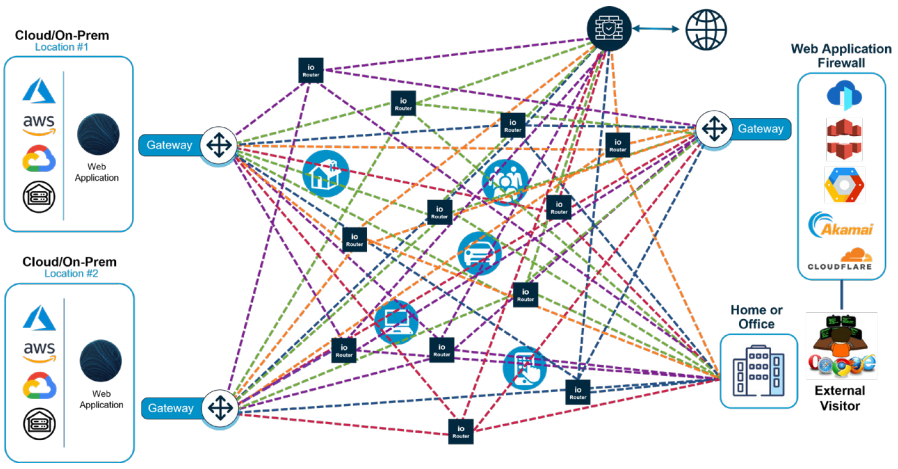
RAVID - A STEALTH, END-TO-END AUTOMATED MOVING TARGET DEFENSE (AMTD) STRATEGY

Introduction to RAVID

RAVID, or Randomized Adaptive Virtual Infrastructure Defense, is a strategic approach to cyber warfare. Instead of relying solely on static perimeter defenses, RAVID introduces unpredictability and resilience by continuously shifting the digital terrain. Inspired by military planning and SIGINT practices, it transforms the virtual battlefield into a fluid, self-correcting ecosystem.

Networking: The Foundation of Stealth and Misdirection

In conventional architectures, networks are the most vulnerable layer, often the initial target for reconnaissance and lateral movement. RAVID addresses this with stealth networking inspired by spread spectrum radio technologies. By obfuscating packet routes, dynamically encrypting each path, and separating the control and data planes, it renders traditional detection methods ineffective.



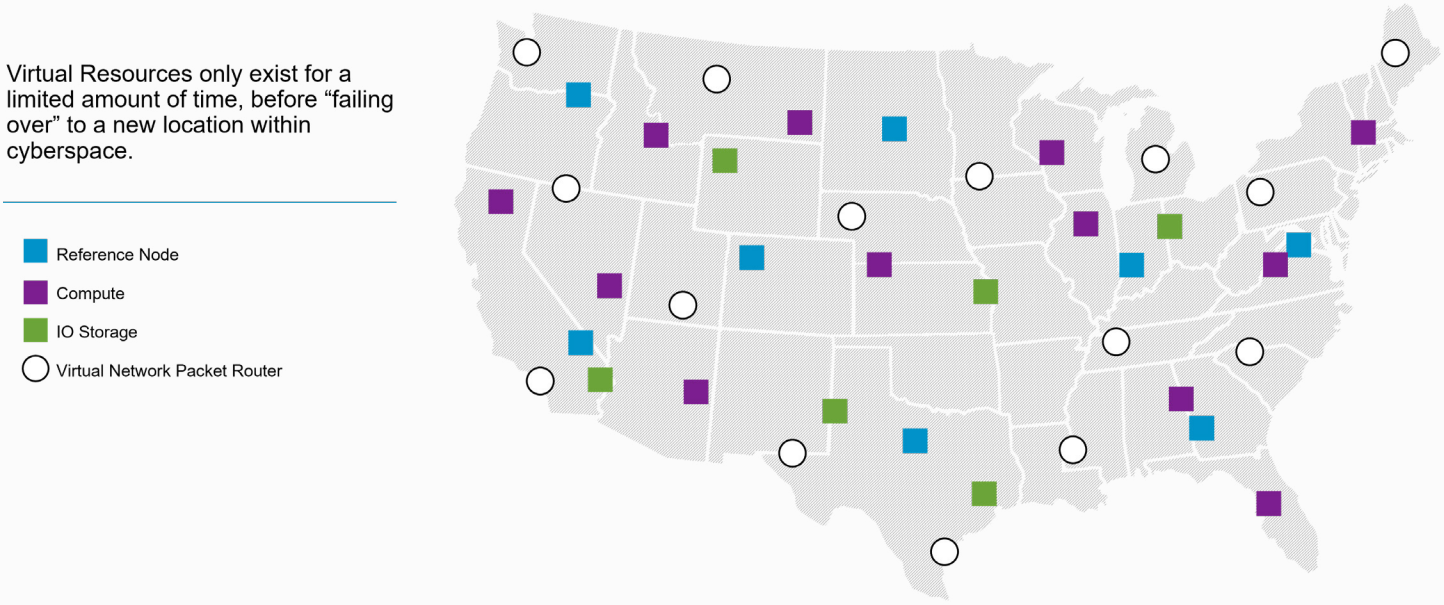
Static IPs are replaced with rotating gateway links, and packet fragmentation across multiple pathways ensures that no single transmission reveals meaningful data. As with legacy RF triangulation, adversaries are left unable to locate or engage real infrastructure. This dynamic routing results in decreased latency and increased resiliency, forming the first line of RAVID's AMTD perimeter.

