TRUEFORT™

E-BOOK

THE COMPREHENSIVE 2024 GUIDE TO Microsegmentation Solutions

+1 201 766 2023 | sales@truefort.com

TRUEFORT.COM

In an ever-changing digital landscape, enterprises – regardless of size – are constantly updating and modernizing their operations, be it in the cloud or within their own data centers. This evolution disrupts the traditional security perimeter, opening up new vulnerabilities that attackers are quick to target. To combat this, many organizations are adopting the zero trust framework. This methodology truly shines when security engineering and incident response teams can seamlessly monitor networks, workloads, devices, and user activities across all environments. Achieving such comprehensive visibility in both cloud and on-premises infrastructures requires advanced data collection and analytical efforts. This is where expert technologies, especially microsegmentation solutions, become indispensable.

Microsegmentation solutions are pivotal in providing the automation and capabilities essential for businesses aiming to integrate zero-trust seamlessly. These solutions empower security teams to:

- Streamline workload management across diverse environments, with emphasis on cloud and hybrid settings.
- Minimize potential attack surfaces and block the lateral spread of any intrusions, including elusive zero-day threats.
- Enhance rapid response mechanisms.
- Facilitate smooth cloud transitions by delineating acceptable application behaviors.
- Incorporate the principle of minimal access privilege into cloud systems.
- Offer instantaneous visibility and responses to suspect activities, while minimizing false alarms.
- Use adaptive automation to enforce security protocols per application, updating them as workload conditions evolve.
- Ensure adherence to regulatory norms and cloud-centric best practice guidelines.

Experience has shown us that successful early adoption of microsegmentation hinges on several critical capabilities. When searching for the ideal workload protection partners, organizations should prioritize solutions that encapsulate the following strengths:

- Precision in continuous application behavioral mapping.
- Advanced traffic analytics and visualization automation.
- Workload behavioral analytics.
- Compliance benchmarking as per CIS standards.
- Real-time management of incidents.
- Diligent file integrity surveillance.
- Comprehensive service account analytics.
- Enterprise-class reporting and custom dashboards.

Automated Application Behavioral Mapping

Before charting a microsegmentation blueprint or transitioning legacy applications to a cloud ecosystem, it's imperative for development, IT, and security teams to fully grasp each application's behavior and potential changes over time. Overlooking this detailed mapping can enfeeble necessary security controls or disrupt application performance. Yet, manual mapping, given today's intricate application networks, is both time-consuming and costly, with untrustworthy CMDBs serving as the perfect example.

Microsegmentation tools equipped with automated dependency mapping deliver results that are not only more cost-effective and swift but also far more accurate than traditional methods. Opt for solutions that adeptly identify relationships within and between applications, all the while offering real-time insights at account, network, and process layers across both legacy and modern cloud platforms. Such granularity and automation ensure a consolidated perspective, enabling security engineers, incident responders, and DevSecOps teams to navigate the application environment and prioritize security zones strategically.

Automated Traffic Analysis and Visualization

The foundation of an adept microsegmentation strategy is rooted in the meticulous mapping of applications and their interdependencies. But that's just the start. Insights from the Enterprise Strategy Group (ESG) emphasize that simply identifying and charting application links and traffic routes might not offer a holistic picture. Deep visibility into application processes and the identities linked with associated services can furnish vital context regarding application behaviors, crucial for pinpointing anomalies.

In your evaluation, gravitate towards microsegmentation tools capable of delivering dynamic, automated visualizations of application traffic – a consolidated view into real-time network communication. Such panoramic traffic visibility nullifies the need for compartmentalized visualization aids and concurrently monitors physical servers and cloud-based applications. This wealth of traffic information not only aids in designing robust rules and triggers but also thwarts CMDB drift and ensures security operations centers (SOCs) can apply a proactive security model that's agile enough to accommodate ever-changing scenarios. Moreover, centralizing traffic data streamlines the attack-neutralization process, cutting down the time needed to defend against and neutralize attacks.

