UNDERSTANDING WORKLOAD BEHAVIORS AND CLOUD DETECTION AND RESPONSE WITH TRUEFORT

EDITED BY JOHN J. MASSERINI
SENIOR ANALYST, TAG CYBER

TAGCYBER TRUEFORT™

UNDERSTANDING WORKLOAD BEHAVIORS AND CLOUD DETECTION AND RESPONSE WITH TRUEFORT

EDITED BYJOHN J. MASSERINI,
SENIOR ANALYST, TAG CYBER

In this book, we dive into the risks and challenges around workload management and Cloud Detection and Response (CDR) and look at how the TrueFort Platform provides actionable insight into the native cloud environment.

–1–

OBSERVABILITY OF A PRODUCTION CLOUD WORKLOAD ENVIRONMENT

DR. EDWARD AMOROSO, TAG CYBER

An accurate inventory and a clear understanding of the cloud production workload environment are crucial for effectively mitigating risks throughout the enterprise.

Until now, much of the approach to cloud solutions has focused on emphasizing ease of use and rapid deployment. However, as the cloud environment proliferates throughout the enterprise, managing and maintaining observability of workloads and applications has become burdensome. This chapter analyzes the risks of an unmanaged cloud environment, addresses the challenge of maintaining an accurate inventory, and proposes potential solutions..

At TAG Cyber, our experience working with enterprise security teams indicates that maintaining production environment observability for cloud-hosted workloads and applications is a significant challenge. The objective is to ensure that security teams understand the various dependencies, behaviors, and other attributes required for cyber protection, but achieving this takes work.

STRATEGIES FOR OBSERVABILITY

Through our collaboration with TrueFort, a leading commercial cybersecurity company, we gained valuable insights into strategies for accomplishing the goal without burdening application security specialists, operations staff, or the application development team. The following sections provide a brief overview of these application protection strategies.

Observing Dependencies – Understanding and managing the network of emerging communications and dependencies is one of the main differences between monolithic applications hosted in traditional data centers and modern applications running in virtualized cloud environments. Specifically, workload and application communications are a major byproduct of a microservice architecture built on containers and orchestration.

Understanding and managing the network of emerging communications and dependencies is one of the main differences between monolithic applications hosted in traditional data centers and modern applications running in virtualized cloud environments.

Gaining Intelligence from Behaviors – Obtaining intelligence about a production application requires actively observing its live behavior. While status reviews and testing provide valuable context, true intelligence is acquired solely through observing communications and dependencies. Integrating this acquired intelligence into the threat stream enables informed action.

A clear understanding of application behavior becomes crucial in hybrid architectures that leverage multiple public cloud services. When adopting a hybrid approach, security teams rely on various reporting tools, which are often inconsistent and incompatible with each other. Therefore, it is essential to maintain a consistent level of visibility across the hybrid infrastructure to establish an accurate view of the production-level posture.

