How Tuitio Stacks Up against the Competition

Tuitio™

Tuitio™ blocks All Endpoint Attacks in Real-time

Tuitio BLOCKS attacks on endpoints without having to recognize the malicious code. It does not just detect code (which is often too late!) It BLOCKS or PREVENTS all forms of malicious code: application exploits, file less (non-malware and in-memory), and socially engineered. Tuitio has always blocked new types of attacks on day one without sacrificing patient-zeroes or relying on an operationally burdensome 'detect and react' posture.

Makes File-less Attacks Boring

All malicious code attacks have a starting place: vulnerable applications, accessible utilities (e.g., PowerShell, cmd.exe, WMI/WMIC, etc.) and user-space. Tuitio places them 'under guard'. Whatever process these starting places spawn, it becomes guarded as Tuitio blocks any harmful action they attempt.

Does Not Fit Existing Endpoint Protection Categories

Leading market analysis firms categorize Tuitio differently, even within their own publications, characterizing Tuitio as application whitelisting and control, isolation and containment, and endpoint zero trust. Clearly, Tuitio applies a different approach.

Puts Prevention back into Endpoint Protection

Tuitio' s very different approach has restored faith in endpoint protection for its enterprise customers. Without Tuitio, large enterprises experience an average of 2.5 successful endpoint attacks per week. EDR is a symptom of expected failure. (Note: Contact us at sales@bravatek.com if you want to learn more about an enterprise version of Tuitio.)

Reverses the Upward Spiraling Costs Trend of the Detect & React Posture

Accenture reported that enterprise 'detect and escalate costs' for 2017 nearly doubled those in 2015.

"Cost-effective, efficient protection that made us more secure. It's not quite set it and forget it, but it's pretty close," Stated Ian Gottesman CIO, Center for Strategic and International Studies (CSIS).

Incident volumes for the different layers of a cyber program correlate with what happens at the endpoint. Tuitio nips attacks at the endpoint, causing an across –the-board reduction in labor hours.

Reduces Alerts Fatigue in Two Ways

Clearly, defeating attacks at the endpoint eliminates alerts from many sources downstream. However, many endpoint protection tools incur an operational burden from the alerts they themselves generate. Tuitio log events are generally notifications of what Tuitio blocked, eliminating dependence on analysts to analyze and react.

Endpoint Protection without Bloat

Tuitio's centrally managed agent weighs less than 1 MB on the hard drive, seldom exceeds 0.1% CPU, and occupies about 10 MB of memory. It is focused on one mission, BLOCKING (not just detecting) all forms of malicious code attacks in real-time.

Alleviates Patch Management Burden

To Tuitio, an unpatched application is no different from a patched one. Neither can do harmful actions. ITO PS can implement patches at their convenience.

Adapts to Endpoint Changes for Nearly 'Set & Forget' Operations

In the real world, nothing is absolutely set and forget. However, because Tuitio naturally adapts to software updates and patches, it's as close to it as anyone is likely to see. Tuitio only needs to know of an application or utilities parent executable, dynamically learning of all child executables and processes at run-time. Agents typically go months without policy updates.

How Tuitio Differs and Works

Tuitio is like a kernel-level traffic cop, tracking what applications and utilities do and spawn, blocking all attempts to alter system-space or mess with the memory of another application to prevent adversaries from accomplishing their goals. Knowing just the full path name for the parent executable of an application or utility (e.g., PowerShell), which seldom changes, Tuitio' s lightweight, kernel-level driver ensures that neither it nor anything it spawns can alter system-space (e.g., add/change files in Windows directory, alter sensitive registry keys, etc.) or inject code into or scrape another application's memory. In user-space, Tuitio only allows trustworthy executable and script launches, yet keeps them and anything they spawn 'under guard.'

Does Tuitio replace Your AV (Anti-Virus)?

Yes, but Tuitio is not a scanning product. Customers with regulatory mandates use Tuitio to block advanced threats and a traditional AV for compliance.

Blocks Pass the Hash/Ticket Attacks

Tuitio policy crafts a "trusted enclave" around the lsass.exe process that Windows uses to replay hashes and tickets whenever an end-user received an authentication challenge for something after logon. Adversaries cannot steal these credentials to move laterally to nearby endpoints.

Deployment is Simple

Simply order your Tuitio software at www.bravatek.com/product/tuitio. It's simple and straightforward. And—if you should need it, we can assist you at sales@bravatek.com.

How Tuitio Stacks Up against the Competition

Supported Platforms (centrally managed from same system)

- Windows XP R3 and Later
- Windows Server 2008 and Later (Server Guard)
- Persistent and Non-Persistent VDI
- Select Linux Server Distributions

Tuitio	OPERATIONAL IMPACT	EDR	ML/EPP	WHITELISTING	CONTAINERS
100%	Overhead (CPU, RAM)	100%	75%	100%	25%
100%	Cloud/Network Dependence	0%	25%	50%	75%
100%	Transparent to End-Users	75%	75%	75%	0%
100%	Adapts to Endpoint Changes	75%	100%	0%	0%
100%	Complex Tuning	75%	50%	0%	75%
100%	Alerts, IR, Remediation Operations	0%	0%	0%	0%
100%	False Positives	50%	50%	75%	75%
100%	High Skills Admin	0%	100%	75%	50%

www.bravatek.com/product/tuitio
June 2018