



TRUEFORT™

+1 201 766 2023 | sales@truefort.com


[TRUEFORT.COM](https://truefort.com)

THE ROI OF MICROSEGMENTATION



We live in a time where cybersecurity threats are rapidly evolving, and businesses need agile, scalable, and efficient methods to protect their IT infrastructure. Microsegmentation, an advanced security strategy, is a leading best-practice solution to counteract modern threats.

But beyond the enhanced security, what is the return on investment (ROI) that businesses can expect from implementing microsegmentation? This document will look deep into the tangible and intangible benefits of adopting this innovative approach.



By 2026, 60% of enterprises working toward Zero Trust architecture will use more than one deployment form of microsegmentation, which is up from less than 5% in 2023.

- GARTNER MARKET GUIDE TO MICROSEGMENTATION



Understanding Microsegmentation

Before calculating the ROI of microsegmentation, it's imperative to grasp its fundamental mechanics and how it diverges from traditional security paradigms. Traditional security models often rely on a perimeter-focused approach, using firewalls, intrusion detection systems, and VPNs to create a fortified boundary around the network. These approaches are increasingly being circumvented by sophisticated threat actors who gain access to a network and, once inside, exploit its "flat" nature. In contrast to these foundational mechanisms, microsegmentation is a security technique that creates secure zones within data centers and cloud environments. This granular approach allows organizations to isolate workloads from one another and secure them individually, thereby creating multiple 'mini-perimeters' within the network. Here's are some of the ways in which microsegmentation provides superior network security:

- ▶ **Lateral Movement:** Traditional perimeter-focused security strategies are often ill-equipped to prevent lateral movement within the network. Once an attacker breaches the outer defenses, they can often traverse the network with ease. Microsegmentation halts this lateral movement by enforcing granular security policies at the workload or application level.
- ▶ **Zero-Day Resilience:** Microsegmentation is particularly effective against zero-day vulnerabilities. By establishing a real-time benchmark of approved activity and logging any deviations, it provides a robust defense against unknown threats that may bypass traditional security measures.
- ▶ **Policy Enforcement:** Traditional security models often rely on static policies that are cumbersome to update. Microsegmentation allows for dynamic policy enforcement, adapting in real-time to changes in the network topology or threat landscape. This ensures that security measures are always aligned with the current state of the network, reducing the attack surface dynamically.

When considering these key differentiators, microsegmentation's tremendous value becomes evident. Effective microsegmentation establishes a real-time benchmark of approved activity, logging any deviation for immediate action. It is one of the most effective remedies against zero-day attacks and unknown factors behind cyberattacks, offering a more agile, scalable, and effective approach to securing modern IT infrastructures.

Direct Cost Savings from Microsegmentation

Cybersecurity threats are not only evolving; they are proliferating and the risks to your organization are expanding accordingly. While the primary objective of microsegmentation is to fortify your organization's security posture, its financial benefits are equally compelling. Microsegmentation is a financially prudent choice in several ways:

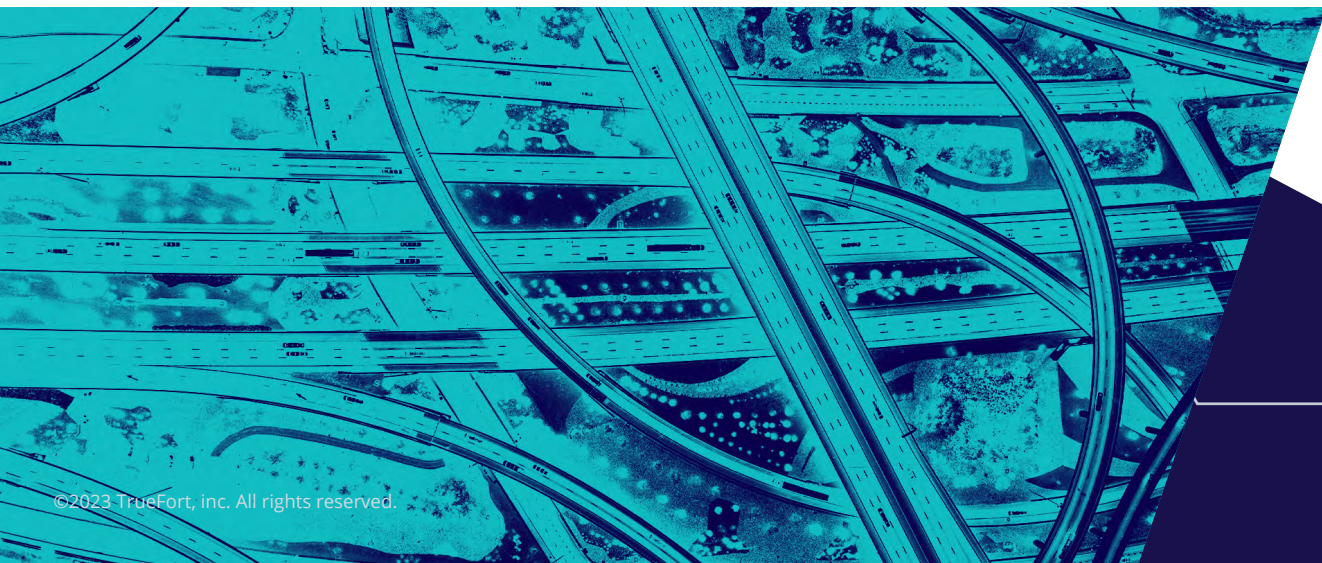
- ▶ **Reduced Attack Surface:** By limiting unnecessary communication between workloads, the attack surface dramatically reduces. Data breaches cost US companies an average of \$9.44B last year. Microsegmentation can prevent potential breaches, saving organizations the exorbitant costs associated with data leaks and system downtimes.
- ▶ **Infrastructure Savings:** One recent study concluded that the average company spends 7.5% of revenue on IT. Microsegmentation can be implemented using software, eliminating the need for multiple hardware appliances and dozens of firewalls. This results in direct savings on procurement, maintenance, and operational costs, plus allows for more efficient use of infrastructure resources, leading to savings on hardware and scaling costs.
- ▶ **Decreased Appliance Inventory:** Almost 20% of IT budgets – 1.5% of annual revenue – is dedicated to hardware. Microsegmentation allows for granular control over network traffic within a data center or cloud environment, reducing the reliance on traditional perimeter firewalls. By segmenting traffic at a more refined level, organizations can deploy fewer physical firewall appliances, leading to reduced hardware, licensing, and maintenance costs. Furthermore, as traffic is regulated more efficiently within the network, there's less need for costly overprovisioning of firewall resources.
- ▶ **Streamlined Security:** Application Ringfencing with microsegmentation makes security more efficient by identifying and isolating critical assets, reducing the impact of security incidents, and reducing the need for time-consuming and costly operations.
- ▶ **Reduced Network Maintenance Costs:** Traditional, perimeter-based network security architectures can be complex and expensive to maintain. Microsegmentation simplifies the security architecture from a centralized platform, which reduces extensive management costs.
- ▶ **Lowered Incident Response Costs:** Faster detection and containment of threats mean less money spent on incident response and remediation. Avoid regulatory fines by meeting PCI DSS (and other) standards and cyber insurance requirements.

Enhancing Compliance and Reducing Fines

Meeting numerous and complex regulatory requirements is a critical aspect of modern risk management. Non-compliance can result in hefty fines and reputational damage that impacts customer trust and market position. Microsegmentation mitigates the risks associated with non-compliance. It is a robust tool that ensures your organization meets stringent data protection and privacy standards in several ways:

- ▶ **Data Protection:** Ensures that sensitive data, whether it's personal data (GDPR) or payment card information (PCI-DSS), is isolated and protected.
- ▶ **Audit Efficiency and Readiness:** Simplified compliance reporting and real-time monitoring streamline the audit process. Organizations are always armed with the evidence they need, reducing the risk of non-compliance penalties and human error.
- ▶ **Third-Party Risk Mitigation:** By extending microsegmentation policies to third-party integrations, organizations can better manage the risks associated with vendor relationships, a growing concern in compliance frameworks.
- ▶ **Dynamic Policy Adaptation:** Microsegmentation enables dynamic adaptation of security policies to meet evolving regulatory requirements, ensuring that compliance is not a one-time event but a continuous process.

Microsegmentation enhances legislative compliance by providing granular security controls to protect sensitive data, ensuring adherence to industry-specific data protection and privacy regulations.



Many compliance standards require robust security controls. Microsegmentation can help organizations meet these requirements more efficiently, potentially reducing the costs of audits and penalties for non-compliance. PCI DSS 4.0, for example, indicates that while segmentation is not mandatory, if a company cannot prove it has effectively segmented its data center or cloud, then the entire system must be evaluated during PCI assessments. This broader assessment can significantly increase any organization's quarterly compliance expenditure.

- ▶ The average cost of a data breach is projected to reach \$4.2 million in 2023
- *IBM*
- ▶ Over 60% of businesses that experience a cyber-attack close their doors within six months
- *National Cyber Security Alliance*
- ▶ In 2023, it is estimated that cybercrime will cost businesses \$10.5 trillion annually
- *Cybersecurity Ventures*
- ▶ 53% of companies have experienced a third-party data breach in the past year
- *Ponemon Institute*



Intangible Benefits and Their Financial Impact

While the direct cost savings of microsegmentation are quantifiable, the strategy also offers a range of intangible benefits that contribute to an organization's financial health. These benefits have a significant impact on long-term profitability and market standing even though you'll never see them on a balance sheet.