In the ever-shifting landscape of cyber warfare, our adversaries evolve unburdened by bureaucracy, while legacy systems and stagnating strategies leave us vulnerable. Echoing lessons learned within the Marine Corps Signals Intelligence (SIGINT) and Electronic Warfare community. This paper outlines a modern, layered defense strategy through an integration of mature COTS components. We implement movement at every opportunity and leverage modern ephemeral networking to create a stealth effect rendering your infrastructure invisible to threat actors.

Much like Secure Compartmented Information (SCI) architecture, we assume compromise is inevitable and engineer for detection, resilience, and recovery. The outcome is a dynamic cyber defense: Randomized Adaptive Virtual Infrastructure Defense (RAVID) a framework that fuses stealth, mobility, and orchestration to protect your systems, improve performance, and save money.

Virtual Infrastructure: Active Failover and Ephemerality

Virtual Resources only exist for a limited amount of time, before “failing over” to a new location within cyberspace.



To reduce attack surfaces and limit exposure, RAVID deploys ephemeral virtual infrastructure across cloud and on-prem environments. Each component is given a time-to-live and automatically decommissioned after use. Failover operations occur proactively based on threat intelligence or predefined intervals, keeping workloads in constant motion.

Through automated orchestration using API calls and CI/CD pipelines, infrastructure can be rehydrated in alternate environments without service interruption. This operational agility not only increases survivability under attack but reduces the burden on IT teams by automating complex provisioning and tear-down processes.

AMTD for Applications: Moving Targets and Smart Deception

Applications under RAVID are containerized and designed for mobility. Using tools native to Kubernetes and major cloud platforms, applications are regularly relocated, spun down, and rebuilt. This ongoing motion invalidates reconnaissance, limits attack windows, and disrupts exploit chains.

During these movements, honeypots remain stationary as deliberate targets. These containers emulate application behavior and are instrumented to capture attacker tactics, techniques, and procedures (TTPs). Telemetry from these decoys feeds back into security systems to enhance detection, prevention, and threat intelligence.

To maintain availability and performance, dynamic Domain Name System (DNS) and geo-distributed load balancers route users to the nearest viable application endpoint. Even during transitions, automated pipelines ensure continuity through version-controlled deployments and rollback capabilities. Application security is no longer dependent on static defenses, but rather on perpetual movement and deception.

Strategic Benefits and Operational Impact

RAVID offers transformational advantages across three key vectors: security, performance, and cost. It significantly reduces the risk of breaches by making systems hard to find, harder to target, and nearly impossible to persist within. Automated movement and failover lead to lower downtime, while virtualized infrastructure lowers dependency on expensive hardware and long-term licenses.

Operationally, RAVID simplifies management by integrating seamlessly into existing DevSecOps pipelines. Security postures become proactive rather than reactive, supported by rich telemetry and adaptive threat response mechanisms. Legacy systems can be wrapped with RAVID techniques, extending their life while modernizing the security architecture.

