REBASOFT

Customer use case: Software services

Organisation Profile

A £40 million software services business with 1000 staff spread across UK & EU countries. The IT team is based in Eastern Europe.

IT profile

The company uses Microsoft based systems. End-users connect via a dial-in VPN's or from remote locations. These are managed through several, non-integrated systems. Systems are managed in house using a variety of opensource and element managers.

Project Drivers

A digital transformation project was established to remove costs and streamline processes. The senior leadership team needed to improve security and gain a single pane of glass view across all elements of the infrastructure to improve response times to issues.

Evaluation and Proof of Concept (PoC)

Rebasoft was chosen for a PoC based on technical features, cost, and ease of deployment. The organisation also wanted to deliver quick results to meet project timeframes. The areas for evaluation were:

- Discover all assets, including hardware, OS, installed applications and enabled features
- Check systems against security policy:
    - Is anti-malware installed?
    - Is disk encryption enabled?
    - Are secure settings enabled to prevent users installing software or Autorun programs from running?
- Report & integrate with existing ticketing and executive reporting systems

Challenges

The organisation had opensource monitoring - Zabbix - to monitor servers and some elements of the network and element managers supporting their firewall and switching infrastructure. There was a degree of overlap in systems and little visibility on compliance with security policy. The other issue was that while there were company owned devices, development systems and supplier managed devices all joined the same flat network.

Developer PCs were often dual boot (Windows & Linux) and the automated patching systems struggled to ensure security controls were installed.

Rebasoft Approach

Rebasoft overcame the challenges

- Quick results: Rebasoft was pre-installed and delivered to site on a dedicated server
- Network data was collected from the existing Extreme networks switching infrastructure
- Configurations were collected directly from the firewalls
- End point data was collected with WMI to allow security compliance reporting

Little involvement was needed from the IT operations team, other than providing credentials and network access (firewall rules). Rebasoft did not need to install software agents on PC’s.

Rebasoft Benefits

The PoC delivered against the organisation’s stated needs:

- Automated discovery found all connected devices and built a reliable, accurate asset baseline
- Direct collection of data, including OS version, installed applications, enabled features was performed without the need for software agents
- Security compliance: endpoints missing malware, checking BitLocker was enabled and AutoPlay/Admin rights settings were simply reported, allowing easy identification of systems for remediation. This found almost 10% of their estate was missing the relevant security controls

Outcome

“We have built a robust security policy which protects the business and our users, and we take a common-sense approach. Rather than having 10 different security systems monitoring 10 different things, we decided to pull everything into one single system, because if you have a number of alerts being triggered in 10 different systems it is quite hard to track them through to conclusion. One system allows us to easily drill through to the issue and rapidly resolve it” – CIO

See for yourself how Rebasoft can improve any organisation’s cyber-resilience