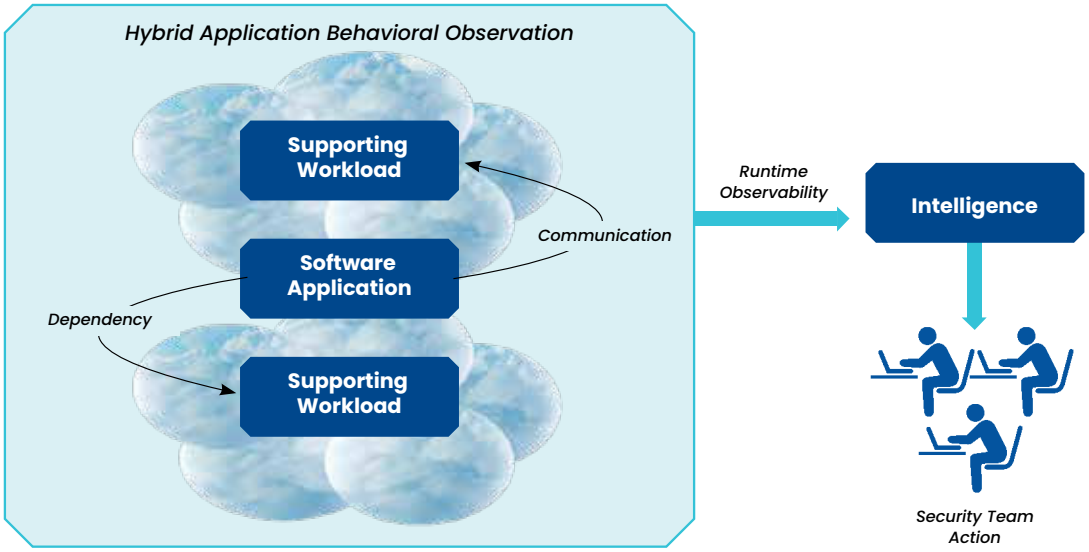

Figure 1: Advantages of Production Application Observability.

LIFECYCLE VISIBILITY

Establishing early visibility during DevOps is essential to the full lifecycle, including production deployment. Delaying the implementation of security controls until after completing the production deployment is a common cybersecurity mistake for all control types. Initiating security integration early during development is more efficient and cost-effective, particularly for modern applications.

Readers will hopefully recognize the importance of establishing a mechanism to observe application behavior throughout the entire lifecycle, including the production-hosted runtime instance. Security teams must base their decisions on dynamic and ongoing observational infrastructure to ensure effective software application protection.

LEVERAGING BEHAVIORAL-BASED WORKLOAD, APPLICATION, AND IDENTITY CONTROLS FOR AUTOMATED WORKLOAD PROTECTION

JOHN J. MASSERINI, TAG CYBER

DevOps is shifting the responsibility for the entire environment away from the legacy server and network admin teams and placing it firmly in the hands of the development world. Automating the management of these workloads, applications, and identities is essential to risk mitigation. Modern development processes have complicated application environment security.

Developers and operations teams are assuming full responsibility for the entire environment in which cloud applications operate. From networks and devices to the application stack, developers can now instantiate entire environments that, historically, required multiple teams and weeks of effort. Also, thanks to the ephemeral nature of the DevOps world, the device and application churn in these environments is enough to make any Configuration Management Database (CMDB) quiver.

Unfortunately, for most enterprises, the new DevOps support staff is neither trained nor tooled to support an around-the-clock, business-critical function. However, by leveraging behavioral analytics and automated workflow execution, we can now utilize environmental analytics to ensure that all network segmentation, device configurations, and identities align with the enterprise's expected norms.

While configuration drift is expected and managed within legacy enterprise infrastructures, the pace of cloud configuration drift is virtually unmanageable without automation. Developers will spin up new cloud environments at will, adjusting segmentation rules, system configuration,

While configuration drift is expected and managed within legacy enterprise infrastructures, the pace of cloud configuration drift is virtually unmanageable without automation.

and account access to suit their individual needs. Monitoring and automatically correcting any missteps is crucial when considering leveraging cloud resources.

FAST-MOVING ENVIRONMENTS HAVE RENDERED LEGACY CONTROLS INEFFECTIVE

In a dynamic cloud environment, attempting to enforce static controls is often an ineffective approach. To truly support the ever-changing nature of cloud environments, the controls must be dynamic, continuously monitoring ongoing activities and adapting accordingly.

carefully devised behavioral analytics model can leverage network segmentation as a perfect use case to manage any drift from expected norms in real time. It enables the elimination or, at the very least, alerts on unapproved network connectivity as it occurs.

This type of real-time modeling is becoming ever more critical with the endless daily onslaught of attackers moving laterally through an environment. Identifying new, malicious traffic and immediately shutting it down gives enterprises a fighting chance.

This same approach applies when evaluating system configuration and file integrity. Security teams can focus on known changes by developing workload baselines around constitutes acceptable configuration drift. In addition, despite the long, onerous, and time-consuming practice of file integrity reporting (typically arriving in "'batch"' reports from overnight processing), documenting file changes is a critical operational control, especially in regulated industries.