RAVID – The Solution

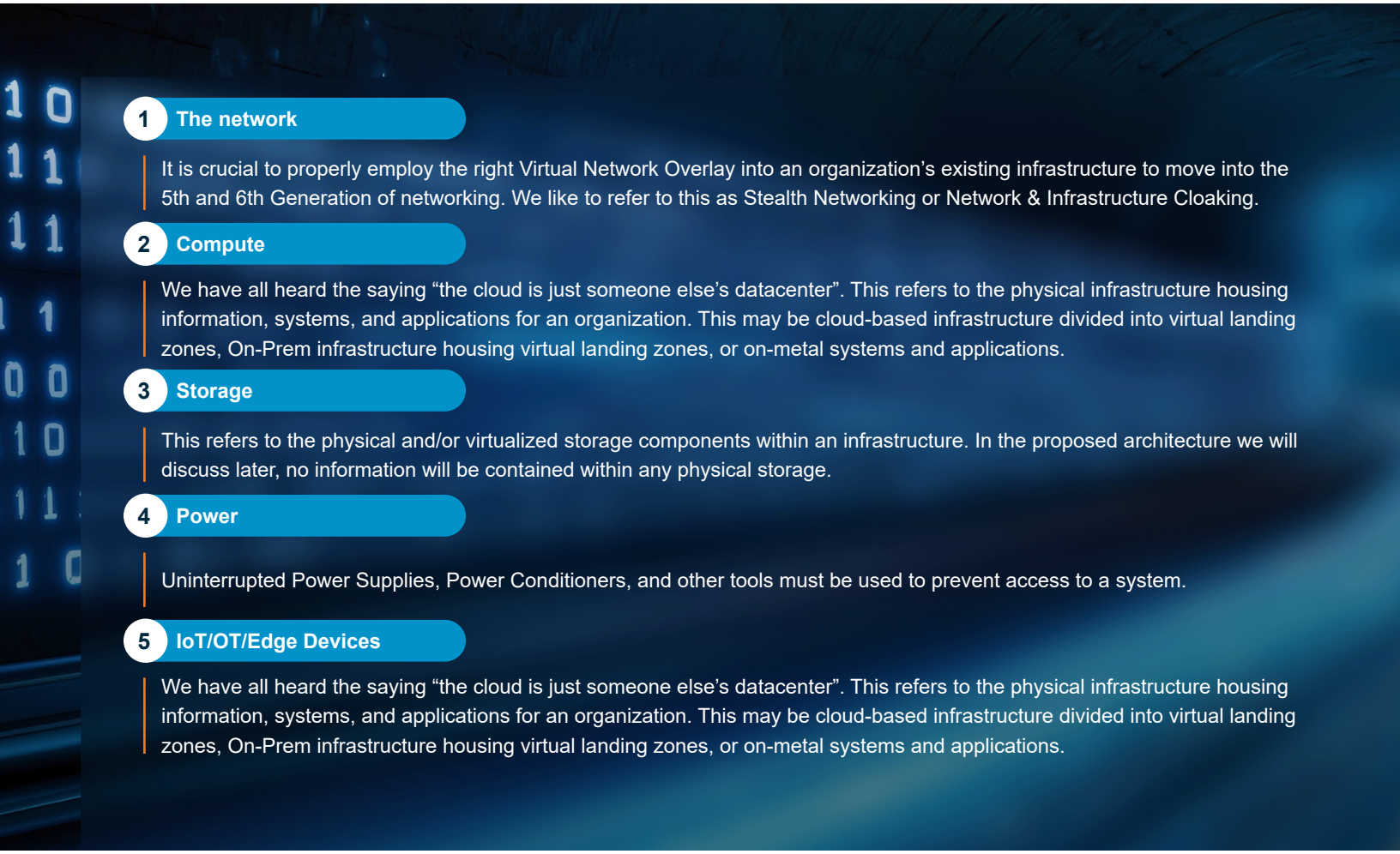
Defining the Virtual Battlefield

One of the great things the Marine Corps SIGINT community taught Team Tyto was how to plan, and more importantly, how to think about planning. We would use concepts like orientation and changing perspective to get the entire team aligned to the battlefield. Those of you who have served likely remember much of this.

