K2 CYBER SECURITY

Datasheet

# K2 Hybrid Cloud Security

## Real-Time Zero-Day Attack and Lateral Movement Prevention

## Key Advantages

- Prevents data breaches in hybrid cloud application infrastructure
- Deterministic security prevents zero-day attacks
- No false positives reduce cost and "alert fatigue"
- Real-time attack detection and alerting
- Single platform for securing applications in virtual machines or containers
- Dynamic micro segmentation policies move with the applications
- End-to-end authentication and encryption of app traffic

**Introducing the first deterministic solution for preventing cyberattacks in real time without false positives while simultaneously closing down lateral movement risk**

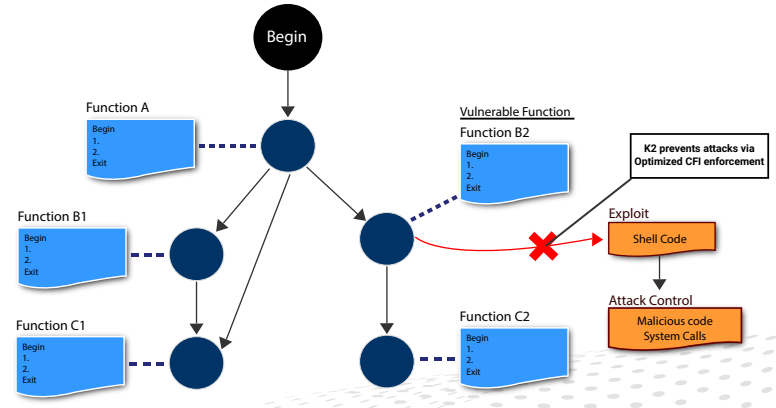
Data center applications no longer live in a fenced, on-premise environment, they exist in the hybrid cloud, virtualized, containerized or split into microservices. To protect this complex application infrastructure comprehensively and effectively, enterprises need a new type of solution that adjusts to the ever changing nature of these highly dynamic environments. IT teams can no longer afford wasting time on false positives or detecting exposed code vulnerabilities weeks or months after the fact.

## K2 Prevent

### Zero-Day Attack Prevention for Hybrid Cloud

Use K2 Prevent to protect your binary software or cloud workloads, including web applications running on bare metal, virtualized hosts or container environments. K2 has developed Optimized CFI™, the first deterministic solution that promises to enable no false positive, highly precise software-based CFI to enterprises, with easy operationalization: no need for source code for instrumentation, expensive re-compiles or hardware forklifts to implement.

K2 Prevent works via an agent that knows the legitimate execution paths of your application infrastructure and instantly alerts when an exploit or web attack occurs. Unlike most security approaches, K2 does not depend on prior behavioral or signature-based knowledge of any attack, enabling the solution to be effective against zero-day attacks.



# K2 Segment

## Micro Segmentation for Even the Most Dynamic Environments

Micro segmentation is becoming a new staple for data center security to protect against lateral movement of cyber attackers. The challenge with existing solutions is the fact that most cannot deal with dynamic IP addressing requirements of today's hybrid cloud.

K2 Segment introduces a new option for enterprises, a micro segmentation that retains security policy across ephemeral and automated environments. Policies are not tied to static IP addresses; they persist even as nodes disappear and re-initiate with different network addresses. Best of all, K2's micro segmentation can be leveraged from the same real-time prevention infrastructure used to stop infiltration events.

K2 Segment retains the ease-of-deployment characteristics of K2 Prevent by automatically discovering application nodes and understanding network traffic communication, making security policy easy to set through a highly visual and intuitive interface.

## Ready for Comprehensive Hybrid Cloud Security?

Whether you're rolling out Kubernetes, on AWS or Azure, trying to shut down attacks on your web applications or close the window of exposure on exposed software, K2 can help you get started.

To schedule a demo or just to learn more about K2, send us an email at info@k2io.com


K2 Cyber Security, Inc
2580 N. First Street, #130
San Jose, CA 95131

Phone: +1 (669) 284 9992
Email: info@k2io.com
Sales: sales@k2io.com

### About K2

K2 Cyber Security provides the most comprehensive protection for cloud against sophisticated attacks. K2's breakthrough in operationalizing Control Flow Integrity technology has for the first time enabled detecting and preventing exploits of zero-day attacks in real time without false positives. K2's platform provides comprehensive hybrid cloud security including real-time attack prevention and dynamic microsegmentation that reduces the risk from lateral movement threats.