



## Application-Centric Cyber Threat Detection

In the recent past, most enterprise organizations have learnt (and most times the hard way) that preventive security methods is not realistic to block all attacks or threats, making it more practical and critical for security teams to prevent those intrusions or vulnerabilities from becoming a data or financial loss. Also, most attacks no longer operate in the "smash and grab" mode, and instead when once inside the network after bypassing perimeter based security systems, now conduct some sort of internal reconnaissance in "stealth" mode. This provides the attacker the golden opportunity to dig in deeper into the entire deployment and also scan for more assets to control to damage. While all organizations have perimeter security and at times end-point security for critical servers and desktop (with security agents), they lag behind in protecting their mission critical "internals" once the threat is inside and is moving laterally in the east-west direction.

Uila assists enterprise organizations combat advanced cyber threats by providing immediate and comprehensive application-centric insight into lateral movement based threats for the Hybrid Enterprise.

### Agentless Cyber Threat Monitoring

Agentless and Scalable Deployment model to identify threat challenges for your mission-critical applications, with built-in classification for over 3200 applications.

### Anomalous Application Behavior

Confidently track critical Application workload characteristics in real time to identify anomalous behaviors such as dependency changes between the critical application and infrastructure resources, deletion or addition of new VMs, etc.

### Application-centric Lateral Movement Threat Detection

Comprehensive Application-centric visibility into lateral (east-west) movement traffic patterns and automated alerting to cyber threats such as malware, DDos, C & C, port scans, Exploit kits, etc.

### Conclusive Chain of Evidence for any Threat

Identify all application transaction data, infrastructure status and network traffic data before, during and after an attack.



## Detect Advanced Malicious Threats in Real-Time for Data Center and Cloud Workloads

- Real-time detection for thousands of emerging threats, including Ransomware, Command & Control, Exploit Kits, Malware Attacks, Port Scans, Obfuscation, SMB Probes, Buffer Overflows, etc.
- Latest signature support and updates from the largest group dedicated to advances in the network security industry .
- Gain overall insights into the historical context of how and the origins of the threats, who is being attacked, time of attack, methods used for the attack, etc.
- Get detailed awareness of Outbound Traffic from your Data Center to the Internet and reduce a huge portion of the risk associated with general Internet connectivity.

## Application Anomaly Detection

- Automatically classify over 3200 applications and map dependencies across apps & infrastructure.
- Identification of unauthorized VMs and their lateral movement.
- Visualize creation or tearing down of dependencies between assets for a multi-tier application indicating a cyber attack.
- Map thousands of cyber threats directly to the anomalous behavior in application performance and dependencies to identify root-cause.

## Lateral Movement Traffic Analysis

- Comprehensive visibility into lateral (east-west) movement traffic patterns to identify custom backdoors and compromised systems. For example, including SMB/SMB2 protocols that maybe used to transfer files/malware, password dumpers, etc.
- Identify unauthorized VMs/servers/connections as well as changes in traffic patterns for existing deployments.