The topo team (Topography) would use the sand table to create a 3D version of the battlespace--complete with hills and valleys, fences, buildings, etc. We would then go over a proposed plan. After orienting the group towards North, the committee would talk through the coordinated movement and assign initial responsibilities.

Knowing that no plan survives first contact, the group would make changes, adapt the plan, and agree on next steps.

After aligning the virtual map over the battlefield, let's consider: how would an adversary attack you? Let's examine the cardinal areas that need to be protected for a fully secure architecture.



1 The network

It is crucial to properly employ the right Virtual Network Overlay into an organization's existing infrastructure to move into the 5th and 6th Generation of networking. We like to refer to this as Stealth Networking or Network & Infrastructure Cloaking.

2 Compute

We have all heard the saying "the cloud is just someone else's datacenter". This refers to the physical infrastructure housing information, systems, and applications for an organization. This may be cloud-based infrastructure divided into virtual landing zones, On-Prem infrastructure housing virtual landing zones, or on-metal systems and applications.

3 Storage

This refers to the physical and/or virtualized storage components within an infrastructure. In the proposed architecture we will discuss later, no information will be contained within any physical storage.

4 Power

Uninterrupted Power Supplies, Power Conditioners, and other tools must be used to prevent access to a system.

5 IoT/OT/Edge Devices

We have all heard the saying "the cloud is just someone else's datacenter". This refers to the physical infrastructure housing information, systems, and applications for an organization. This may be cloud-based infrastructure divided into virtual landing zones, On-Prem infrastructure housing virtual landing zones, or on-metal systems and applications.

Considering current systems in the context of historical warfare gives us an understanding of maturity. As warfare moved from trench warfare to stealth fighters, it became continually harder to hit one's target. From stationary, to movement, to an ever-progressing increase in speed and maneuverability, it was difficult for targeting and detection systems to keep up.

It is infinitely harder to detect or attack a moving target. It is then exponentially more difficult to identify or attack that moving target if it has a stealth capability.

When it comes to our adversaries, they can't attack what they can't find.

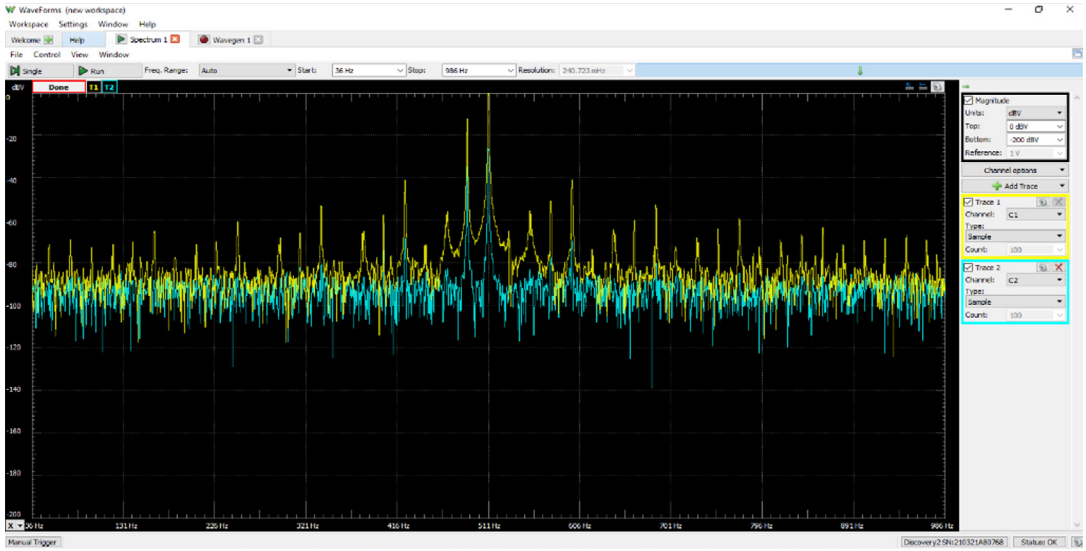
Finding the Signal in the Noise

The network has traditionally been the most vulnerable part of our systems. We count on legacy practices and tools such as encryption and VPNs to protect our data, but they are no longer sufficient and are exceedingly expensive at scale.

