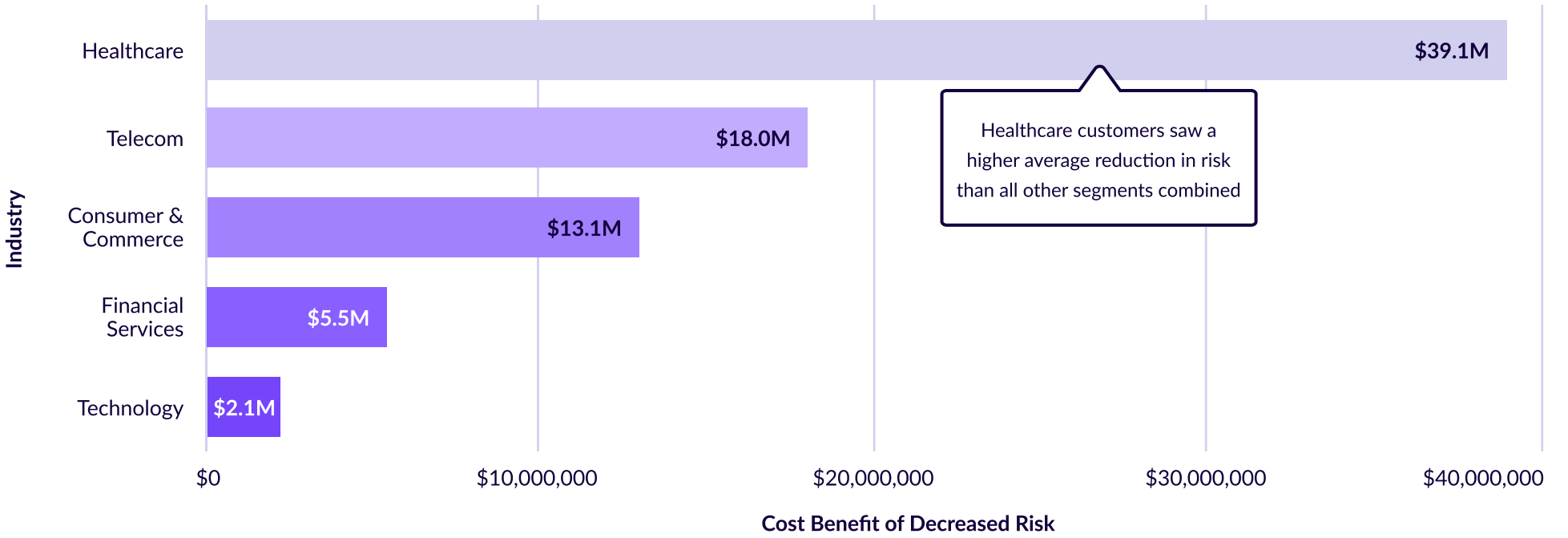
Value Unlocked for Healthcare Organizations

Healthcare customers derive high benefits of $39 million from reduction of security risk



When it comes to adopting secure container practices, Healthcare organizations experienced the most significant financial benefits of any industry segment, with an average total impact of $50 million annually. These gains are primarily driven by a $39 million reduction in risk on average, reflecting the sector's heightened sensitivity to security breaches due to the presence of regulated and sensitive medical data, as well as strict compliance requirements within HIPAA. The risk of revenue loss from breaches — especially through customer attrition or loss of market share — is significantly reduced through proactive security measures. Healthcare companies leveraging Chainguard Containers benefit by outsourcing image hardening, which streamlines operations while ensuring compliance and resilience across complex, regulated environments. Healthcare companies benefit by outsourcing image hardening, which streamlines operations while ensuring compliance and resilience across complex, regulated environments.

Healthcare organizations benefit the most from decreased risk



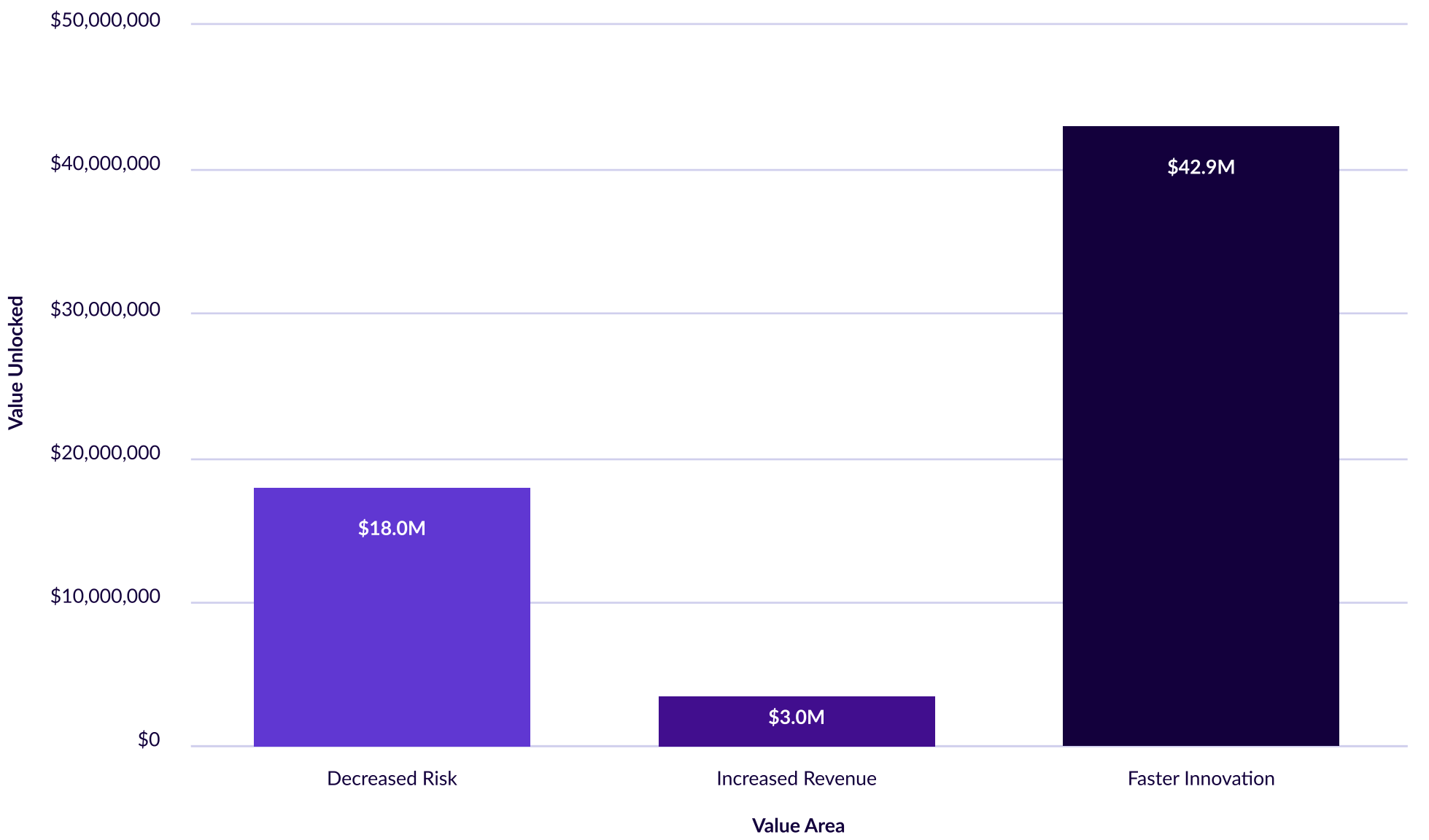
On the revenue side, Healthcare customers also achieved an average of $7.3 million in increased revenue, fueled by one major organization unlocking $11.5 million in new opportunities by expanding into new markets and increasing deal size. Additionally, cost savings in this sector totaled an average of $2.7 million. The main contributor to these savings is CVE remediation, which accounted for an average of $1.8 million and involved a large number of software engineers. By eliminating time-consuming, manual vulnerability management tasks, healthcare providers can focus engineering capacity on innovation and patient-oriented solutions, while maintaining strict compliance and security postures.