Workload Behavior Analytics

As technological frameworks burgeon into the cloud and corporate workforces become increasingly dispersed, the volume of data navigating through systems skyrockets. This torrent of data can inadvertently camouflage malicious activities. Microsegmentation tools enriched with workload behavior analysis apply advanced machine learning algorithms, sifting through vast data pools to delineate patterns of trusted connections, communication streams, usage frequencies, and command executions at an operating system level.

Having a baseline of trustworthy behavioral patterns equips the microsegmentation tool to craft security profiles tailored to each application. This, in turn, allows for the auto-generation of segmentation policies that safeguard workloads without compromising their utility or functionality. An optimal microsegmentation tool should manifest this workload behavior as an extensive trust graph, furnishing vital data that can refine security tactics and simplify recovery efforts. Leveraging workload behavior within microsegmentation to empower a proactive security model aids in minimizing false alerts, channeling resources towards pressing events, and conserving time.

CIS Compliance Benchmarking

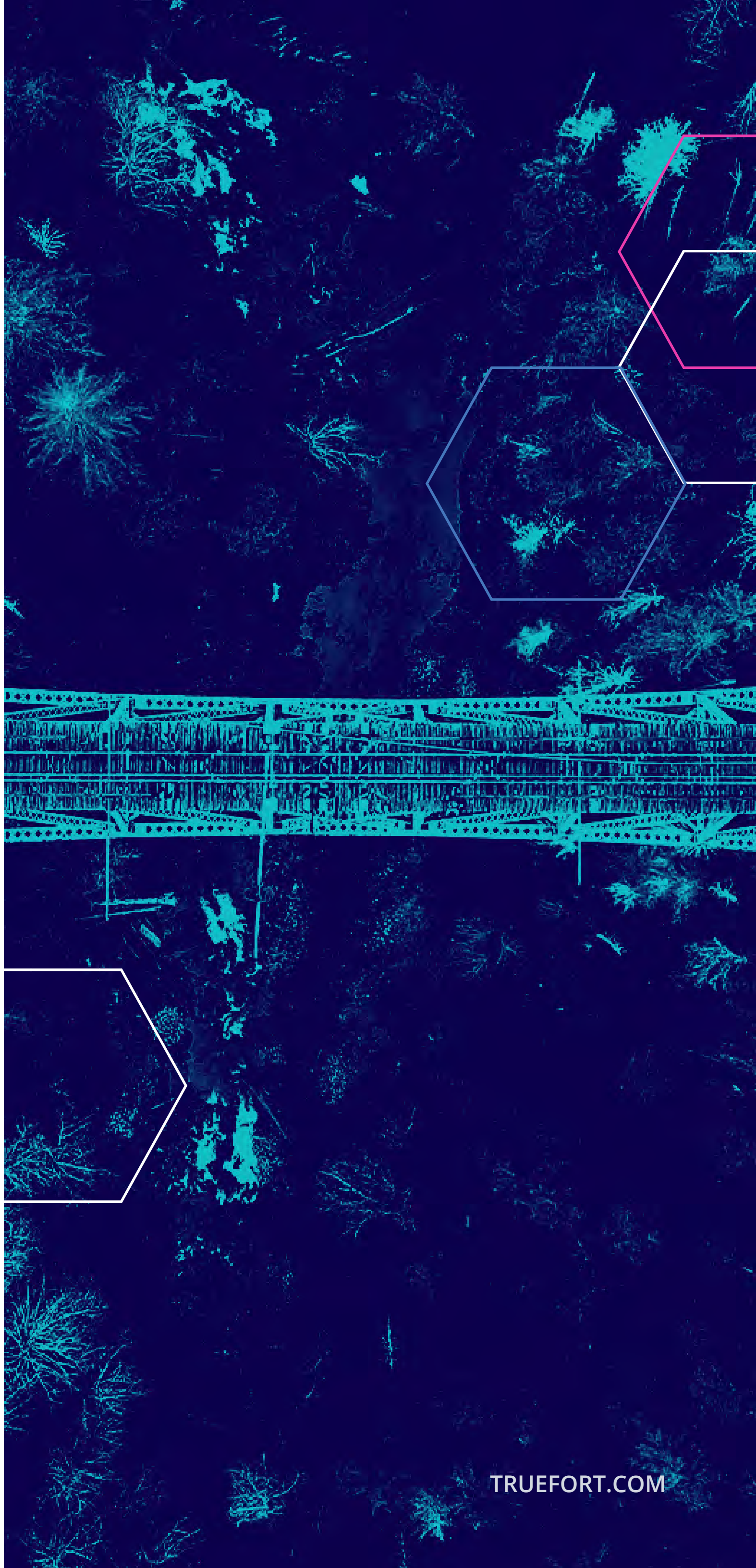
The majority of establishments are bound by contractual obligations to adhere to CIS best practices. Additionally, many superimpose their bespoke best practices over CIS recommendations to cater to specific organizational needs. Given CIS's stature as an esteemed industry benchmark, it's paramount for microsegmentation solutions to feature benchmark analysis ensuring that configuration policies are compliant across Windows, Linux, and UNIX systems.