- ▶ **Reputation:** A single data breach can significantly damage a company's reputation. With enhanced security from microsegmentation, organizations can bolster customer trust, potentially leading to increased customer retention and acquisition.
- ▶ **Operational Efficiency:** By understanding specific communication pathways, organizations can ensure that applications and workloads operate more efficiently. This can indirectly lead to increased productivity and better service delivery when misconfigurations and other unnecessary behavior is remedied.
- ▶ **Future-Proofing:** As the organization grows and evolves, so does its network. Microsegmentation offers a flexible, scalable approach to network security that can adapt without major overhauls, avoiding future costs.

Putting Numbers to the ROI

While the direct cost savings of microsegmentation are quantifiable, the strategy also offers a range of intangible benefits that contribute to an organization's financial health. These benefits have a significant impact on long-term profitability and market standing even though you'll never see them on a balance sheet.

- ▶ **Cost Avoidance:** Calculate the potential costs associated with data breaches, non-compliance fines, and hardware procurement. These represent the costs you potentially avoid by implementing microsegmentation.
- ▶ **Operational Savings:** Consider the time saved by IT teams in not having to manage multiple hardware appliances or recover from breaches. Translate this time into monetary values based on average salaries and operational costs.
- ▶ **Revenue Protection:** Consider the potential loss in customers or revenue from a damaged reputation due to a security incident. By enhancing security through microsegmentation, this revenue is protected.

Combining these factors provides a holistic view of the ROI of microsegmentation.

Real-World ROI: Case Studies

- **Case Study 1:** A Fortune 100 financial institution, after adopting microsegmentation, thwarted advanced persistent threats, saving potential breach costs estimated at \$5 million. Additionally, they reported a 40% reduction in time spent on compliance reporting.
- **Case Study 2:** A household name and e-commerce giant, leveraging microsegmentation, reduced its infrastructure costs by 30%. Their enhanced security posture also contributed to a 20% increase in customer trust, translating to increased sales.
- **Case Study 3:** A Fortune 500 manufacturing company achieved immediate application visibility, granular dependency mapping, and support for their legacy environments – all while still in the proof of concept phase of their microsegmentation implementation.

What our customers say:

- “This is one of the first times I’ve had a short visit because the evidence was all just ready.”
- Auditor for TrueFort banking client
- “This does even more than we thought.”
- Security architect protecting a top 5 US bank
- “Oh my god! We need to get this installed everywhere right away.”
- Cybersecurity lead for national energy co.

Implementing Microsegmentation: Considerations for Maximum ROI

Achieving maximum ROI from microsegmentation requires strategic approach that aligns with your organizational goals and risk profiles. Below are key areas to consider to ensure you extract the most value from your new security initiative:

- ▶ **Phased Implementation:** Begin by segmenting the most mission-critical applications to see immediate security and compliance benefits. Expand gradually. Proceed to less critical parts of the network after you've assessed the impact of your microsegmentation implementation and smoothed out any issues.
- ▶ **Ongoing Monitoring and Continuous Improvement:** The threat landscape is ever-changing. Your microsegmentation policies should adapt in real-time to these changes. Establish mechanisms for frequent feedback from security operations centers (SOCs) and incident response teams and use that data to fine-tune your approach.
- ▶ **Employee Training:** Ensure that all stakeholders, from IT staff to C-suite executives, understand the benefits and methods of microsegmentation. Invest in training programs that equip all department with the skills needed to optimize microsegmentation effectively.
- ▶ **Cost-Benefit Analysis:** Account for the initial investment in software and training. Weigh these expenses against the long-term savings from reduced security incidents, lower compliance costs, and optimized infrastructure.
- ▶ **Vendor Selection:** Choose a vendor whose solution offers the features most relevant to your specific needs. Engage in the due diligence necessary to manage the risk of using a third party to provide microsegmentation.
- ▶ **Scalability:** Ensure the solution you select can scale with your organization's growth and evolving security requirements.

In Conclusion

Microsegmentation is not just a security strategy; it's an investment in your organization's future. As cyber threats grow in complexity, the ROI from a fortified security posture, enhanced compliance, and operational efficiency will only increase.

The question of whether companies should invest in microsegmentation has been resolved with a resounding YES across industries including finance, manufacturing, retail and more. All that's left to wonder about is how much longer you're going to put it off – and what might happen while you wait.

Learn how TrueFort can enable zero trust application for your organization through microsegmentation and other application-centric controls. [Request a demo](#) today.

ABOUT TRUEFORT

TrueFort® Platform puts you in control of lateral movement across the data center and cloud. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Learn how TrueFort can enable zero trust application protection for your organization through microsegmentation and other application-centric controls.

Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

For more information, visit truefort.com and follow us on [Twitter](#) and [LinkedIn](#).



TRUEFORT™

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