Chainguard Containers are well-positioned to help organizations in the Healthcare industry vastly reduce their risk profile, while also powering these organizations to achieve critical compliance requirements. In January 2025, HIPAA announced new guidelines around vulnerability management, which include a strict SLA around CVE remediation and a requirement to regularly audit healthcare organizations' environments to ensure they stay CVE-free. Since Chainguard Containers start at zero CVEs and stay there, Healthcare organizations can quickly see time to value without needing to maintain continuous compliance in-house.

Telecommunications & Infrastructure

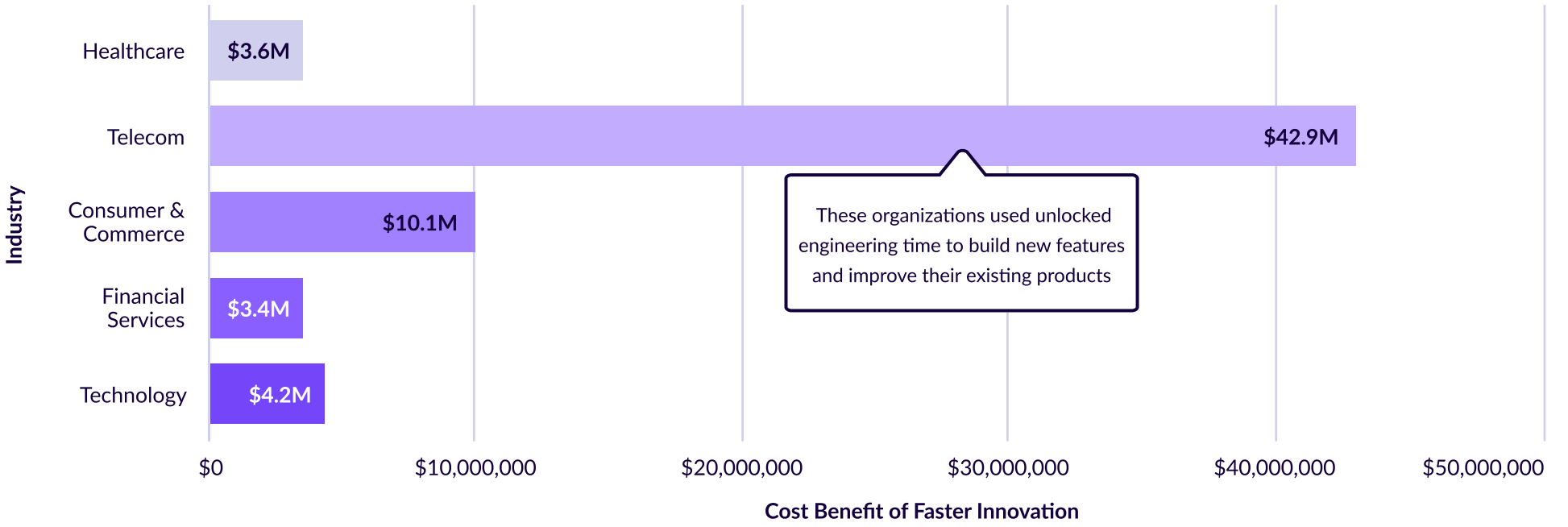
Value Unlocked for Telecommunications & Infrastructure Organizations

Telecommunications & Infrastructure customers unlock an average of almost $43 million with faster innovation



Telecommunications & Infrastructure (Telecom) organizations have unlocked an average of $49 million in total benefits by improving their container security posture and accelerating innovation. Faster innovation was a major contributor, with an average of $43 million added, especially by large enterprise customers introducing new B2C offerings. These innovations enabled them to deliver new services while maintaining a strong security baseline quickly, a critical requirement in this highly competitive and consumer-facing industry. These companies realized significant efficiency gains and revenue expansion by optimizing their DevSecOps pipelines for speed and resilience.

Telecommunications & Infrastructure organizations benefit the most from faster innovation



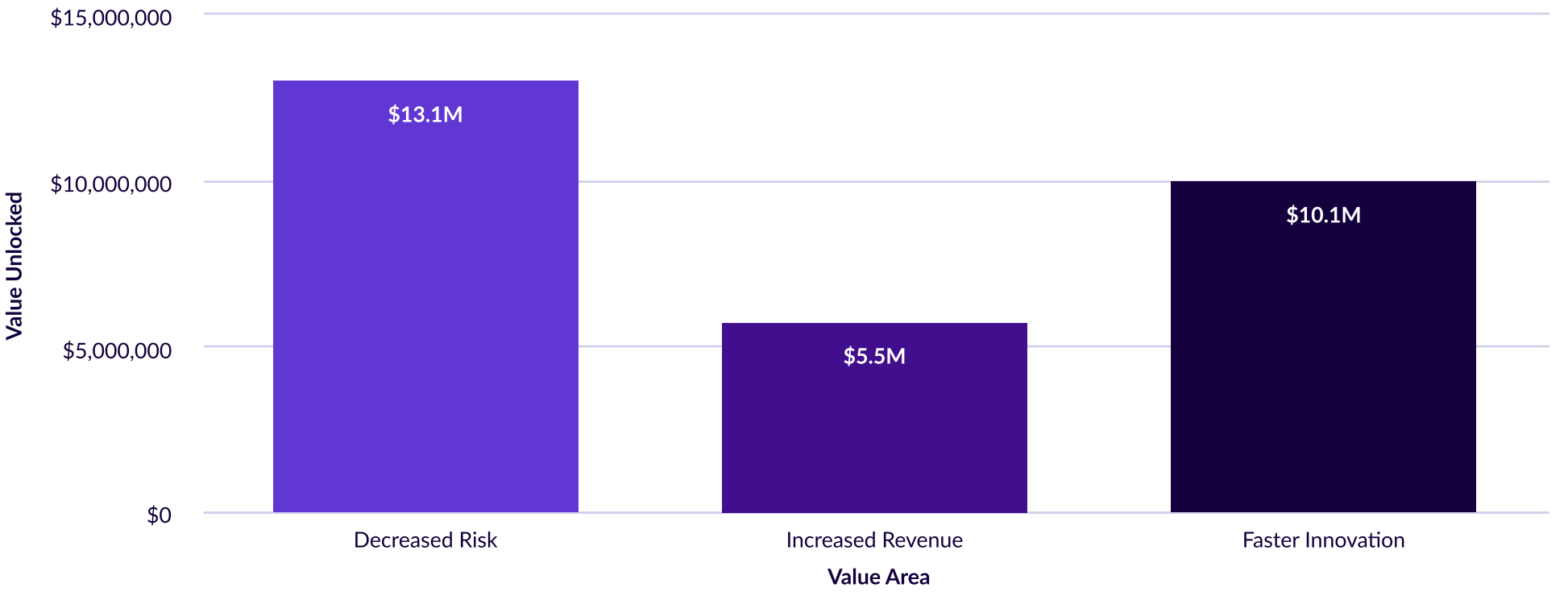
These organizations also achieved an average of $18 million in decreased risk, largely by reducing the potential for customer churn following security incidents. With revenue thresholds exceeding $10 billion, telecom companies are particularly vulnerable to reputational damage and regulatory scrutiny when breaches occur. These security investments translated into an average of $3 million in increased revenue, as providers gained access to federal and other security-conscious customers, underscoring the dual business and operational value of container hardening and continuous vulnerability management.