By leveraging continual file integrity monitoring, the workloads remain far more stable and secure, increasing confidence in the controls and a cleaner regulatory reporting mechanism.

SERVICE ACCOUNTS AND AUTOMATION BRING ACCESS MANAGEMENT MISSES

Finally, one of the most pervasive risks within a modern DevOps cloud environment is, arguably, the lack of controls around access. Identity management, specifically "roles" and "service accounts," wreaks untold havoc in most cloud environments. As cloud environments manage access differently than legacy, on-prem environments, the "old way" of managing access does little to mitigate access risk. Plus, trust relationships often spiral uncontrollably thanks to how cloud environments inherit access, leaving unintended and unwanted cross-workload trust relationships.

Understanding the intricate relationships between access rights, roles, workloads, and devices presents a compelling case for implementing a machine learning-based analytical solution. The value extends across network segments and individual devices. Incorporating behavior analytics

into a real-time file integrity monitoring solution allows security teams to gain valuable insights often unavailable to them in the past.

A shared source of truth between application and security teams is a essential. Behavioral analytics-based automation can play a pivotal role in mitigating risk, but doing so requires a solid set of agreed parameters between the DevOps and security teams, which is challenging to achieve. Developing an environmental baseline that includes system configurations, access controls, and network segmentation rules is crucial in a successful trust-based DevOps/security partnership.

Both teams can achieve their ultimate goals by developing a model that defines acceptable or unacceptable drift levels. When evaluating behavioral-based solutions, those that can assess the environment and provide a "current state" model are invaluable in finding that common ground between DevOps and security.

THE CHALLENGES OF CLOUD DETECTION AND RESPONSE

CHRISTOPHER R. WILDER, TAG CYBER

Detecting unexpected behavior in a cloud environment is often challenging due to the lack of instrumentation and the continual churn of devices and applications. Being able to separate legitimate attacks from everyday '"noise"' is a critical function that enterprises must develop to leverage cloud environments.

The detection and response solutions landscape is teeming with options, ncluding Network Detection and Response (NDR), Endpoint Detection and Response (EDR), and now. Extended Detection and Response (XDR). This convergence encompasses NDR, EDR, Security Information and Event Management (SIEM), , and threat intelligence, providing a comprehensive suite of capabilities.

Now, we have Cloud Detection and Response (CDR), which focuses on detection and response solutions for cloud workloads. CDR allows security operations (SOC) teams to ensure the integrity of virtual machines (VMs), containers, cloud APIs, and third-party applications.

Due to the massive recent increase in Software-as-a-Service (SaaS) and public cloud services, CDR is one of the fastest-growing segments in cybersecurity, with most organizations moving critical business systems like email, collaboration, sales, marketing, and HR to the cloud.

As a result of this transformation, cybersecurity teams must adapt to a radically different threat landscape in the cloud, with little control over the networks and security controls that underpin the operation of vital business systems.

Bad actors increasingly deploy sophisticated attacks (credential stuffing, social engineering, spear phishing, and more) to access cloud resources. For example, our team has tracked a 2X increase in attacks against cloud and SaaS providers from the same time last year, with Docker containers, Microsoft Azure, and Amazon Web Services (AWS) targeted by threat actors such as TeamTNT and the 8220 Gang.

Detecting unexpected behavior in a cloud environment is often challenging due to the lack of instrumentation and the continual churn of devices and applications.

LACK OF VISIBILITY INTO THIRD-PARTY APPLICATIONS AND ENVIRONMENTS

CDR solves a significant void in every enterprise infrastructure, especially if they support SaaS, Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) solutions. Gaining control and visibility over systems managed by external IT teams proves challenging and cumbersome. Moreover, the absence of visibility into cloud environments and applications adds complexity to incident response and threat-hunting efforts for (SOC) teams.

