TRUEFORT®

SOLUTION BRIEF

TrueFort® Platform: Protecting Cloud Workloads

Ensuring a safe and visible cloud experience across the entire org.

As organizations continue to transition towards a cloud-centric world, the stakes are higher than ever to ensure a resilient cybersecurity posture. Protecting cloud workloads, particularly against ransomware, data exfiltration, and lateral movement attacks, is a critical task for organizations today.

This brief will discuss how the TrueFort Platform secures cloud workloads, reduces risks, and fosters a secure cloud environment.

Application-Centric Segmentation: Building Robust Defense

TrueFort Platform focuses on application-centric segmentation, enforcing workload segmentation that underpins a solid defense against lateral movement within your network infrastructure.

By making use of this model, enterprises can:

- Develop a robust layer of defense, preventing malware from hopping between workloads.
- Protect against ransomware attacks by curbing the spread of infection within the network, while the continuous monitoring workload behavior to swiftly identify and respond to unusual activities.
- Halt data exfiltration attempts by applying strict segmentation rules, preventing unauthorized access and data movement.

Application-centric segmentation also supports SOC teams by providing clear historical forensics and real-time action, thus helping organizations respond rapidly and decisively to potential threats.

- The proportion of people hybrid working, using organizational cloud services, has risen **10%** in the last **12** months.
  (c/o gov.org)
- Data residency across cloud services creates complex choices in regard to balancing business needs against growing risks to provide adequate data security and compliance
  (c/o Gartner)
- As of 2022, over **60%** of all corporate data is stored in the cloud.
  (c/o Statistica)

Trusted Workload Profiles: Continuous Monitoring for Unusual Activities

A core feature of the TrueFort Platform is its emphasis on trusted workload profiles. By establishing and monitoring each workload's 'normal' behavior, TrueFort continuously checks for drift in this behavior. Any activities outside the expected norm are immediately flagged, ensuring that potential threats are rapidly identified and mitigated.

Benefits of trusted workload profiles include:

- Reduced false positives by establishing and monitoring 'normal' behavior patterns.
- Real-time alerting (or blocking) of any activities outside of the expected norms.
- Enhancing your security team's situational awareness and ability to respond swiftly to threats.

Automated Segmentation Policies: Understanding and Managing Trust

Understanding, managing, and controlling trust around workloads is a complex but necessary task to protect against unknown risks that threaten sensitive data. The TrueFort Platform makes this task easier by offering automated segmentation policies.

TrueFort's automated segmentation policies:

- Simplify the process of managing trust around workloads.
- Proactively protect against risks that threaten sensitive data.
- Free up valuable time for your security team to focus on other critical tasks.

Least Privilege Access: Reducing Risk in Cloud Environments

TrueFort's approach to reducing risk in cloud environments involves leveraging learned behavior to create least privileged access policies. By adhering to the principle of least privilege - granting only the minimum access necessary for a task - TrueFort Platform minimizes potential attack vectors. This robust security practice reduces the risk of threat actors exploiting overly generous access permissions, protecting critical service accounts that are often unmonitored.

"I've never seen the noise of a cloud environment so clearly translated."

Cloud Network Eng,
Manufacturing Org.

"Nobody, and I mean NOBODY, else is doing this."

Dir. Sec. Eng, Top 5 Telecom

TrueFort and Kubernetes: A Seamless Partnership

TrueFort also provides a unique approach to securing Kubernetes, offering a comprehensive solution for container microsegmentation. By baselining the runtime behavior of containers, TrueFort can easily spot anomalies and allow for real-time response. This functionality is particularly important for organizations that heavily rely on containerized applications, making TrueFort an excellent choice for Kubernetes security.

One Comprehensive Platform

TrueFort Platform's complete suite of features offers a robust and effective approach to securing cloud workloads. Through application-centric segmentation, trusted workload profiles, automated segmentation policies, least privilege access, and Kubernetes security, TrueFort provides organizations with the tools necessary to ensure a secure cloud environment. TrueFort Platform's ability to detect and react to potential threats in real-time and its automated systems that simplify security management make it the best practice option for organizations looking to safeguard their cloud workloads.

ABOUT TRUEFORT

TrueFort 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. 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

TRUEFORT.COM