TRUEFORT

ARTICLE

Reducing Your Security Attack Surface With Application Risk Posture Management

Forbes Technology Council

Sameer Malhotra
FORBES COUNCILS MEMBER

Sameer Malhotra is co-founder and CEO of TrueFort, a former Wall Street tech exec and an expert in IT infrastructure and cyber security.

Applications and their associated data are the lifeblood of virtually every modern organization. As a result, they represent high-value targets for attackers. However, traditional security architectures focus primarily on the underlying IT infrastructure and, as such, provide limited visibility into the application environment. This creates a large attack surface for potential exploits and increases security risks to the business.

To address this blind spot, a new discipline called application risk posture management is filling the void. It encompasses a broad range of capabilities that enable organizations to assess, understand and manage their risk posture through an application lens—across both development and production environments. The intelligence that application risk posture management provides can enable business and operations personnel to document their environment's current risk profile, compliance status and areas for improvement to reduce the likelihood of a successful attack.

How It Works

Application risk posture management relies on real-time telemetry to assess how application components interact with each other, determine their expected (normal) behaviors and continuously monitor and assess compliance and risk across the entire application environment.

Visibility

Application security layer visibility makes security organizations much more responsive to conditions that threaten business continuity. Specific benefits include:

- **Policy visibility and consistent enforcement across cloud, hybrid and legacy applications.**
- **Continuous discovery and identification of new application workloads.**
- **Alerting on risky new deployments or changes to existing applications.**
- **Contextual risk assessment versus simple comparison to frameworks and external standards (e.g., ISO, NIST, CIS).**
- **Continuous application risk management, risk visualization and risk prioritization.**
- **Verifying operational activities are being performed as expected.**

Risk Scoring

Application risk posture management also includes risk scoring at both a security operations and business impact level. This requires discovery technologies that catalog an organization's application environment portfolio and apply risk scoring metrics to rank applications based on their value and business criticality. These business-impact metrics can then be used as a dimension of overall risk assessment, reporting and operational remediation prioritization.

Role-Specific Views

One of the most useful capabilities of application risk posture management is the ability to customize the views of risk posture status by role in the organization. For example, CISOs can view and interact with executive-level information that summarizes current and historical application risk levels and their potential business impact. This level of reporting gives security executives the information they need to translate complex security operational information into business-friendly performance metrics that the executive team and the board can understand and evaluate more easily.

Similarly, for operating teams, risk metrics can be tailored to specific responsibilities within the organization. For example, application owners can view the risk posture of their application portfolios, and SOC analysts can see overall application threat event metrics, while other security operations teams can assess compliance with current control policies at a glance.

Application risk posture management serves many purposes. Here are several examples we were involved with that show how security leaders have used it to reduce security risks.

Cross-team coordination:
Despite having a shared goal of protecting a company's infrastructure and data, security teams can be siloed in their view of the security landscape. A leading telecommunications provider uses application risk posture management to achieve more holistic visibility and information sharing across development, security and threat hunting teams.

Up-to-date app inventory and status:
Keeping track of modern application environments is no easy task. The real-time telemetry and insights from application risk posture management are enabling a healthcare company's security teams to maintain an up-to-date understanding of what's in their environment and how it's performing, even as applications are updated or added.

Track progress:
One of the leading benefits provided by application risk posture management is the ability to measure results over time. CISOs struggle to show where and how they have been effective. The CISO at one leading financial services organization is using application risk posture management to maintain visibility across all team activities in a complex application environment and to monitor, measure and communicate progress.

IMPLEMENTATION TIPS

1. Because of the dynamic nature of application environments, native solutions that provide security visibility, monitoring and reporting between and among applications and their workloads are required to assess and effectively manage enterprise application risk posture. Retrofitted tools from other security areas such as network monitoring will lack sufficient depth and breadth.
2. Make sure the data is available in real time to avoid the need to match up data with varied time stamps and ensure a continuous and accurate view of the environment with no latency.
3. Software is only one element of successful application posture management. Equally important is using the information and insights from an enhanced understanding of the application environment to drive discussions that align business and security functions, such as determining the business criticality of various applications. Create a forum to share statuses across functional security teams. This shared visibility into each other's worlds can pay big dividends in strengthening communications and security best practices.
4. Monitor application security posture metrics over time to make decisions about resourcing, budgets, response protocols and more. When improvements are achieved in one area and resources are needed in another, having the necessary data can enable better decision-making so hard-won resources can be redirected where they are needed most.

Application risks are among the greatest threats now facing enterprise security teams. Adding application risk posture management to the security toolbox can make organizations more efficient and effective at preventing and containing breaches.

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application-centric Fortress platform delivers comprehensive realtime cloud-to-the-ground insight, protection and automated response with patented machine intelligence and a single or bring-your-own agent. Fortress overcomes the application security blindspots inherent in legacy infrastructure-centric tools, providing unparalleled visibility and protection for applications in on-prem, hybrid and cloud environments and for security teams across the enterprise. Fortress speeds response times, minimizes the blast radius of compromises, prioritizes resources, and enhances application risk posture.

TRUEFORT

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM