TRUEFORT®

SOLUTION BRIEF

Microsegmentation

A Strategic Essential and Superior ROI vs Standard Network Segmentation

Traditional network infrastructures falter against the sophisticated dynamics of modern cyber threats, and modern organizations are being forced to reconsider their security strategies. The concept of network segmentation, once a cornerstone of digital defense, is now superseded by its more advanced counterpart: microsegmentation.

Microsegmentation presents a more straightforward approach to isolating critical data, essential in complex cybersecurity environments.

Decoding Microsegmentation

Microsegmentation divides a network into secure, distinct segments down to the individual workload level. It contrasts sharply with traditional models by offering protection beyond the network's IP address-based hardware. This method ensures software-defined policies and controls for any size segment, leading to enhanced management and security.

The Advantages of Microsegmentation

- **Enhanced Security Posture:** Microsegmentation's fine-grained control over network traffic significantly reduces the attack surface. It impedes the lateral movement of attackers, providing robust protection against zero-day attacks and aiding in breach containment.
- **Significant ROI:** By reducing the need for managing extensive internal firewalls, organizations significantly reduce the associated TCO. Previously handled with manual rules, automation leads to direct operational cost savings. Microsegmentation reduces both attack surface and response times while easing network security operations.
- **Improved Compliance Management:** Microsegmentation facilitates compliance with regulatory standards and streamlines reporting, ensuring data is protected in isolated zones.

- **30%** of organizations have more than 100 internal firewalls set up on their network. (Statistica)
- The average single firewall costs approximately **$8,250** (between $1,500 and $15,000) including product cost, installation fee, and subscription. (Forrester)
- By 2026, **60%** of enterprises aiming for a zero-trust architecture will adopt multiple forms of microsegmentation, a significant leap from less than **5%** in 2023. (Gartner)

- **Operational Efficiency and Flexibility:** Automated and dynamic policy enforcement reduces complexity. Its scalability and adaptability make it suitable for various environments, including cloud-based enterprise applications.
- **Enhanced Incident Response:** Rapid threat isolation and anomaly detection become more efficient, improving overall threat management.

Comparing Approaches

- **Microsegmentation vs. Inaction:** Neglecting to enhance traditional network security methods increases manual efforts over fivefold, whereas microsegmentation provides an automated defense mechanism.
- **Microsegmentation vs. Traditional Infrastructure:** While leveraging existing infrastructure may seem cost-effective, it lacks the business context and flexibility of microsegmentation.

"This is a total eye-opener. Your product capabilities are massively understated."

CISO, Finacial Services Industry

"We need to get this installed everywhere, right away!"

Cybersecurity lead and TrueFort customer

Regulatory Compliance and the Microsegmentation Mandate

Microsegmentation's approach aligns with modern compliance mandates like NIST, HIPAA, and PCI DSS 4.0, demanding more stringent data protection and access controls. Its precise controls enable organizations to meet these requirements effectively, providing clearer audit trails and data flow mapping.

A Strategic Imperative

As network complexity increases, a granular security approach will become indispensable in network security strategies, offering unparalleled benefits over traditional methods.

The adoption of microsegmentation is not just beneficial but essential in safeguarding against the evolving landscape of cybersecurity threats, and modern security platforms have eased implementation challenges, making the microsegmentation transition smooth and more effective.

In the quest to protect critical business assets, embracing microsegmentation is a strategic imperative for contemporary organizations.

ABOUT TRUEFORT

TrueFort® Platform puts you in control of lateral movement across the data center and cloud, protecting service accounts and against zero-day threats. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. 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 LinkedIn.

TRUEFORT®

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

+1 201 766 2023
sales@truefort.com