Professional Services

JOINT (Guide, Do & Review): Accelerating Your Implementation

Our JOINT (Guide, Do & Review) implementation offering is designed for customers who wish to accelerate their Guardicore deployment while implementing and managing subsequent policies themselves with guidance from our experts. Working alongside our experts as we implement your first security policy objective will give your team the training required to implement future policies in your datacenter and/or cloud environments self-sufficiently.

Our team will work with you to plan the security architecture and assess any application design considerations. This includes everything from defining and documenting the labelling strategy, to labelling your assets in Guardicore Centra, to the formal creation and fine-tuning of policies to support your use-case(s).

After the first policy implementation, our engineers will continue to provide assistance as your team implements future policies, remaining part of your extended team until your policy and protection objectives are met.

TURNKEY: Comprehensive Implementation

Our TURNKEY implementation offering is designed for customers who require complete, end-to-end implementation assistance for the design, implementation, and management of their Guardicore implementation.

Our team will work with you to plan the security architecture and assess any application design considerations. This includes everything from defining and documenting the labelling strategy, to labelling your assets in Guardicore Centra, to the formal creation and fine-tuning of policies to support multiple security initiatives.

As part of this offering, you may select from our policy objectives to ensure that your Guardicore implementation achieves specific desired outcomes. You may select multiple policy objectives, or focus on a specific high-priority objective. Our engineers will implement the required labels and rules to create a set of policies that align with your pre-identified objectives.
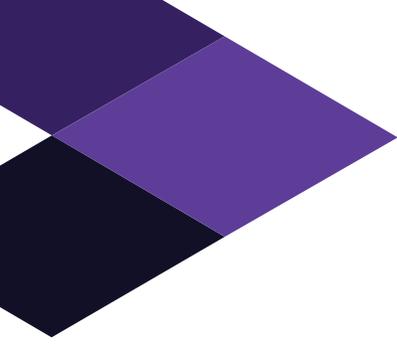
Policy Use Cases:

- **Environment Segmentation** - Servers from different environments will not be allowed to communicate, except for explicitly allowed communications.

- **Application Ring-Fencing** - Critical applications should only communicate with explicitly allowed parties. Internal application communications will be allowed.

- **Application Micro-Segmentation** - Internal and external traffic of critical applications will only be allowed if explicitly approved ("zero trust").

- **Control Privileged Access to Server**s - Server access control policy, for example; restricting management ports to jump boxes only, or preventing access to specific servers based on user-identity of the source.

- **Security Best Practices Enforcement** - Implementation of 'blacklist' rules to enforce network security best practices

Task	JOINT	TURNKEY
Architecture Planning	✓	✓
Installation (SaaS or On-Prem)	✓	✓
Implementation of Labelling Schema	✓	✓
Guidance on Policy Creation	✓	✓
Implement Guardicore Policy	1x Policy	Unlimited[1]
End User Training	✓	✓

[1] Turnkey includes a set number of days to accomplish your policy goals.

Guardicore

Guardicore

About Guardicore

Guardicore is a data center and cloud security company that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security – for any application, in any IT environment.

More information is available at www.guardicore.com