Reveal

Autonomous application visibility for seamless threat modeling

Automated Threat Modeling with Reveal

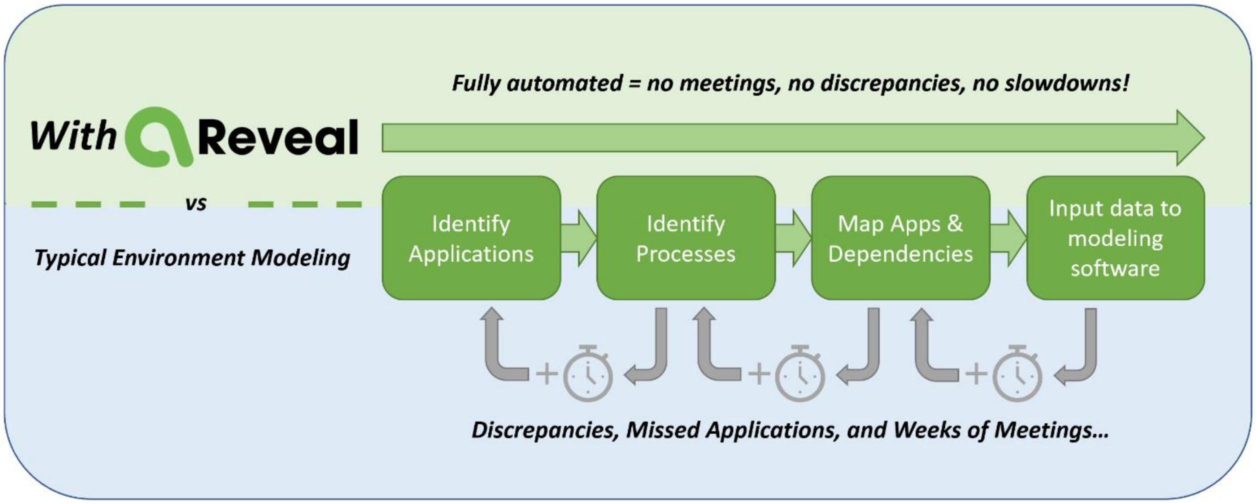
Threat modeling, the act of building & testing a modeled environment against modern threats, is an essential practice for every company. This helps gain a comprehensive understanding of one's attack surface, build a defense strategy, and guarantee their security in an everchanging paradigm.

Modern threats are often persistent and malicious that migrate laterally through web apps, internal enterprise applications, and databases. Properly mapping your application flows, dependencies, and infrastructure is critical for an accurate threat modeling.

This exhaustive process can take hundreds of engineering man-hours, requiring meetings with dozens of internal IT engineers, architects, application managers, etc. just to understand the application's location, open ports, APIs and allowed connections to the outside world. As enterprises trend towards zero-trust architectures, application behavior becomes even more difficult to manage, as it requires extensive knowledge of all whitelisted communications for every domain.

Often, this manual process fails to uncover all application behavior, especially with 3-tier applications like web portals and business apps. These discrepancies can lead to massive holes in one's east-west security system, leaving critical paths to user data and exfiltration open. As a result, failing the threat modeling.

Avocado Reveal™ is our latest revolution in inside-out application visibility. The new gold standard of deep visibility for threat modeling is here to provide gap-free coverage with minimal or no involvement, saving enterprises time and money while helping minimize cyber risk.



Fully automated = no meetings, no discrepancies, no slowdowns!

With Reveal

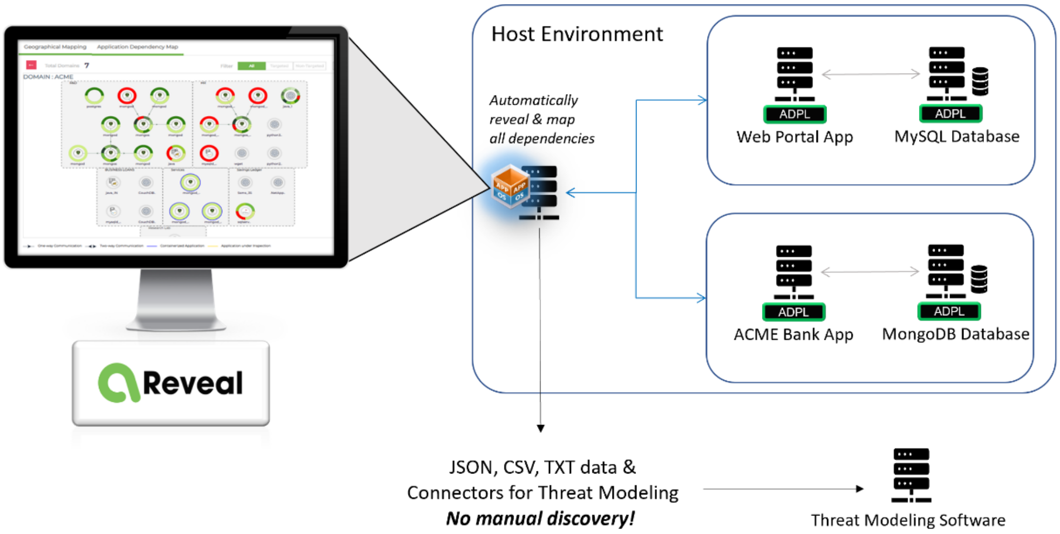
vs

Typical Environment Modeling

Identify Applications → Identify Processes → Map Apps & Dependencies → Input data to modeling software

Discrepancies, Missed Applications, and Weeks of Meetings…

Reveal



Automation for Cost Optimization & Gap-Free Coverage

Save time and money by removing developers and designers from the threat modeling process. Reveal enables enterprises with:

- Automated application discovery everywhere
- Identifying dependencies & generating matrices (data flow diagrams)
- Automated discovery of API's, URL's, etc.
- Feeding JSON information into industry-leading threat modeler software

Threat modeling helps understand how apps respond to threats in your ecosystem. Ensure complete coverage by using Reveal to:

- Map application components that even developers may be unaware of
- Understand multi-faceted 3-tier application flows with ease
- Support all proprietary & open-source applications in any language

Extensive Support & Integrations

Native Supports:

- All major cloud providers & container deployments
- On-prem: Bare-metal, Virtualized, and Containerized
- Universal Windows & Linux support for Java, C/C++, Python, etc. (including legacy apps)
- Custom support for Microsoft applications (Sharepoint, Exchange, IIS)

Full Programmability & Integrations:

- Scriptable with REST API's throughout
- JSON, .csv, .txt, .pdf, & standard outputs

aws splunk> Azure servicenow kubernetes Google Cloud