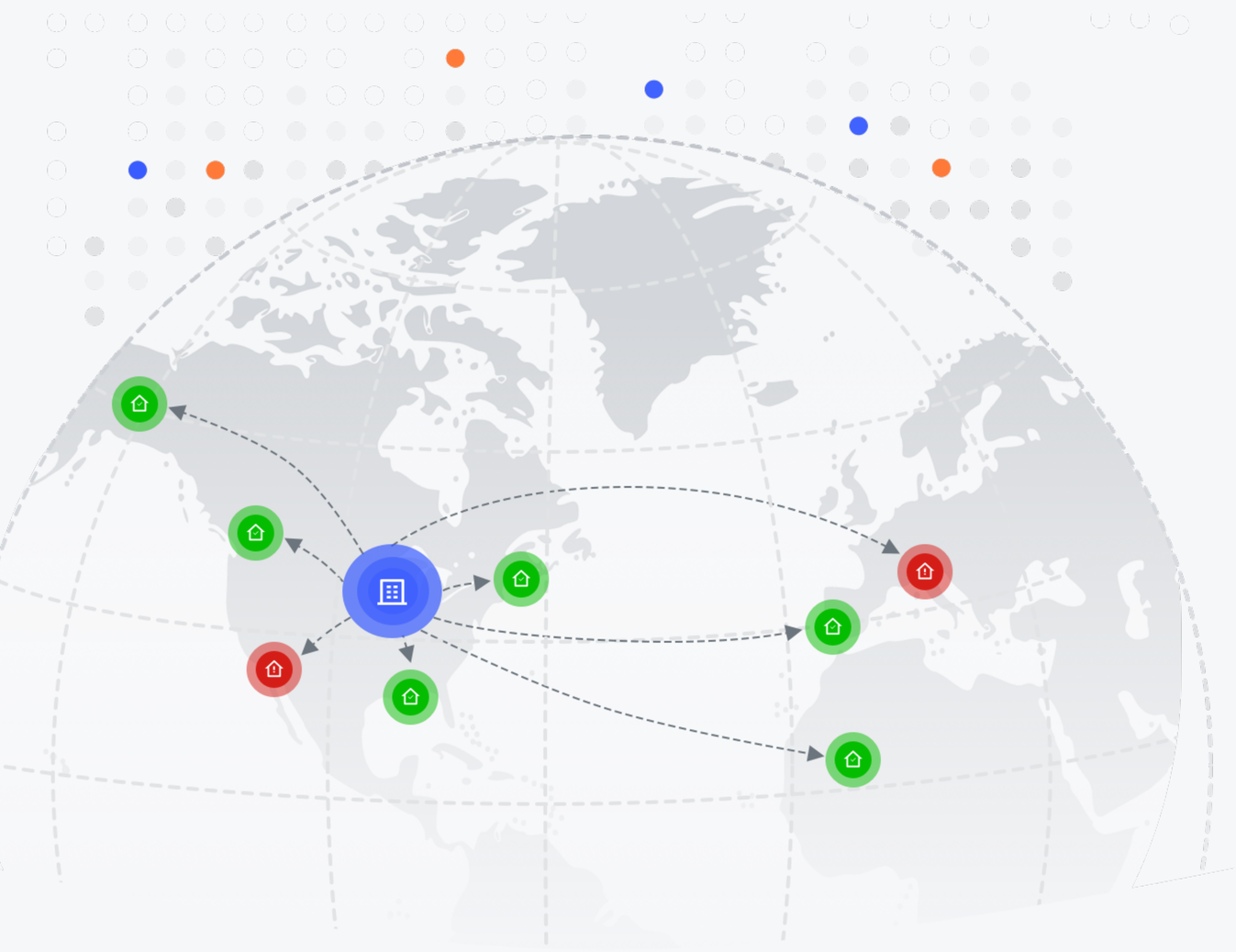
YOUR NEW ATTACK SURFACE

Employee Home Networks

The Enterprise Attack Surface has Grown over 600% with Remote Work

As a result of a mass trend to work from home, the "Attack Surface" that we once knew, made up of Internet-facing corporate assets, exploded to include the entire remote workforce, without traditional asset monitoring for those home networks.

As enterprises consider the feasibility of semi-permanent remote work in the future, Censys can help organizations and enterprises discover and protect the new shape of their attack surface.