CDR SOLUTIONS ARE DIFFICULT TO DEPLOY IN MULTI-CLOUD ENVIRONMENTS

Most organizations are leveraging the benefits of multi-cloud environments to extend functionality and choices. Unfortunately, deploying in disparate cloud environments increases complexity, scalability, costs, and difficulty. Multi-cloud environment security is more complex than single-cloud systems, which require teams to deploy consistent controls and security guidelines to ensure adequate visibility and prevent costly misconfigurations..

THE CHALLENGE OF MONITORING AND IDENTIFYING CLOUD MISCONFIGURATIONS

The most common reasons for cloud data breaches are misconfiguration, stale credentials, and the inability to investigate and mitigate security incidents. Our research indicates that the average cost of a non-cloud breach is four to five million dollars per breach, whereas a cloud-based data breach is well over seven million dollars, depending on the value of the information. Although CDR is effective for incident detection and response, additional measures are necessary to minimize the noise generated by third-party providers and reduce the number of false threat signals.

In summary, SOC teams need comprehensive visibility across the entire domain to ensure CDR effectiveness. This visibility should encompass activity from containers, VMs, endpoints, and network data. In many cases, CDR rounds out the detection and response solutions stack, but there are challenges.

Enterprises require enhanced visibility into their third-party service environments to monitor and manage security effectively. CDR can provide a clearer line-of-sight into hosted applications, security controls, user activities, privileges, and indicators. This improved visibility enables prompt response to alerts and enhances the organization's overall security posture.

DEVELOPING A SUCCESSFUL MICRO-SEGMENTATION STRATEGY

DR. EDWARD AMOROSO, TAG CYBER

The foundation of successful cloud adoption is the definition and management of a strong micro-segmentation strategy. Minimizing trust relationships and enforcing predefined application and workload behavior provides a solid foundation for a secure cloud environment.

A hybrid environment in cybersecurity refers to a computing infrastructure that combines on-premises data centers, private clouds, and public clouds—allowing organizations to leverage the benefits of on-premise and cloud computing environments. However, managing security in a hybrid environment can be challenging due to infrstructure complexity and the need to maintain consistent security policies across different environments.

Consistent application of security controls is crucial to maintaining the confidentiality, integrity, and availability of organizational data and resources. In addition, organizations must implement appropriate security measures to protect data moving between different environments, such as encryption and secure data transfer protocols.

Micro-segmentation is a pivotal component that empowers enterprises to construct secure cloud deployments that lay the groundwork for enforcing controls at a granular level. Micro-segmentation also minimizes unrestricted enterprise movement, deals with abuse of cloud-based permissions, and provides a baseline for how applications should work. TrueFort approaches micro-segmentation from the perspective of lateral movement after compromise.

Lateral movement refers to attackers spreading across a network or container environment to gain access to high-level accounts and sensitive data. Attackers often use this technique after a successful network penetration to escalate their access privileges and achieve their malicious goals.

The objective is to manage network connections and service accounts to protect workloads, reduce attack surfaces, and secure the local infrastructure. TrueFort meets these objectives with application intelligence and agent deployment, which we explore in the next section.

Micro-segmentation is a pivotal component that empowers enterprises to construct secure cloud deployments that lay the groundwork for enforcing controls at a granular level.

APPLICATION INTELLIGENCE

The initial step in deploying micro-segmentation involves identifying the dependencies, interactions, and data sharing between the microsegment and its surrounding environment and entities. However, this challenging task demands a comprehensive understanding of the microsegment's dynamic runtime behavior, static characteristics, and associated workloads and applications.

The shift from deploying monolithic applications in corporate data centers to the microservice-based deployment of containers in cloud and SaaS environments emphasizes the importance of highlighting dependencies. Visualizing the resulting interactions between application components as a mesh enables efficient data transfer, sharing, and communication.