Such benchmarking features slash the time and effort required to sustain secure rollouts and ideal system configurations. An added advantage would be solutions that alert teams of any deviations post-deployment, empowering DevSecOps teams to rectify them instantaneously. Prompt correction of configuration drift buttresses the security of dynamic hybrid ecosystems and ensures systems are perpetually audit-ready.

Real-Time Incident Management

With enterprises making a beeline for cloud-based applications, traditional firewalls and IP address-centric controls, once the bulwarks against threats, now fall short. Shielding the multifaceted hybrid landscape mandates instantaneous visibility coupled with an automated incident response – a domain where legacy SIEM and XDR tools falter. These older systems grapple with analyzing the colossal data output from cloud applications, and their static rules struggle to keep pace with the evolving threats in the cloud milieu.

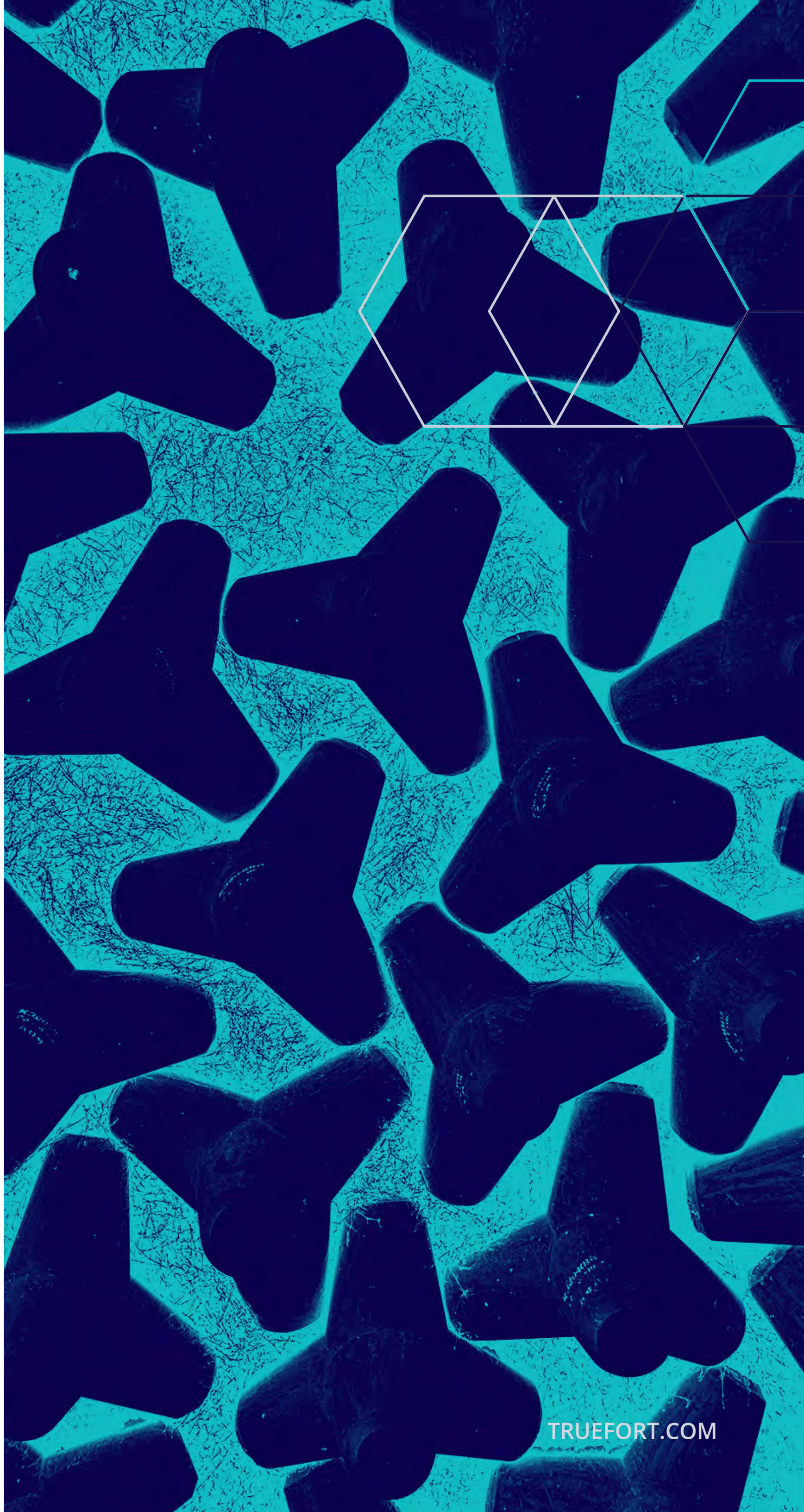
This is where a microsegmentation solution armed with real-time incident management comes to the rescue. Such a system, tailored for cloud-adapted incident management, leverages a baseline of workload behavior and traffic patterns to rapidly spot potentially malicious anomalies. Upon detection, the system can autonomously initiate responsive measures in synchronized third-party systems, curtail the attacker's potential lateral spread, and tweak the microsegmentation policies pertaining to the affected workload. With this real-time incident management prowess, security mechanisms can detect and quarantine compromises at the application tier, be it in the cloud or in data centers. This proactive approach minimizes damage and grants incident response teams the luxury of time to identify the root causes and bolster the defenses against residual vulnerabilities.



File Integrity Monitoring

Beyond the CIS benchmarks, File Integrity Monitoring (FIM) is often mandated by industry regulators. Stringent regulatory standards like PCI DSS, NIST, SOX, FISMA, and HIPAA necessitate an exhaustive audit trail for any modifications in pivotal configuration files, elevating FIM to a cornerstone of contemporary cybersecurity. Many older security tools, conceived before the dawn of cloud migrations, are ill-equipped to handle FIM for cloud-hosted files. Moreover, they may falter in assisting security teams in pinpointing the exact changes in a file, thereby prolonging the time taken by experts to decipher the events. Simultaneously, attackers can exploit minute file aberrations to breach vital workloads.

A microsegmentation solution tailored for blended environments should not only apprise the SOC when files, configurations, or binaries undergo alterations but also contrast the old and new files, rendering the changes effortlessly discernible. Tools fortified with workload behavior analytics promptly detect discrepancies in versions, alteration dates, content, and checksums, affording incident response teams precious time to orchestrate their countermeasures.