From an information warfare perspective, most attacks begin with the network. Although the attack may not specifically be on a network component or the network itself, threat actors are able to gain insight through legacy systems and networks. Information such as source and destination of a VPN.

Although they may not break encryption in real time, they are able to identify flows of interest and monitor for future transmissions. Handshakes, and entire streams of data are captured for offline processing, or what is called Harvest Now, Decrypt Later (HNDL) attacks.

Other attacks are also informed from the network, potentially presenting the source and destination of an IP transmission, allowing a threat actor to triangulate friendly locations for further attack.



This process closely mirrors the methods historically used to intercept enemy communications within the Marine Corps Signals Intelligence (SIGINT) community. Operators would monitor the electromagnetic spectrum continuously, a practice colloquially referred to as “spinning and grinning.” This entailed manually rotating a dial to sweep forward and backward through radio frequencies in search of signals of interest

The spectrum analyzer (shown above) display would show a shifting noise floor as the dial moved. Occasionally, a distinct signal would pierce through the ambient noise. Operators would then fine-tune the dial to isolate that spike, allowing them to intercept and analyze the transmission. Directional analysis tools were used to determine the signal’s azimuth, which was then communicated to other collection sites. The azimuth and frequency would be passed to other friendly collection locations so they too could tune in, listen, and determine an azimuth from their location. This led to the triangulation, or location of the enemy transmission.

As adversaries began encrypting their transmissions, the content became inaccessible in real time. However, the signal itself could still be captured and stored for offline decryption—an approach analogous to modern Harvest Now, Decrypt Later (HNDL) cyberattack strategies. Despite encryption, triangulation and subsequent targeting of the source remained feasible, underscoring the vulnerabilities inherent in legacy communication systems.

The next progression in radio communications that is mimicked in today’s cyber communications would be the concept of frequency hopping. In the world of VPN technologies, many have heard of a “Hopping VPN” - a VPN that moves from one path to another systematically over time. Similarly, frequency-hopping rendered manual tracking ineffective, as signals would appear and vanish across the spectrum unpredictably. Computational tools were required to track these transient signals and reassemble them into coherent data streams.

While manual azimuth determination became obsolete, digital systems enabled continued signal tracking and offline processing. Adversaries operating under the assumption of stealth found their efforts undermined by superior signal intelligence capabilities. Although they believed they were moving quickly enough to remain undetected, they underestimated the persistence and precision of the tracking systems.

This principle remains relevant in today’s cyber domain. Most IT infrastructures are static and easily located, which means they can be identified and targeted with enough time. Without adopting adaptive, stealth-based architectures, organizations remain highly vulnerable in a threat landscape that continues to accelerate.

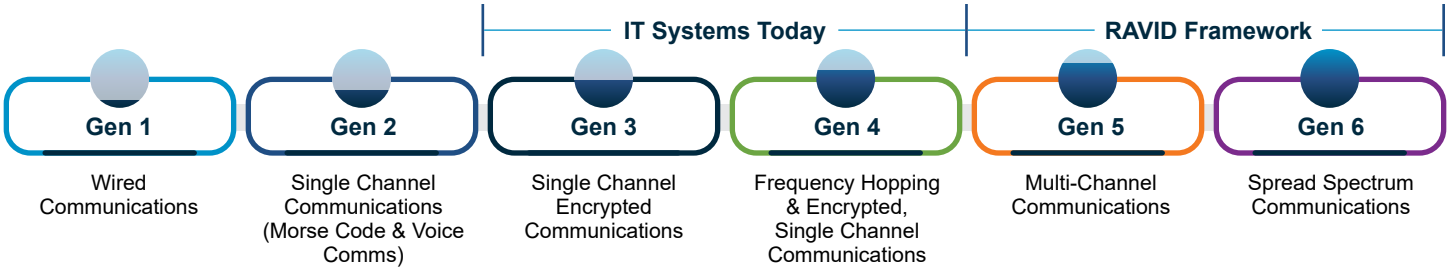
The Network: Radio Communications or Cyber Communications, the Solution is the Same

Applying the lessons learned from Spread Spectrum communications to the virtual world

The TTPs required to protect SCI information and leverage spread spectrum communications are well-established. We will cover several areas, starting with the Network.

