Find everything on your network, work out what it is, and keep it current.

Rebasoft runs as virtual appliances on your own infrastructure. It discovers continuously, without agents or subnet sweeps, and brings the network, servers, cloud and device management into a single asset inventory, matched to vulnerability and end-of-life data.

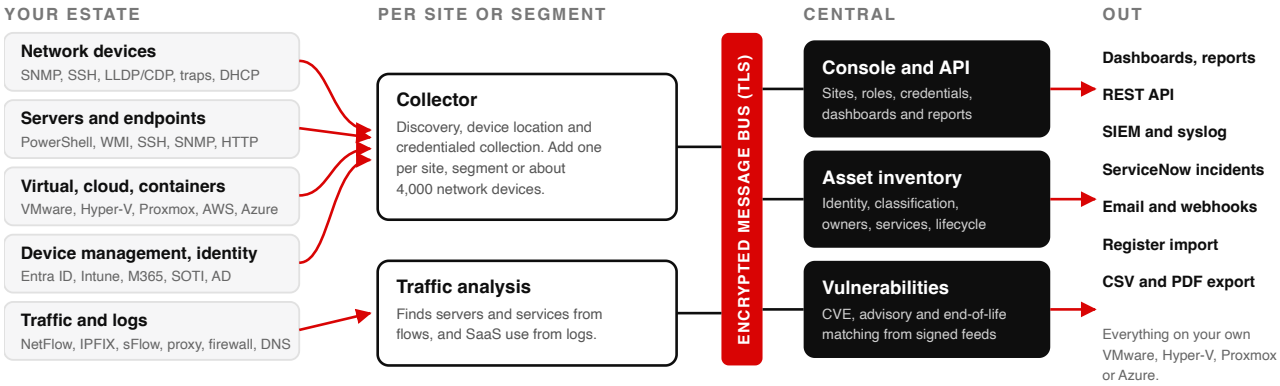
0
agents or endpoint changes needed

3 VMs
for production, up to about 1,000 network devices

Every port
every device located on its switch port

420,000
assets in the enterprise sizing scenario

HOW IT FITS TOGETHER



HOW DISCOVERY WORKS

01
Learn from the network
From a few seed switches and routers, it reads the ARP, MAC and LLDP/CDP tables the network already keeps, plus traps, DHCP relay and syslog as events happen. No subnet sweeps.

02
Locate every device
Each MAC address is placed on the access port where it connects, with its history. Uplinks and trunks are ignored, so you know where anything is and can spot unmanaged kit.

03
Collect the gentle way
For each host it checks a few ports and picks the least intrusive method that works. Every attempt is audited, and a rejected credential is locked out estate-wide, so accounts are never locked.

04
Resolve and enrich
Sightings merge on the strongest identifier: machine ID, hardware serial, then MAC. Software is matched to CVE and end-of-life data, and each asset carries its site, owner and service.

WHAT IT COLLECTS

Hosts: OS, hardware and serials, software and patches, services, local accounts and hardening settings. Printers, cameras, UPS and NAS over HTTP and IPP.

Network: interfaces, VLANs, neighbours, routes, health, configuration, and where every MAC address connects.

Cloud and virtual: VMs, disks, snapshots, networking and Kubernetes clusters, with the operating system inside each guest.

Progress you can see: every asset moves from detected to discovered, collected and attributed, with the reason any is held back.

SECURE BY DESIGN

Your data stays with you: each customer has its own deployment, and every host keeps its database locally, never exposed on the network.

Encrypted throughout: HTTPS (TLS 1.2 and 1.3) to the console and TLS on the bus. Credentials are encrypted for each collector and decrypted only at the moment of use.

Sign-in and roles: local users with MFA, LDAP/AD or Entra ID. Site-scoped roles apply to every page, report and API call.

Safe and audited: rate limits and cooldowns mean it cannot overload a device, and every user action and collection attempt is logged.

DEPLOYMENT AND SIZING

Production	Three VMs (console, collector, traffic analysis): up to about 1,000 network devices and 25,000 assets
Mid-size	Four VMs: up to about 2,500 network devices, 60,000 assets and 50 console users
Large, multi-site	Add a collector per site, segment or firewall zone; sized to 20,000 network devices and 420,000 assets

Virtual appliances for VMware, Hyper-V, Proxmox or Azure, with a single-VM option for evaluation. Run by your team or your partner, and extended with approved policies where the built-in collection does not reach.