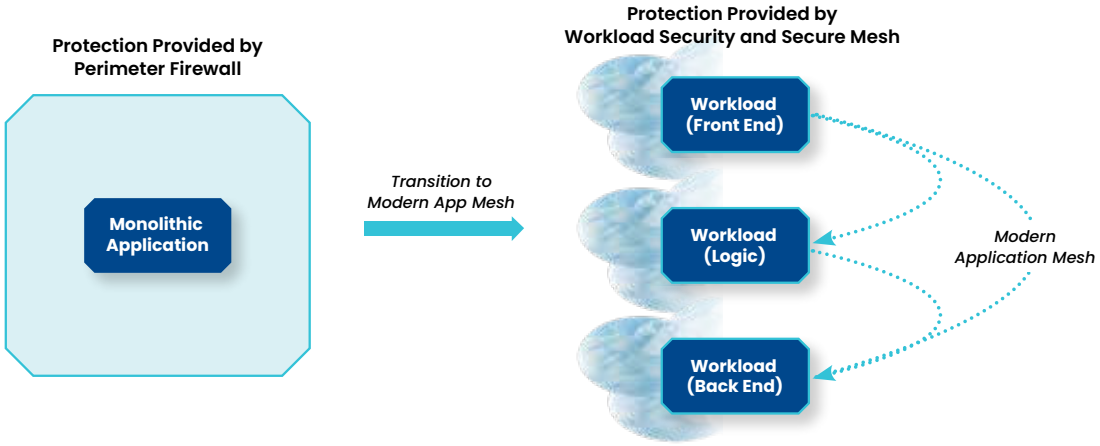

Figure 1: From Monolithic Apps to Mesh-Based Deployment

The TrueFort platform addresses the need for visibility by gathering intelligence on application operation and utilization. It achieves this by extracting telemetry from the interactions and communications in a modern hybrid deployment. Typical use cases encompass business logic interactions with front-end and back-end systems to facilitate seamless data flow.

TrueFort supports this application intelligence, a fundamental foundation for micro-segmentation. Instead of relying on the data output from a next-generation firewall (NGFW) at the corporate perimeter, TrueFort's platform collects telemetry data throughout the application mesh, offering a comprehensive and platform-based approach.

AGENT DEPLOYMENT

The second requirement for micro-segmentation entails establishing a secure interaction between the hosted workloads and their surrounding environment. Fortunately, cybersecurity has reached a level of maturity where numerous exceptional commercial options are available to implement the necessary controls for such arrangements.

To that end, TrueFort has forged a partnership with CrowdStrike, a leading commercial endpoint security provider. This partnership enables direct integration with the widely adopted Falcon platform, leveraging existing Falcon deployments to fulfill various cybersecurity objectives associated with Zero Trust. Notable features facilitated through the TrueFort and CrowdStrike partnership include:

- **Agent Reuse** – For existing Falcon customers, there's no requirement for an additional agent to engage the application intelligence or microsegment enforcement provided by TrueFort.
- **Unified Visibility** – Enterprise teams with an existing Falcon deployment can direct TrueFort telemetry to this platform to enhance and improve the quality of the visibility.
- **Detection and Response** – TrueFort's application intelligence can more directly connect with immediate detection and response processes.

Since enterprise-level cybersecurity incorporates pre-existing deployed controls, the concern lies in the ability of modern cybersecurity tools to interact and integrate with existing platforms. The partnership between TrueFort and CrowdStrike is a testament to this encouraging trend, showcasing the importance of collaboration and compatibility in cybersecurity.

RECOMMENDED STRATEGY

For enterprise teams aiming to implement an effective micro-segmentation strategy, it is essential to include the following steps in all management planning associated with this shared endeavor:

- **Step 1: Ensure Visibility** – Make sure a plan is in place to develop application intelligence and insight into the interactions between workloads in a modern mesh arrangement across multi-cloud.
- **Step 2: Review Integration Options** – Review and take full advantage of options to integrate planned commercial tools via their application programming interface (API) or through pre-planned integrations, such as with TrueFort and CrowdStrike.
- **Step 3: Work with Capable Vendors** – Always select and work with capable vendors who can guide day-to-day tactical and longer-term strategic decisions toward options that reduce cost, reduce risk, and maximize value.

Follow these management steps in all planning and execution activity toward a micro-segmentation-based deployment to help reduce the risk for operational workloads and overall project management.

