

EBOOK #2

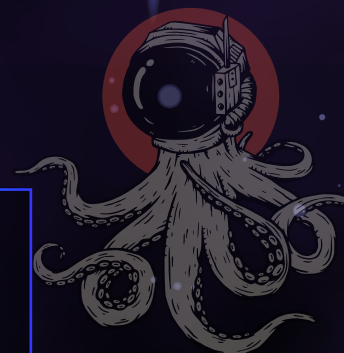
---

# How to Spot Monsters

Identity management is core  
to Zero Trust



**GUIDEPOINT**  
SECURITY



# How to Spot Monsters

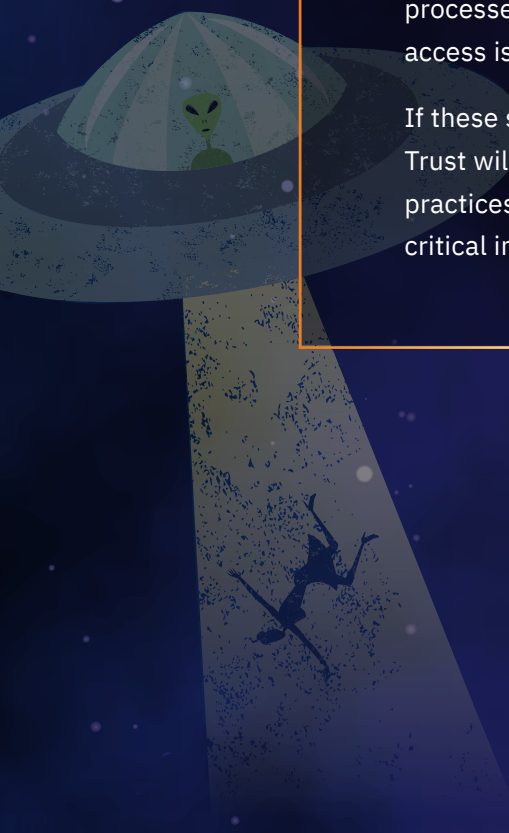
## Identity management is core to Zero Trust

With Zero Trust, access is enforced for *any* subject that is accessing applications or data. To achieve true Zero Trust, the access decision needs to be based on not only the positive identification of the subject, but also other contextual information, like the health of the endpoint the subject is using and the health of the network where the request originates.

Identity Management is at the heart of Zero Trust. Information about the endpoint and the source network gives additional context, but the subject's identity is central in making access decisions. Knowing the subject and the types of authorizations they have is key to any access decision.

Because Zero Trust relies on near-real time information about users and their authorizations, it is essential that underlying business processes are automated so that information about users and their access is current.

If these supporting processes are inefficient, enforcement of Zero Trust will be impossible. Creating efficient Identity Management practices and automating key Identity Management processes are critical in achieving true Zero Trust enforcement.