Chainguard Containers help telecom companies overcome the persistent security and compliance challenges associated with CVE management in large, distributed environments. These organizations operate critical infrastructure and consumer-facing services, where even minor vulnerabilities can lead to significant operational disruptions or reputational damage. Chainguard's zero-CVE container images eliminate the need for manual triage, patching, and image hardening, freeing engineering teams from the toil of maintaining secure baselines across vast, dynamic container fleets. This enables faster deployment of new services while ensuring consistent compliance with demanding regulatory frameworks like FedRAMP. By automating security at the container level, Chainguard empowers telecom companies to maintain trust, reduce exposure, and innovate at the speed their markets demand—all without the drag of traditional CVE remediation workflows.

Consumer & Commerce

Value Unlocked for Consumer & Commerce Organizations

Consumer & Commerce customers see an average benefit of over $13 million as a result of decreased risk



Consumer & Commerce organizations achieved substantial financial benefits by investing in secure container management practices, with average documented value unlocked reaching $32 million. The most significant contributions come from an average of $13 million in decreased risk and $10 million from faster innovation. This ROI is particularly pronounced in customer-facing environments, where the impact of security breaches is magnified by reputational damage and customer churn.

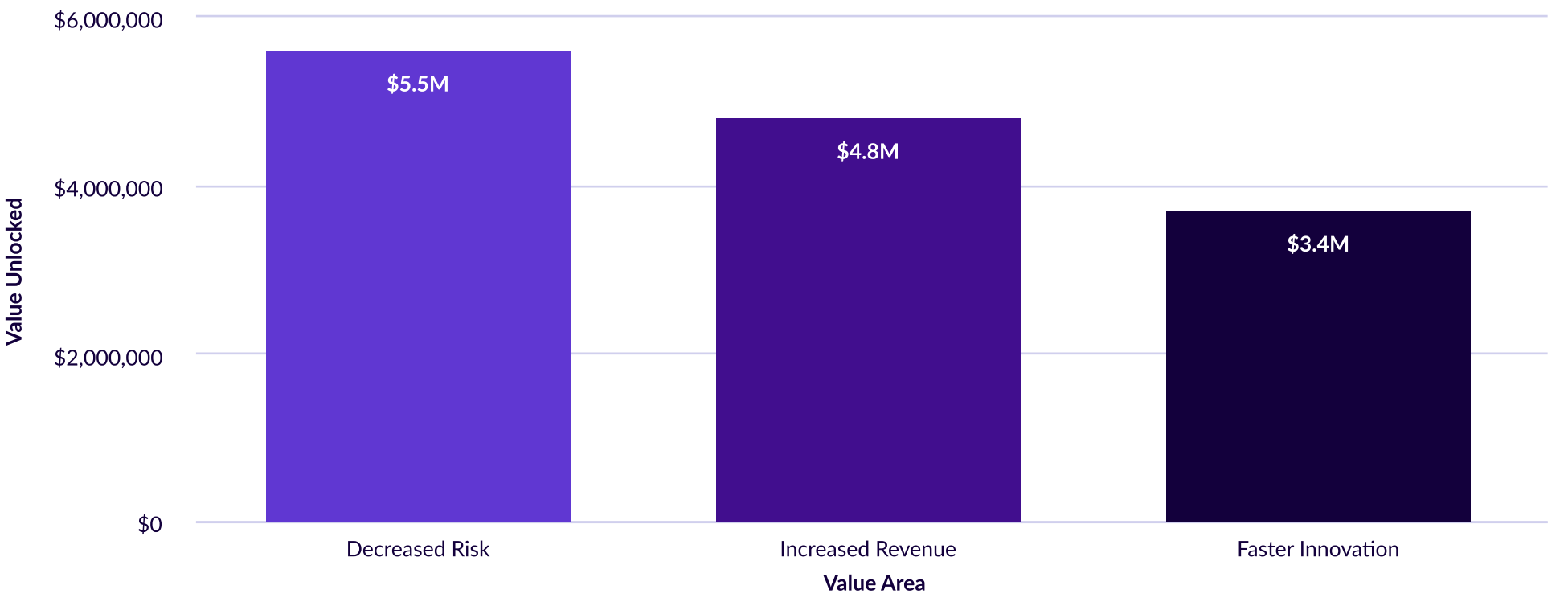
Faster innovation also played a critical role, contributing to increased speed-to-market and enabling the delivery of secure new features to end users. This strategic agility translated into an average of $5.5 million in increased revenue, largely driven by a global e-commerce leader unlocking $6.5 million in new business by meeting the security expectations of highly regulated markets.

Chainguard Containers enable consumer & commerce companies to maintain security and compliance in fast-paced, customer-facing environments without slowing down product development. These organizations typically operate with high deployment velocity and complex microservice architectures, making traditional CVE management, such as manual patching and compliance tracking, an ongoing drain on engineering resources. By providing pre-hardened, zero-CVE container images, Chainguard removes the burden of continuous vulnerability triage and image maintenance. This allows development teams to focus on delivering new features and experiences quickly, while ensuring security standards are met by default. In an industry where brand reputation and customer trust are tightly linked to perceived security, Chainguard gives companies the confidence to innovate rapidly without compromising their risk posture or operational efficiency

Financial Services

Value Unlocked for Financial Services Organizations

Financial Services customers increased ROI by unlocking revenue and reducing risk



Financial Services organizations quickly realize substantial cost savings and revenue growth by addressing CVE management and improving container security practices. The value unlocked for these companies averaged $14 million, driven by $5.5 million in decreased risk and $4.9 million in increased revenue on average. These numbers stemmed from improved vulnerability management, faster remediation, and reduced exposure to compliance penalties and customer churn.