Censys Enterprise HNRI Tool Identifies:

- **Exposed IOT and embedded devices**, such as cameras and routers
- **Remote desktop sharing**, such as PCAnywhere and RDP
- **Exposed Microsoft LAN protocols like SMB -** a popular vector for ransomware
- **Exposed telnet, FTP, and the like -** plaintext services found on many IOT devices and home routers - many with default credentials
- **Network management exposures**, such as Intel AMT and SNMP

Why Censys?

Censys provides an automated monitoring solution, integrated with your existing IT work flow, to scan your employees' home networks for exposures and vulnerabilities. The Censys HNRI ASM tool allows you to map your workforce, alerts you when risks are detected and allows you to investigate changes over time.

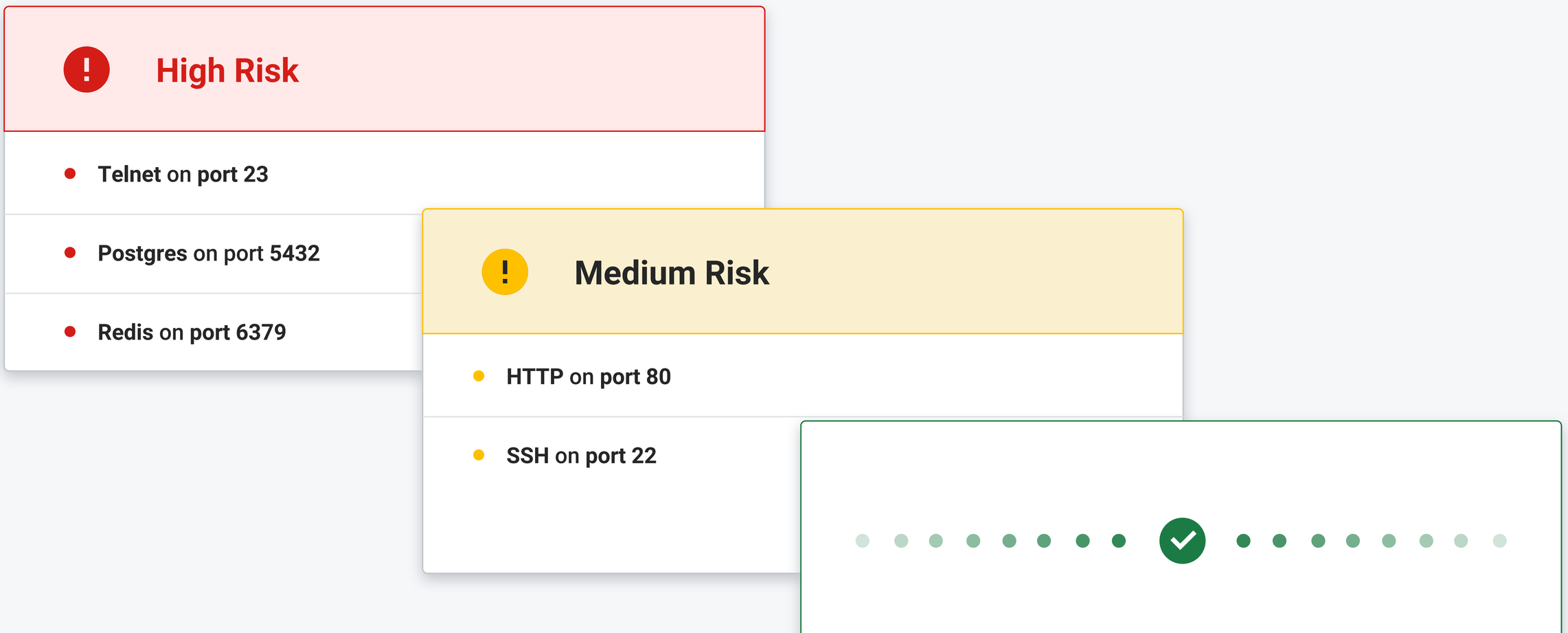
LEARN MORE AT CENSYS.IO/PRODUCT/HNRI

THE NEW FRONTIER IN ENTERPRISE SECURITY

Home Networks

Censys provides a free version of our **Home Network Risk Identifier (HRNI)** tool that is available to all consumers. Anyone working from home can visit **https://me.censys.io** and instantly see any risks exposed on their home host.

HNRI free consumer tool highlights any risks, or confirms the network is secure



HNRI: Free Consumer Tool

This manual tool for remote workers allows users to send screenshots to their IT team when they discover something risky on their home network

SEE A DEMO

LEARN MORE AT CENSYS.IO/PRODUCT/HNRI