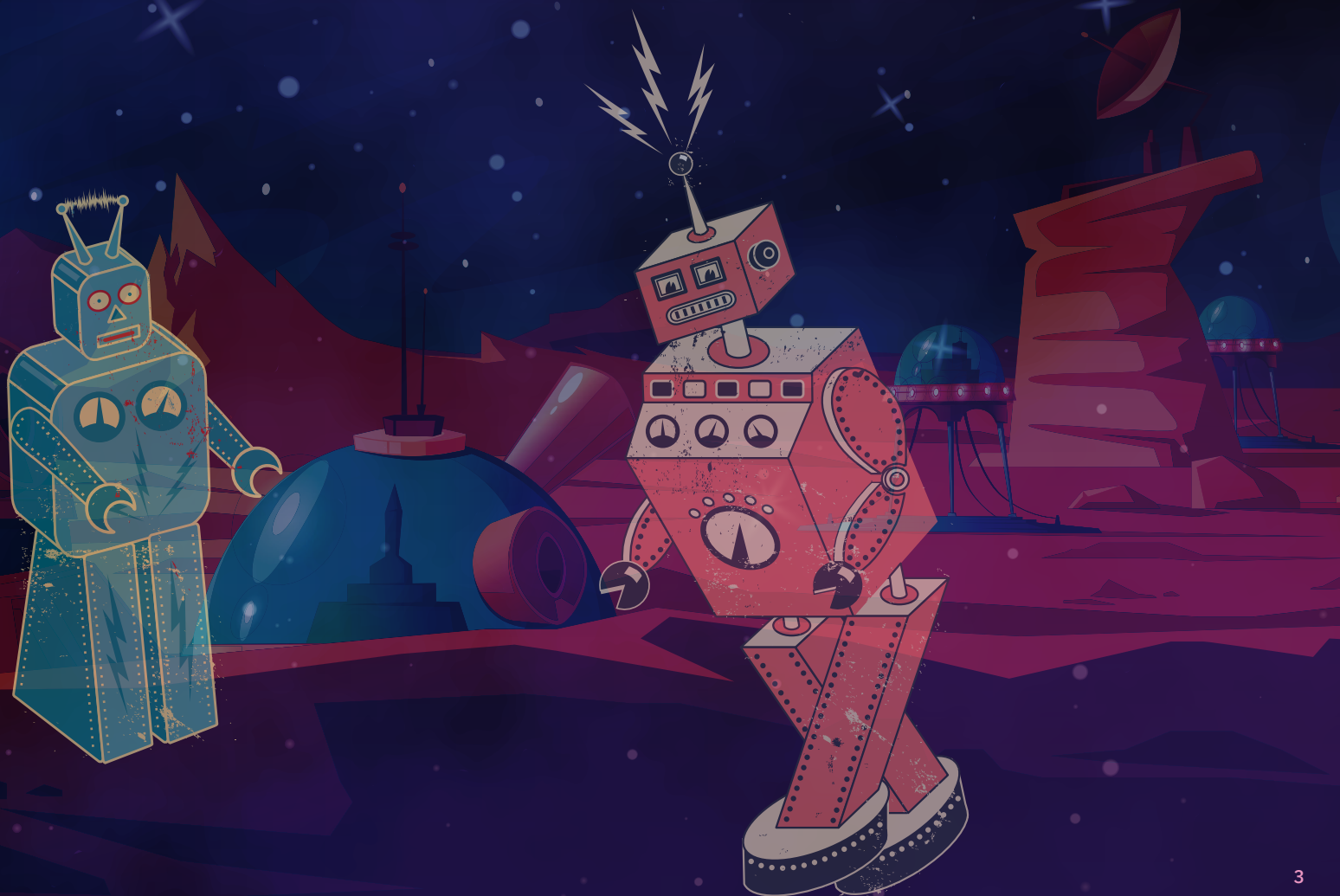


# Building Your Killer Robot Base

## Architectural requirements for Zero Trust

Once all the core capabilities are implemented and key security functions and business processes are automated, the next part is orchestration. Orchestration involves integration with technology solutions at the network and endpoints that evaluate risks and present this information to a policy enforcement point (PEP). The PEP(s) will use this in addition to other information such as the location of the subject, time of access, and behavioral data to enforce real-time access decisions.

Each infrastructure layer will need analytics and risk scoring capabilities to determine the overall health of the layer, possibly based on a confidence score. The orchestration layer collects the risk information and presents it to policy enforcement points.






# From Here to Planet Z

## The capability journey

The journey from legacy security to the enforcement of Zero Trust is agile and incremental. Stage one requires organizations to determine what they're missing regarding foundational security capabilities and acquire them. Stage two is improving the maturity of those foundational pieces to improve coverage, increase automation, and implement analytics capabilities. Organizations that already have foundational capabilities in place can further improve coverage and reduce risk through ongoing integrations before starting Zero Trust.

These two stages will improve overall security maturity and position organizations to implement a full Zero Trust Architecture



To get you started on your way to Zero Trust adoption, check out GuidePoint Security's comprehensive consulting **workshops** or **contact us** for more information.



# GUIDEPOINT

SECURITY



2201 Cooperative Way, Suite 225, Herndon, VA 20171  
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132  
06.2022