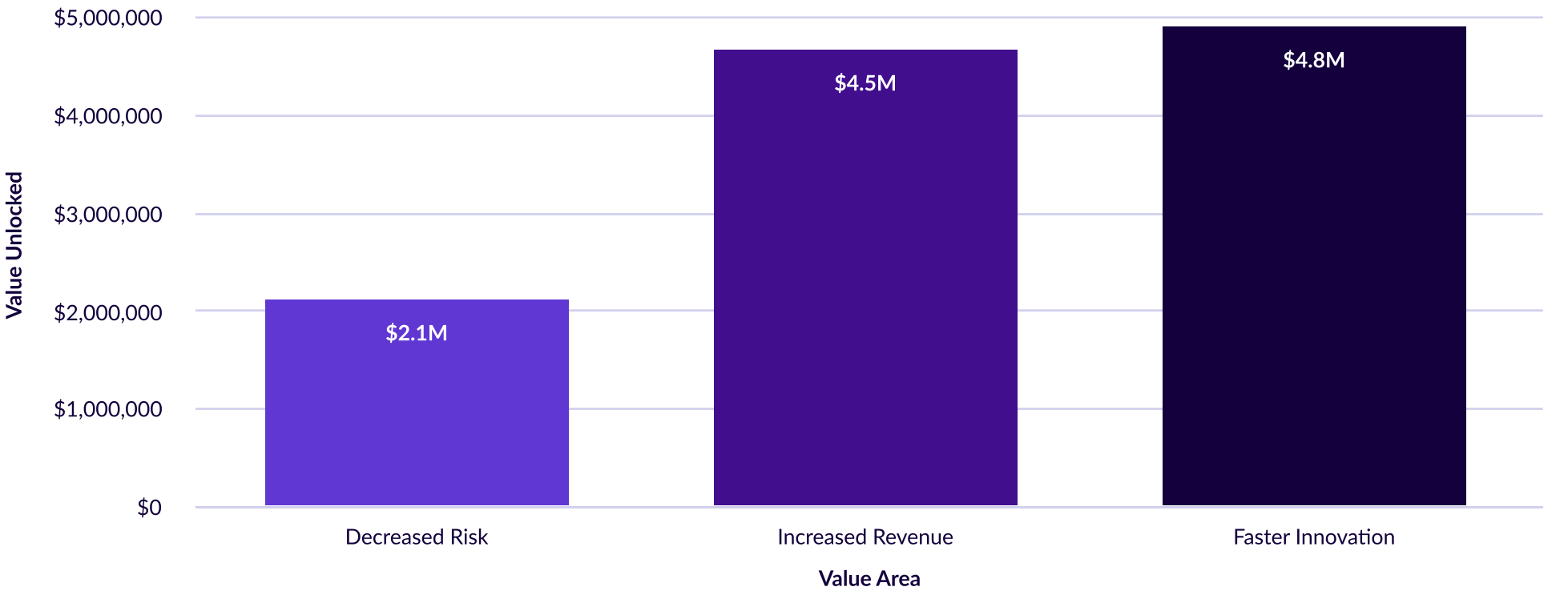
The need for CVE management comes from internal and external audiences in the Financial Services industry. These organizations operate in highly-regulated environments, where the cost saving measures mentioned earlier in the report greatly reduce the businesses' overall risk profiles. Security-focused organizations in this industry often have internal security mandates to reduce risk and keep sensitive customer data safe. This reduction in risk also opens up the opportunity for more revenue, and unlocks new markets via compliance frameworks like FedRAMP and PCI-DSS.

Chainguard Containers support financial services organizations in meeting rigorous security and compliance demands without diverting valuable engineering resources from core initiatives. These organizations face strict requirements around vulnerability remediation, audit readiness, and data protection. Traditional in-house CVE management often leads to fragmented workflows, compliance gaps, and significant overhead across engineering and security teams. Chainguard's zero-CVE container images eliminate these challenges by delivering secure, compliant baselines out of the box, simplifying adherence to compliance standards like PCI-DSS. This proactive approach not only strengthens security posture, but also reduces operational friction, allowing teams to focus on delivering secure financial products and services with greater speed and reliability.

Technology

Value Unlocked for Technology Organizations

Technology customers benefitted from faster innovation, helping lead to increased revenue



Technology companies are realizing strong value from investing in secure software supply chains, with average total documented benefits of $9 million. The primary driver of this value is faster innovation, accounting for $4.8 million, followed closely by $4.6 million in increased revenue. One customer in the cloud services space, for example, unlocked $4.9 million by accelerating feature delivery to its B2B customer base. Similarly, customers working on FedRAMP certification saw the greatest revenue impact, at an average of $5.8 million, by accessing highly regulated and security-conscious markets, enabling them to expand their reach and increase deal sizes.

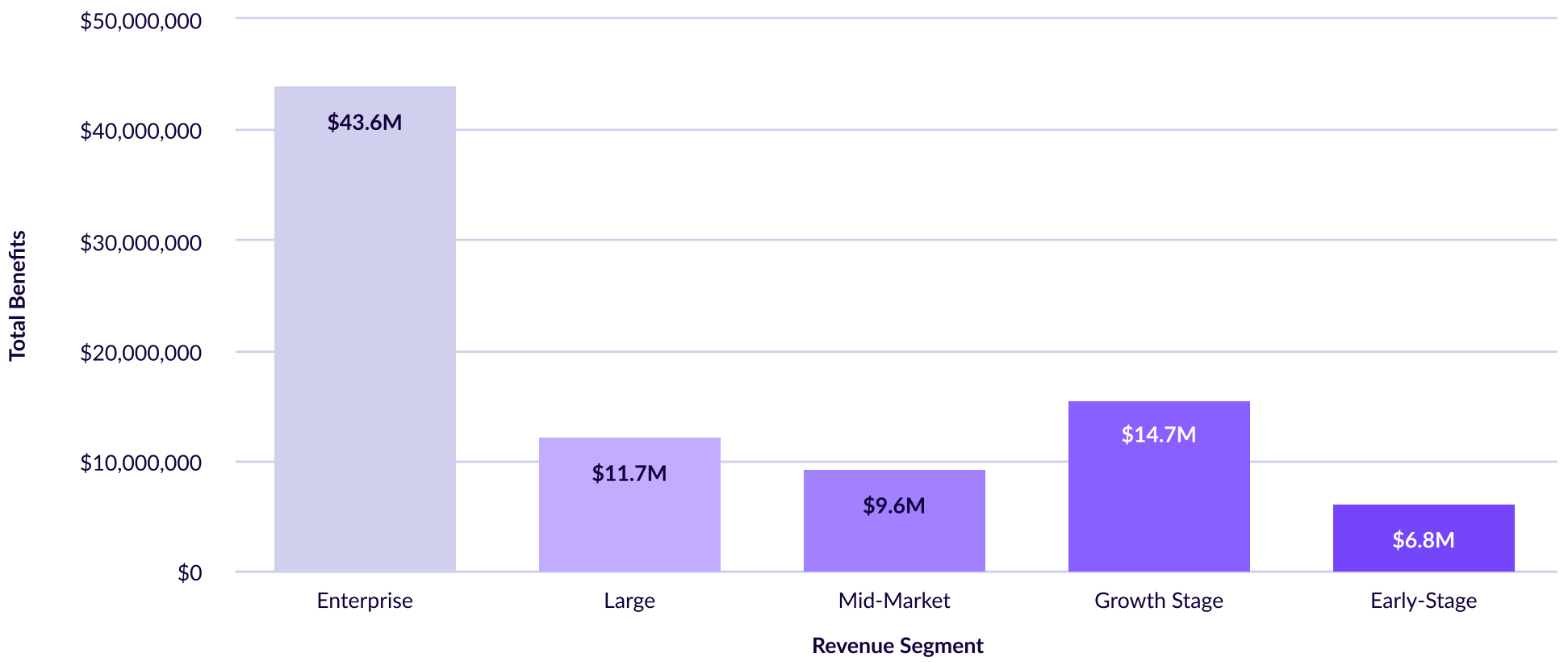
Outsourcing CVE management frees up engineering resources and reduces the overhead associated with security operations, allowing technology companies to focus more on core product innovation while maintaining a trusted security posture. This led to the increased revenue and faster innovation numbers, but it also contributes to reduced risk, as engineers can focus on building from a secure base, instead of patching in security after the products have been built.