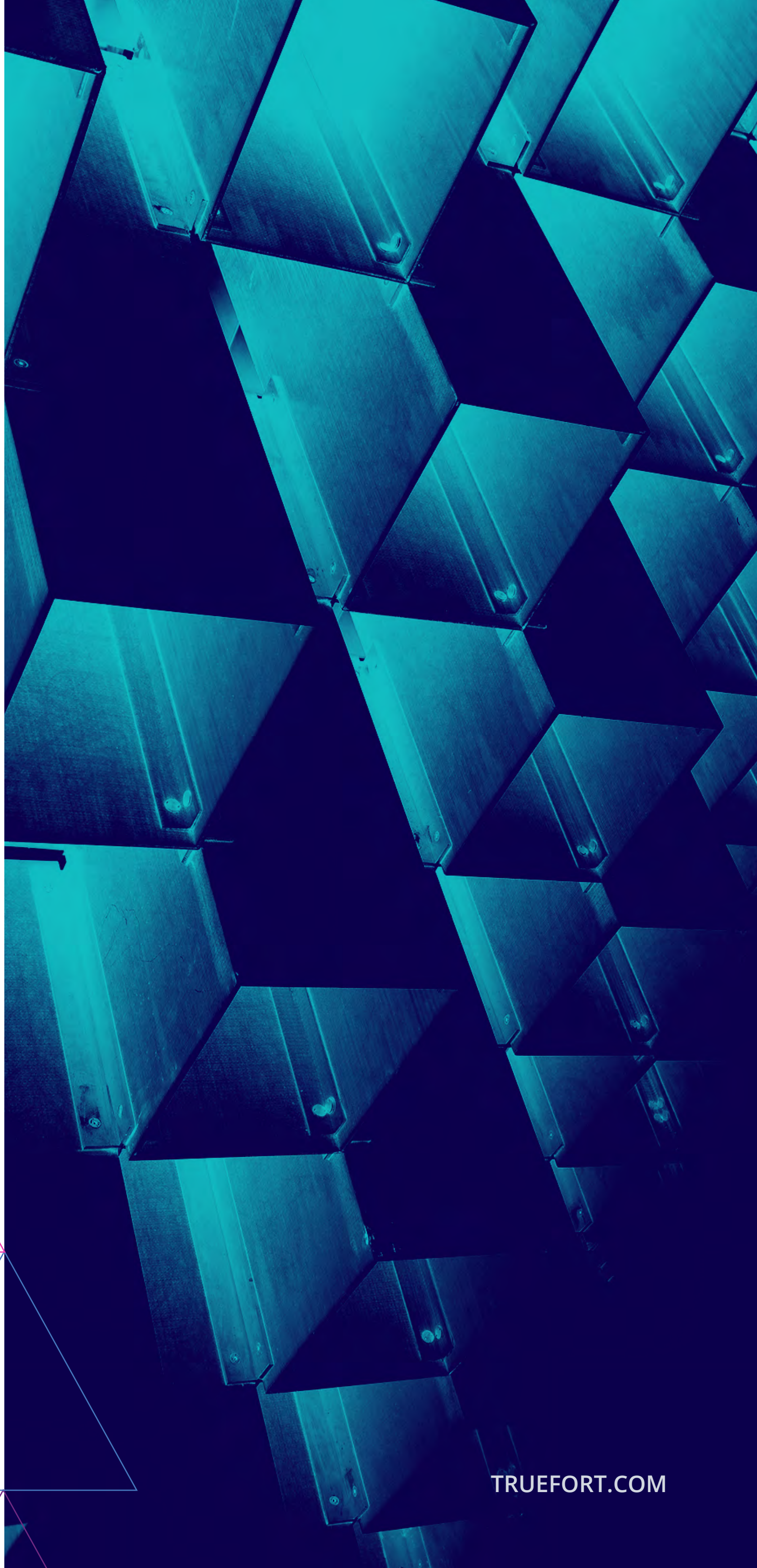


Service Account Analytics

Although service accounts are indispensable for most firms to virtualize resources, automate tasks, manage IoT gadgets, and ensure unhindered operations of applications and data, they don't typically align with individual humans. This makes them easy to overlook, and they often escape regular monitoring. Left unchecked, these can serve as gateways for attackers.

