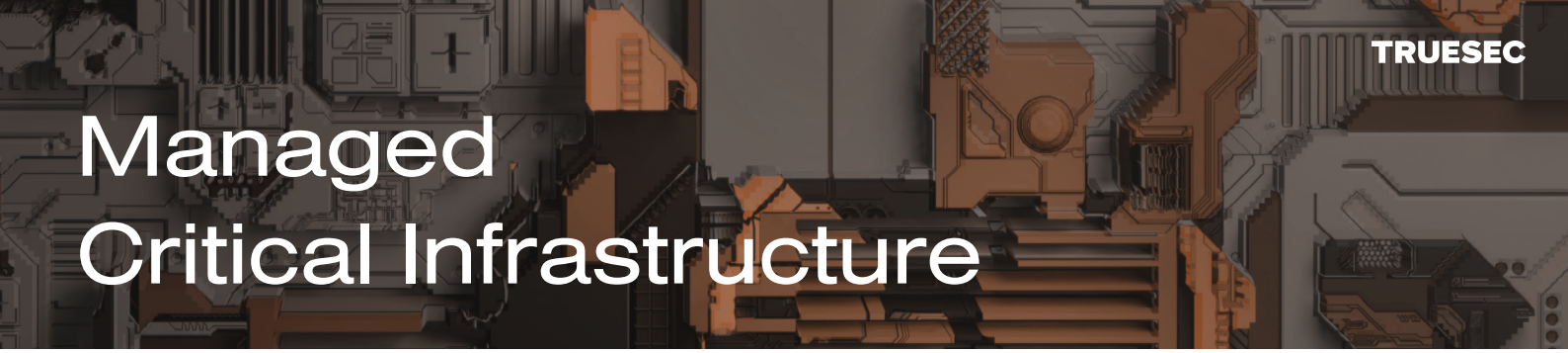

TRUESEC

Managed Critical Infrastructure

What's Managed Critical Infrastructure?

When operating a modern IT infrastructure, a core concept is to utilize tiering/segmentation or a Zero Trust design.

Tiering creates an environment where the most critical data is kept in the most secure tier, with management access available only to Tier 0 administrators. This makes it more difficult for cybercriminals' lateral movement and subsequent credential elevation within your IT environment.

Unfortunately, when working in different IT environments, we rarely see this type of tiering implemented. It's often assumed that such a project will be a lengthy, complex undertaking, which makes organizations apprehensive about implementing the change.

With Truesec's MCI service, you'll gain a more secure infrastructure and a managed service to secure the most critical infrastructure in your organization's IT environment.

With MCI you'll gain:

- Tiering implementation using a battle-proven, efficient method.
- A more secure environment initally focusing on Tier 0, which then can be managed externally by Truesec or internally by your own organization.
- The ability to protect your most valuable assets and systems without adding complexity for the business.
- Advice from Truesec on how to continually increase your cyber resilience.

What We Do

We'll protect your organization from digital threats by securing your most critical infrastructure. To do this, we begin with a secure architecture design and implementation focused on Tier 0. This is usually implemented in your environment within a few days without impacting your business.

Not only will we set up the basis for Tier 0 security, but we'll also implement Tier 1, Tier 2, and a tier for endpoints. These are fully operational and are preferably used by your operations team to secure more of your environment.

We'll move the Tier 0 systems (e.g., domain controllers, certificate servers, etc.) into the newly secure Tier 0, and from then on, we'll manage and operate these services. This will include all the necessary time for communications, questions from your operations team, and work according to the service (including weekends).

About Us

As a global cybersecurity company, we're proud to be at the forefront of protecting organizations and our society against cyber threats. Our purpose has been clear since day one: Creating safety and sustainability in a digital world by preventing cyber breach and minimizing impact. We never cease to challenge and reinvent ourselves to help defend your most valuable data assets every day.

TRUESEC

A Safe Digital Future

Contact Us

truesec.com hello@truesec.com

The Truesec Promise

We always strive for the best results for our customers.
That's a Truesec promise.

What We've Learned

We're one of the most trusted organizations in cyber incident response, collaborating with global leaders in the community to learn and educate. One of the more common techniques we see cybercriminals use is moving laterally through networks (e.g., from computer to computer) until they find credentials that allow them to elevate their privileges. They continue to do this until they obtain domain admin access.

Thanks to a tiered model for the Active Directory, the attacker will not find anything outside of the tier they're in.

By implementing tiering, we create multiple zones, or "tiers," that separate frequently compromised devices such as regular workstations from the valuable ones (e.g., domain controllers, backup systems, PKI, and other business-critical applications or systems).

After the implementation, we then deliver management of Tier 0 as a managed service (see overview for Active Directory Tiering Implementation for more information about tiering).

Implementation Deliverables

Depending on the exact design and requirements for each customer environment, the precise scope of each implementation can vary. Here are some frequently included deliverables:

- Active Directory
- Certificates
- Deployment
- Documentation (including scripts)
- Active Directory Federation Services (AFDS)
- Hardware Templates
- Patch Management
- Monitoring
- Remote Management
- Automation
- Reference Image (Windows Server)
- VM Templates (Windows Server)
- Software Defined Networking
- Software Defined Storage (Scale-Out File Servers)
- Software Defined Compute (Hyper-V Hosts)
- Windows Azure Pack for Self Service of Virtual Machines

Typical Deliverables

A high-level summary of day-to-day operations:

- Tier 0 level access model and process
- Maintenance activities
- Change process
- Report and verification
- User support model

How To Get Started With Managed Critical Infrastructure

Start by talking to your Truesec customer contact or any of our experts. Together we'll begin the journey to protect your organization's sensitive information and safeguard your corporate brand by scoping the assignment and determining what actions would benefit your organization the most.

By implementing AD Tiering, you'll acquire experts who use a battle-proven, efficient methodology to implement and document tiering without impacting your business. This will increase your capability to protect your most valuable assets and systems. Additionally, by having MCI as a service, you can be assured that your organization is up to date and will always have experts to turn to for advice.

Contact Us
truesec.com
hello@truesec.com