Chainguard Containers help technology companies accelerate product development while maintaining a strong security foundation across their software supply chains. Tech companies often move quickly, delivering infrastructure, platforms, or applications to other security-conscious businesses. Managing CVEs manually can slow innovation, increase engineering toil, and introduce risk, especially when compliance requirements like FedRAMP are in play. Chainguard addresses these pain points by providing zero-CVE, hardened container images that integrate seamlessly into DevOps workflows. This allows tech teams to focus on building and scaling products without being bogged down by vulnerability triage, patching cycles, or compliance overhead—ensuring they meet customer expectations for speed and security simultaneously.

Value Unlocked by Revenue Segment

We also broke out the value Chainguard Containers customers unlocked based on company size, starting again with the overall total benefits:

Overall Value Unlocked by Revenue Segment



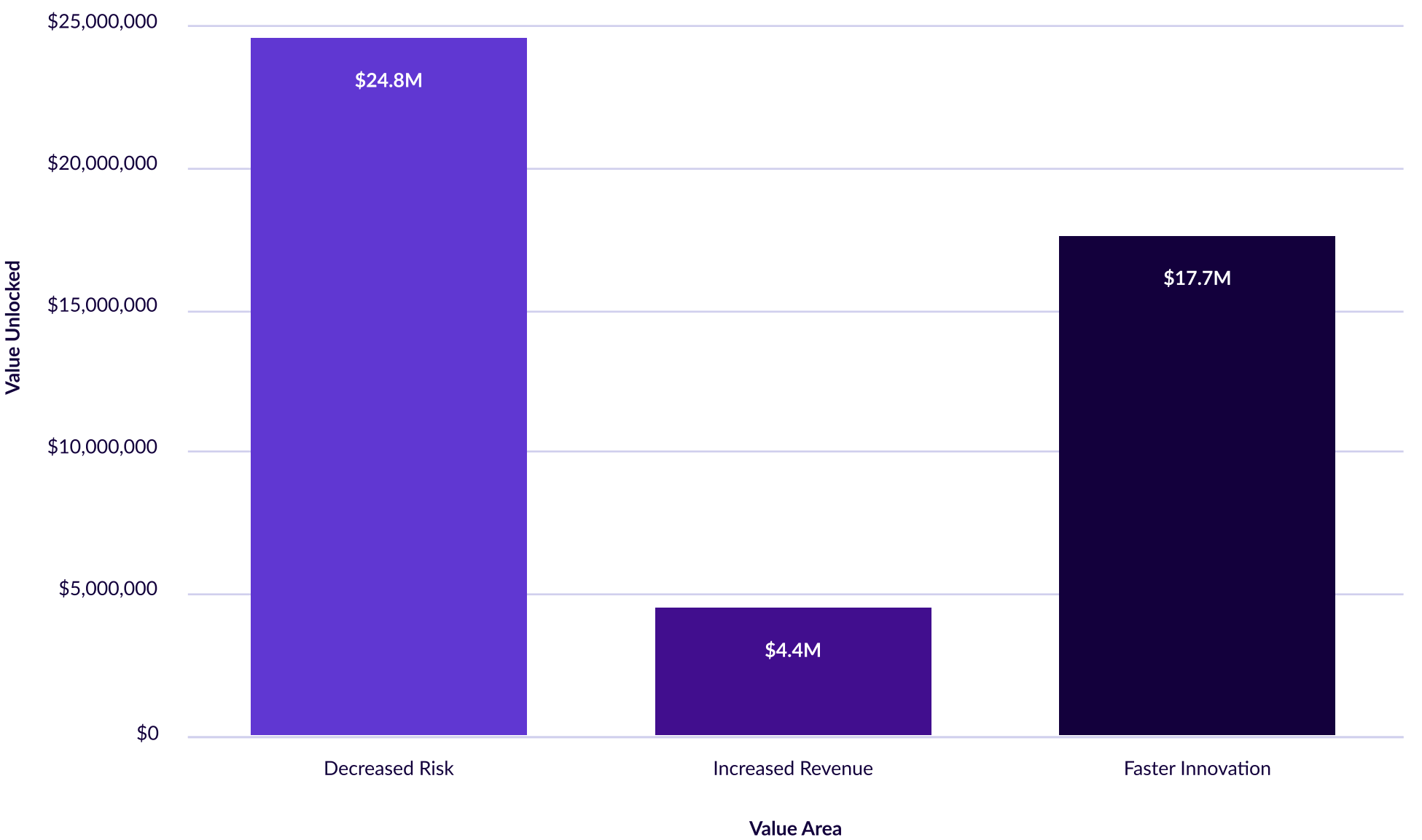
As detailed earlier in the report, organizations that utilize more container images, and thus dedicate more headcount to CVE management when choosing to do it in-house, see the most value when outsourcing the task. Enterprise organizations almost always have a large container footprint, and managing CVEs in the amount of containers present in a typical enterprise environment is a major challenge. This led to enterprise organizations seeing massive value in outsourcing CVE management.

For smaller organizations, there are often fewer container images, but also less headcount to manage them. Engineering teams at Early-Stage and Growth-Stage organizations must dedicate a large portion of their time to developing and improving products in order to grow the business. When they are forced to spend time remediating CVEs and hardening containers, they are spending less time on tasks that move the needle for the business during critical early stages. These organizations also see immense value in outsourcing CVE management tasks.