Yet, identifying all dormant service accounts accumulated over prolonged deployments demands significant resources – both time and money – more than most establishments are willing to invest. And even if every dormant account is identified and secured, without a comprehensive dependency map for each, essential business operations could be disrupted. A microsegmentation tool that envelops service accounts within its automated mapping functions could be the panacea, effectively sealing potential breach points.

The analytical features of service accounts should autonomously detect service accounts and their dependencies, offering a meticulous list of all active service accounts in an environment and their actions. It should identify proprietors, gauge account activity frequency, and identify dormant accounts. With this comprehensive view into service accounts, SOC teams can preemptively mitigate vulnerabilities, forestalling potential breaches by malicious actors.



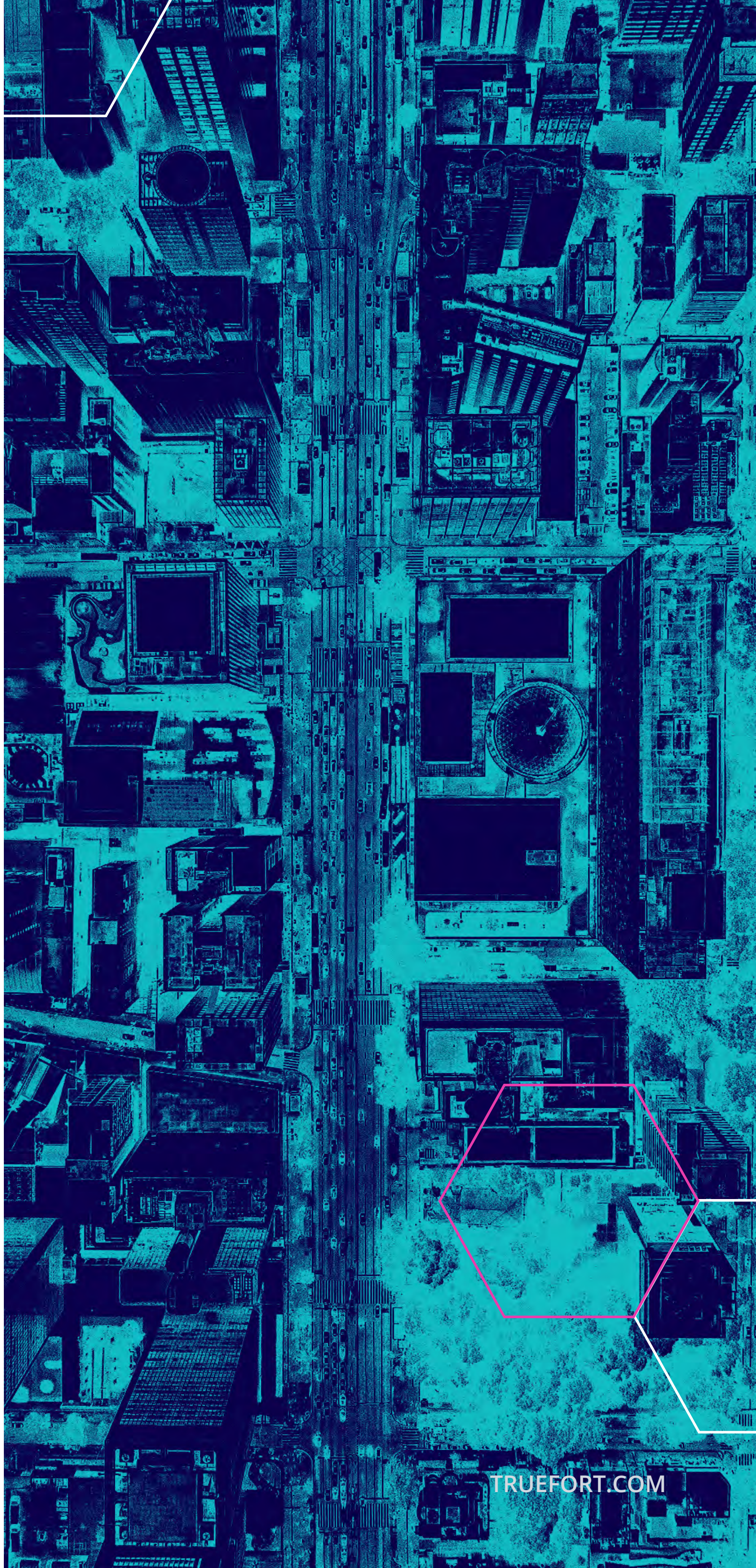
Shield Against Zero-Day Exploits

Zero-day attacks – which exploit unreported software vulnerabilities – rank among the most covert cybersecurity threats. Given their propensity to exploit vulnerabilities before developers can patch them, defending against such threats demands a specialized security platform with strategies meticulously designed to thwart such unpredictable attacks.

Any robust defense mechanism must pivot on behavioral analytics. Rather than solely relying on recognized threat signatures, which are ineffective against zero-day threats, a superior platform should assess the customary behavior of applications and processes within a company's environment. By establishing a benchmark of what constitutes "usual" or "necessary" behavior, the platform can swiftly detect outliers or deviations that might indicate a zero-day attack.

Real-time telemetry that spans network, process, identity, and software behavior is crucial. Such a multifaceted, instantaneous analysis ensures that any abnormality, even if it's a pioneering exploit technique, is promptly detected. Upon detection, the platform should initiate automated countermeasures, efficiently containing and mitigating the initial compromise.