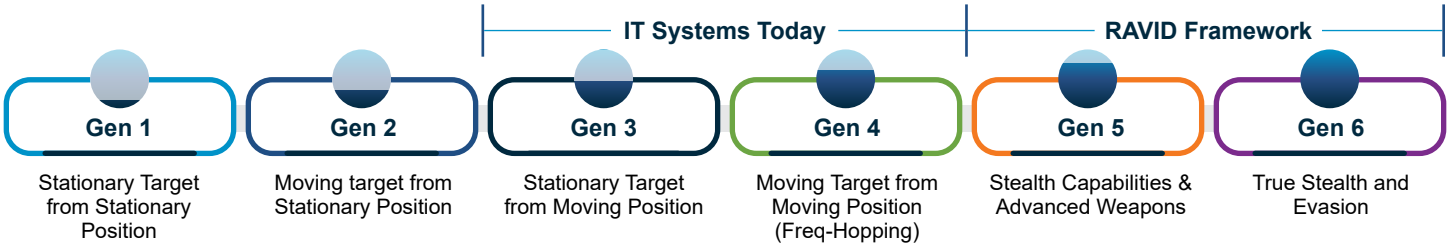
It's time to move away from point-to-point network communications with singular encrypted pathways responsible for security. Leveraging the stealth networking capabilities described in this document brings forward the security and efficiency of spread spectrum communications applied to the cyber battlefield.

For intelligence professionals, this switch was transformative. Traditionally, signals would appear separately from the noise floor. With the adoption of spread spectrum methods, those signals no longer stood apart. They were dispersed across the spectrum, effectively concealed within ambient noise. As a result, no single signal fragment contained meaningful intelligence on its own. As with data at the SCI level, the secret was distributed and hidden.



The evolutional maturity of most deployed systems today

In the cyber battlefield, most systems are employing 3rd and 4th generation defenses against 5th and 6th generation attacks. This is evidenced by the ever-growing number of hacks seen throughout our news feeds.



Even "modern" offerings such as those from ZScaler are leveraging legacy VPN and MPLS technology for communications. This macro-segmentation is the original answer to preventing lateral movement within an environment. In the case of ZScaler, they have a mesh of these legacy connections, with computers acting as virtual traffic cops monitoring IO flow.

These systems are incredibly expensive and complex to adopt and add latency overhead, often detrimental to operational systems. This requires large teams and expenses to adapt existing tools and applications into the new infrastructure. Finally, they require a rip-and-replace type solution of existing IT purchases, regardless of planned end of life.