Enterprise ($10 billion+)

Value Unlocked for Enterprise Organizations

Enterprise customers unlock an average of almost $25 million by decreasing risk

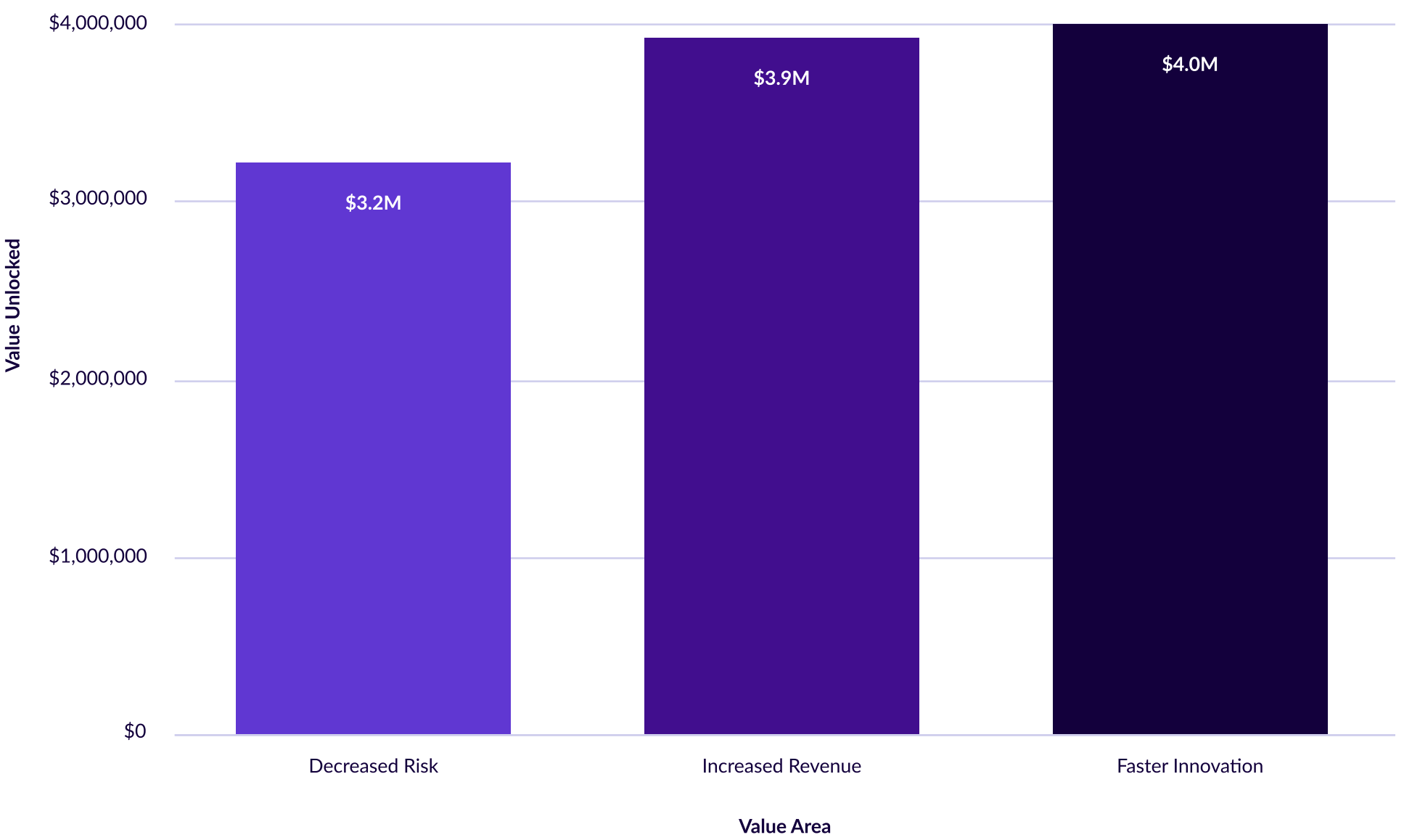


Unsurprisingly, enterprise organizations receive the highest total value unlocked for outsourcing CVE management at over $43 million on average, with the highest average benefits in the decreased risk ($25 million) and faster innovation ($18 million) cost areas. While avoiding things like data breaches and reputation risk is important for all organizations, it's essential for large enterprises, where the overall cost of customer churn in the event of a data breach or security issue is exponentially higher compared to other revenue segments. Some of these organizations are also in highly regulated industries, where compliance with frameworks like HIPAA, PCI-DSS, and others is required to avoid fines and other penalties in the event of a security incident.

Large ($1 billion–$10 billion)

Value Unlocked for Large Organizations

Large customers unlock around $4 million on average from both increased revenue and faster innovation