Additionally, adherence to the principle of least privilege is pivotal, ensuring applications and processes can only access indispensable resources. This strategy curtails the potential impact of a zero-day exploit by reducing available pathways to attackers post-breach. In essence, while zero-day exploits are devised to elude recognized defenses, a behavioral-centric approach buttressed by real-time analysis and stringent adherence to the principle of least privilege presents a formidable line of defense against these erratic threats.



Maximizing Time-to-Value: A Golden Rule

Although not strictly a capability, time-to-value (TTV) is an emergent attribute of a judiciously selected microsegmentation solution. Rapid realization of value significantly bolsters the odds of enduring success in zero trust deployment. Insights from ESG reveal that a staggering 40% of enterprises surveyed temporarily shelved their zero-trust initiatives, primarily because organizations lose momentum when they don't perceive tangible value.

Microsegmentation tools that are user-friendly, laden with cost-effective automation, offer incisive analysis, and harmoniously integrate with existing infrastructure drastically reduce implementation efforts and bestow immediate tangible benefits. Instead of deploying multiple agents from different vendors, it is possible to use existing agents (like Crowdstrike or SentinalOne) to gather telemetry, visibility, and understanding of an enterprises security posture. Monumental enterprise-wide initiatives require unwavering support from top-tier management and key stakeholders to truly succeed. However, with tangible benefits early on in the journey, even if pioneering advocates transition out and fiscal allocations are constrained, you'll have the impetus to persevere.

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. 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.

Key offerings include:

- Automated dependency mapping across environments.
- Comprehensive behavior analysis for processes and workloads.
- Vulnerable service account protection and analysis.
- In-depth application behavior insights.
- Proactively protect against zero-day attacks.
- Advanced threat detection with real-time analytics.
- Comprehensive east-west traffic insights.

Discover how TrueFort can redefine your microsegmentation journey.
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