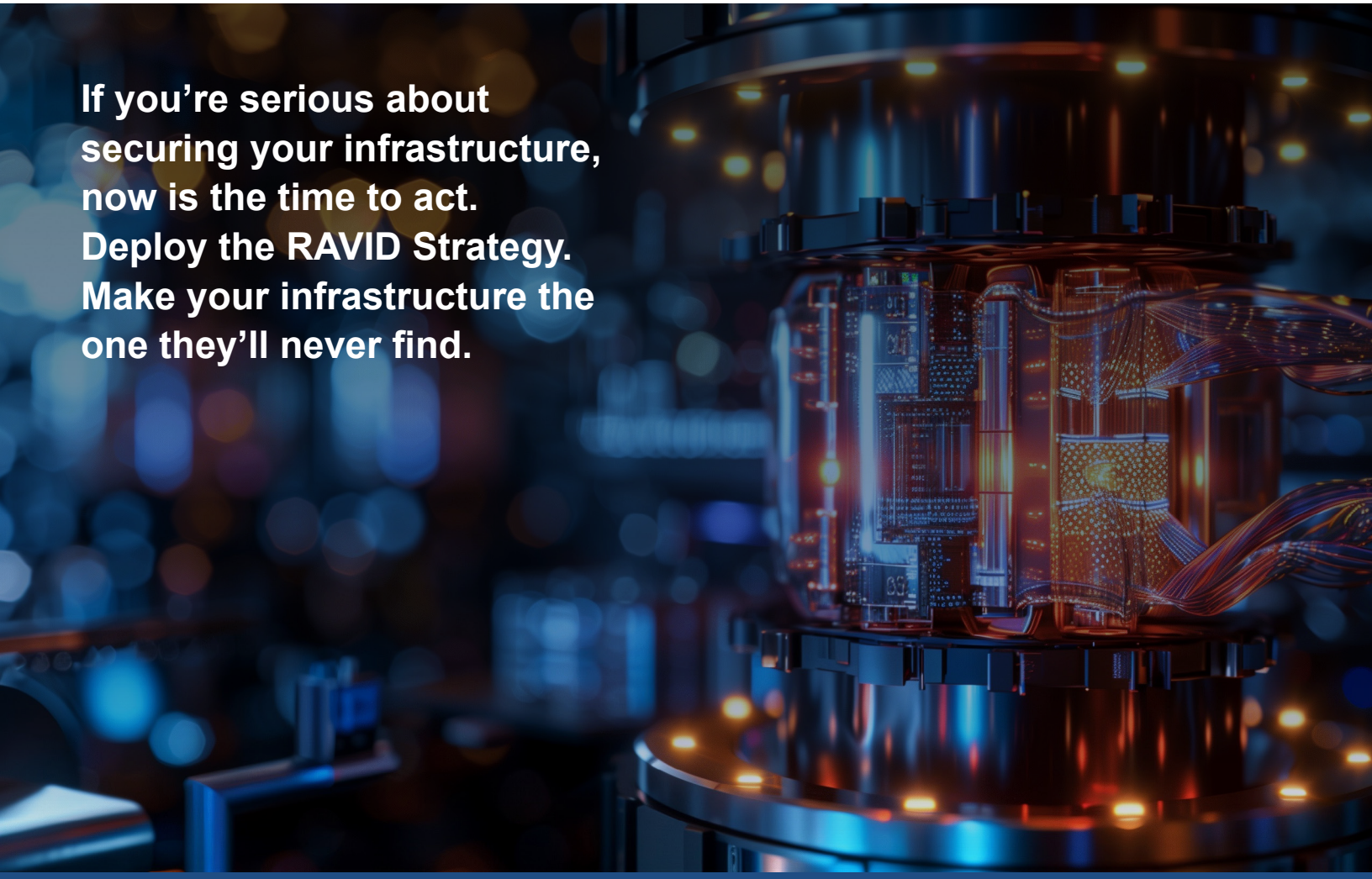
From a threat actor's perspective, what these legacy systems have in common is that all components are stationary. The physical infrastructure is predictable and easily navigated, while the virtual infrastructure within remains stationary. For example, an API endpoint remains in one location withstanding repeated assault attempts, in wait for a proper authentication to be executed.

Conclusion: Now Is the Time to Move

The era of static defenses is over. In a digital battlespace where adversaries are agile, adaptive, and relentless, we must abandon the illusion that perimeter firewalls and stationary systems will keep systems safe. RAVID offers more than a defensive framework. It offers a paradigm shifts to a proactive, stealth-based architecture that renders digital infrastructure observable to friendly forces, while being elusive, unpredictable, and resilient to threats.

Much like the evolution of warfare from stationary infantry lines to stealth fighters, the future of cyber defense lies in perpetual motion, deception, and orchestration. RAVID doesn't just defend; it maneuvers. It learns, adapts, and survives. It makes your systems harder to find, harder to target, and nearly impossible to exploit.

This is a call to leaders, architects, and defenders: adopt a strategy that reflects the battlefield as it truly exists. RAVID empowers you to fight smarter, stay ahead, and secure the mission-critical systems that modern life depends on.



About Tyto Athene

Tyto Athene delivers mission-focused solutions that keep critical missions future-focused and future-ready. We utilize adaptive architecture and continuous integration to secure essential data, so our clients can make informed decisions, create decisive advantages, and drive dominance. We do more than solve the needs of now, we deploy what's next.

TYTO Athene

DATA TO DOMINANCE

For more information about our digital transformation services, please email bd@gotyto.com

/company/gotyto

https://gotyto.com