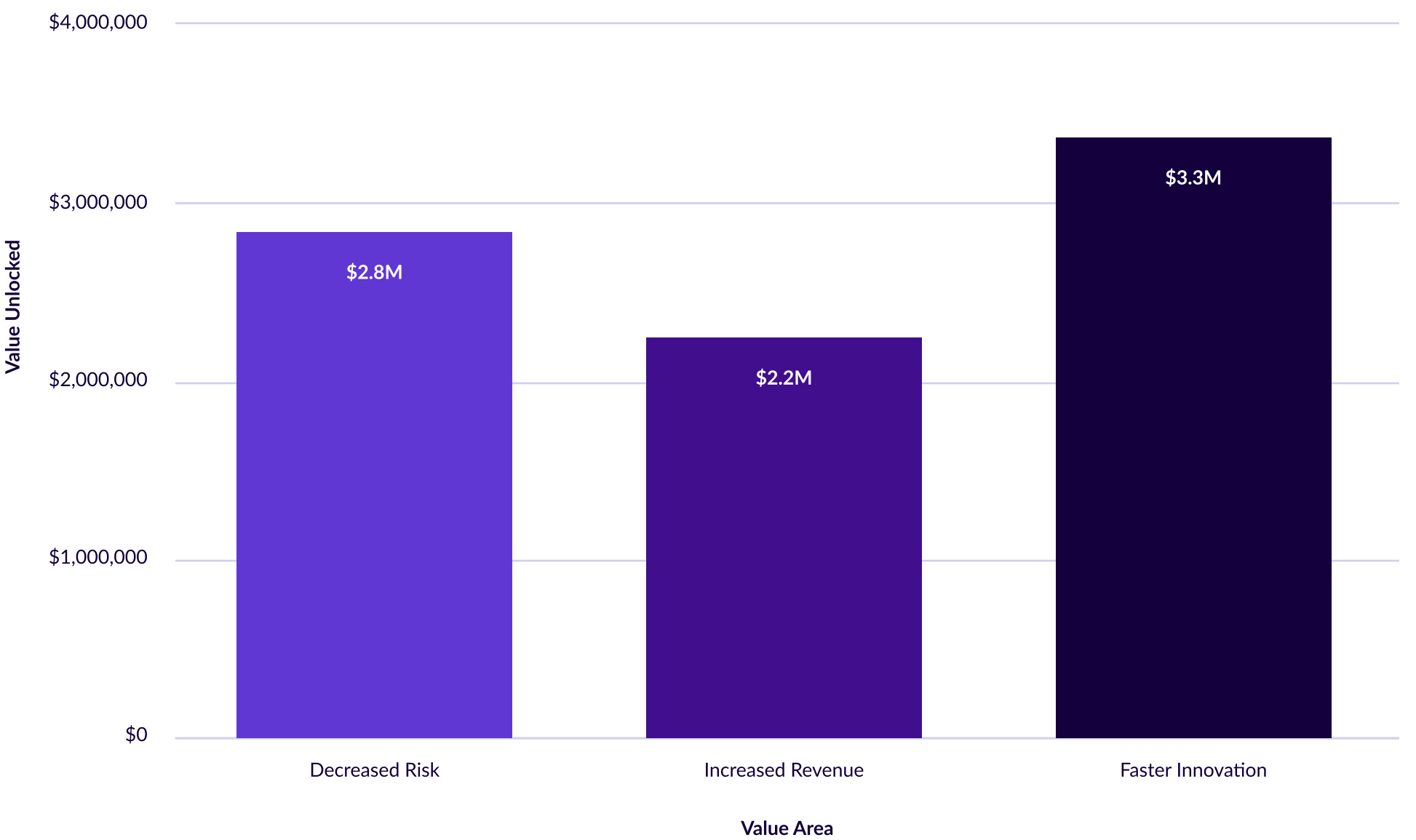


Large enterprises averaged approximately $12 million in annual benefits, showing balanced value across all categories. Average benefits of $4.1 million from faster innovation and $4 million from increased revenue dominated benefits for Large enterprises, driven by Chainguard's impact on accelerating software delivery and enabling revenue-generating releases. The average decreased risk ($3.3 million) was also significant due to compliance improvements.

Mid-Market ($500 million–$1 billion)

Value Unlocked for Mid-Market Organizations

Mid-market customers get balanced average benefits in increased revenue, faster innovation, and decreased risk

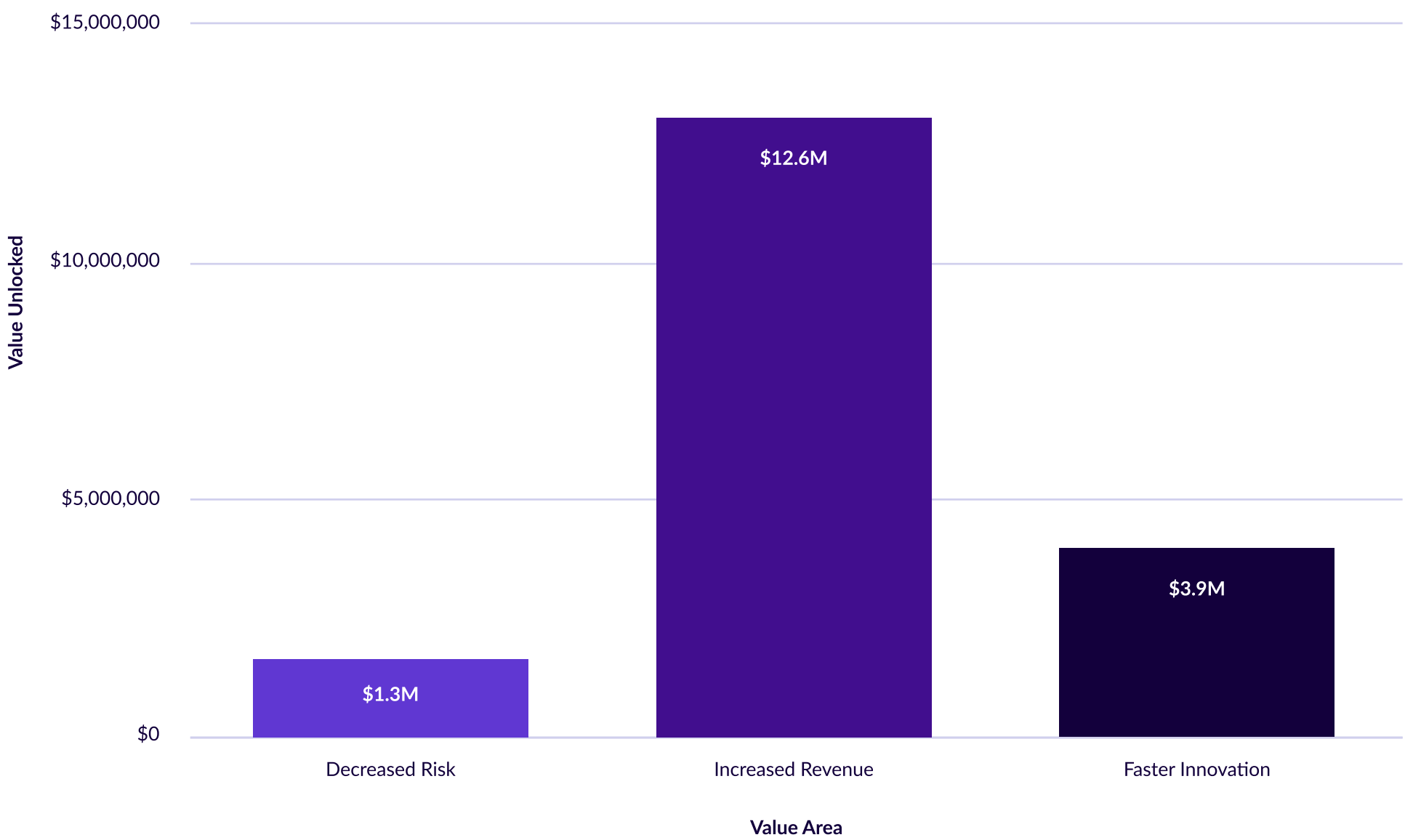


Mid-market companies averaged $9.6 million in annual benefits, with strong contributions from innovation gains ($3.3 million) and cost savings ($2.9 million). By automating patching and vulnerability response, lean teams achieved secure scalability. This accelerated innovation is driving an average of $2.3 million in increased revenue and market share growth. Furthermore, an average decrease of $2.8 million in risk reflected enhanced security postures, reducing customer escalations as these organizations ventured into more sensitive markets.