OVERVIEW OF THE TRUEFORT PLATFORM AND A PROPOSED ACTION PLAN FOR ENTERPRISE

DAVID NEUMAN, TAG CYBER

Enterprise teams looking to protect their cloud enterprise should consider the TrueFort Workload protection platform in their enterprise action plan.

As cloud workloads increasingly become the standard for modern businesses, they bring numerous advantages, such as scalability, flexibility, and cost savings. However, the growing prevalence of cloud computing also comes with heightened security challenges that are progressively more complex and challenging to address.

Increasing visibility and control represents a key challenge in safeguarding cloud workloads. Cloud environments exhibit high levels of dynamism, continuously spinning up and down workloads and complicating resource and data monitoring within the environment. This dynamic nature poses difficulties in ensuring the comprehensive security of all cloud workloads and preventing the exposure of vulnerabilities.

Another challenge is the evolving threat landscape. As cybercriminals become more sophisticated, they find new and more effective ways to target cloud workloads. Threats such as ransomware, data breaches, and DDoS attacks can significantly damage an organization's reputation and financial stability, making cloud workload protection a critical component of any comprehensive security strategy.

Furthermore, businesses must comply with compliance and regulatory requirements, which can vary depending on the industry and location. These requirements often dictate the implementation of specific security controls and policies, underscoring the significance of aligning the cloud workload protection strategy with these compliance measures.

TrueFort allows organizations to integrate security controls and policies into the cloud environment, ensuring all workloads have the appropriate protection controls

APPROACH TO AN ENTERPRISE ACTION PLAN

Protecting cloud workloads is complex and challenging, requiring a comprehensive and proactive approach. Businesses must deeply understand their cloud environments, implement robust security controls and policies, stay current on the latest threats and vulnerabilities, and ensure compliance with all applicable regulations and standards. This approach requires an enterprise action plan with the TrueFort platform.

To establish an effective cloud workload protection strategy, **define the cloud workload protection requirements.** This process entails identifying the workloads that need protection, determining the appropriate level of protection for each workload, and outlining the security controls and policies to achieve the desired security level. It also means understanding business requirements and considering any compliance or regulatory requirements.

Obtain a comprehensive understanding of the enterprise by **gaining visibility into existing cloud workloads and protection controls**. First, conduct an extensive inventory of all cloud workloads in the environment, including identifying all resources, applications, and data stores within the cloud environment and their associated protection controls. Next, review the existing protection controls for network security, access controls, encryption, and monitoring areas. Finally, identify any gaps or vulnerabilities in the current protection controls.

Integration is a critical aspect of the enterprise action plan. TrueFort allows organizations to **integrate security controls and policies into the cloud environment,** ensuring all workloads have the appropriate protection controls, including access controls, encryption, network security, and monitoring.

Create assurance and operational efficiency through continuous verification. TrueFort uses extensive native rule packs and policies to enable security teams to verify that an application's hardening status is maintained in a secure state and brought back into compliance if it deviates. Based on a baseline of approved activity, the TrueFort Platform detects and prevents the spread of anomalous activity within the data center or cloud.

In addition, data, network access, and configuration parameters are monitored against a trusted baseline of expected behaviors, alerting teams of deviations and changes. This approach limits the scope and impact of a cyberattack, shortening the duration of a security incident by stopping bad actors from reaching any valued target. Moreover, continuous monitoring and management of applications, systems, and infrastructure are possible, ensuring adherence to user-defined policies and industry mandates such as CIS benchmarks, NIST, PCI, NYDFS, and others.

CONTINUE THE JOURNEY

Cloud workload protection is not a "one and done" project; an enterprise action plan must continue evolving and improving with the business. Improving the cloud workload protection strategy involves identifying new threats and vulnerabilities, updating protection requirements, and implementing new security controls and policies—all of which involve regularly reviewing the cloud workload security posture and adjusting the protection strategy to meet the evolving security landscape. TrueFort empowers teams to maintain positive control of their cloud enterprise and actively contribute to business growth, success, and protection.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.