Growth-Stage ($100 million–$500 million)

Value Unlocked for Growth-Stage Organizations

Growth-stage customers increased revenue by an average of $12 million by unlocking new security-conscious customers

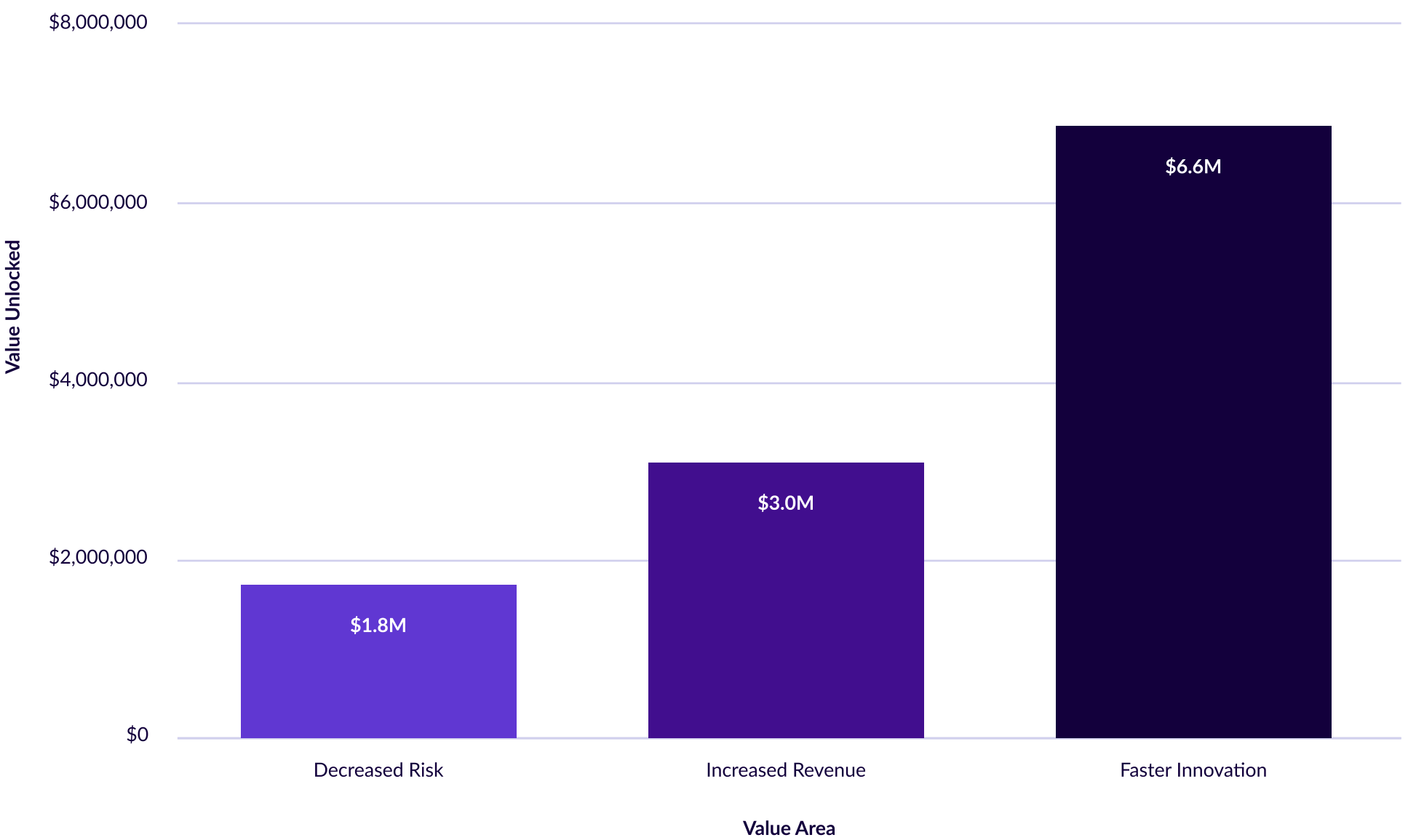


Growth-stage firms saw over $14 million in average value unlocked annually, with higher revenue contributing an average of $12 million in benefits. Chainguard helped with revenue growth by unblocking enterprise deals with hardened, compliant container images. Growth-stage customers benefited from an average of $3.9 million through faster feature and product launches. Gains in faster innovation and considerable cost savings demonstrated enhanced productivity and greater headcount efficiency. Benefits from risk reduction also accounted for an average of $1.3 million annually, reflecting early-stage mitigation of audit failures and critical vulnerabilities as they prepared for regulatory scrutiny.

Early-Stage (<$100 million)

Value Unlocked for Early-Stage Organizations

Early-stage customers benefited from an average of over $6 million in faster innovation to roll out new products and services



Early-stage customers saw $6.8 million in average total value unlocked. These organizations reaped the benefits of faster innovation, with an average return on investment of $6.6 million. They also unlocked an average of $3 million from revenue acceleration. These startups used Chainguard to ship faster, reduce engineering toil, and win design partners by meeting enterprise security standards.

Reducing Your Cost of CVEs with Chainguard Containers

As demonstrated across both industry and revenue segments, CVE management imposes measurable costs on organizations of all sizes. These costs are not always immediately visible on a balance sheet, but they manifest in missed compliance deadlines, reallocated engineering cycles, delayed product releases, and lost business opportunities. Outsourcing CVE management using a solution like Chainguard Containers can lead to serious, tangible return on investment.

Organizations saw this return on investment come to life in several of the areas above. For organizations in highly-regulated industries like Healthcare, Financial Services, and Telecom, Chainguard Containers is the perfect solution to not only reduce risk by removing CVEs in environments where sensitive data must be protected, but also to help these companies unlock new markets by accelerating compliance towards frameworks like HIPAA, PCI DSS, and FedRAMP.

On average, Chainguard customers saw the following returns on investment after transitioning from in-house CVE Management:

- $1.9 million per year of cost savings
- $5 million per year of increased revenue
- $9.18 million per year in faster innovation
- $10.98 million per year in decreased risk

Chainguard Containers is a future-proof solution engineered to eliminate the operational and strategic overhead of CVE management. Powered by Chainguard OS, Chainguard's bootstrapped Linux distro, and supported by the Chainguard Factory, our automation and build system, Chainguard Containers are rebuilt daily from upstream source code and are ready to be deployed in your environment with zero CVEs. We designed these container images to help organizations avoid the resource-intensive work of image hardening, streamline compliance, and reallocate engineering time to product development and innovation. This allows engineering teams to focus on the future and do what they love to do: build world-class products and solutions.

The data presented in this report is grounded in real outcomes from Chainguard customers across sectors and of every size. These organizations adopted Chainguard Containers to reduce security overhead, meet compliance requirements more efficiently, and accelerate release velocity. And many of these organizations are realizing massive returns on investment quickly, with customers feeling the effects within weeks or months of initial onboarding.

> **"Our partnership with Chainguard enabled us to meet or exceed the rigorous standards required in highly regulated industries and government sectors where we serve our customers. By reducing the burden of patching and hardening associated with managing supply chain risks, we can increase our developers' focus on driving innovation in support of our customers' missions."**
>
> Andrew Cunje, CISO at Appian

To hear more about other customers' experiences with Chainguard, check out our customer stories. And if you are interested in reducing the cost of CVE management at your organization, talk to an expert today.