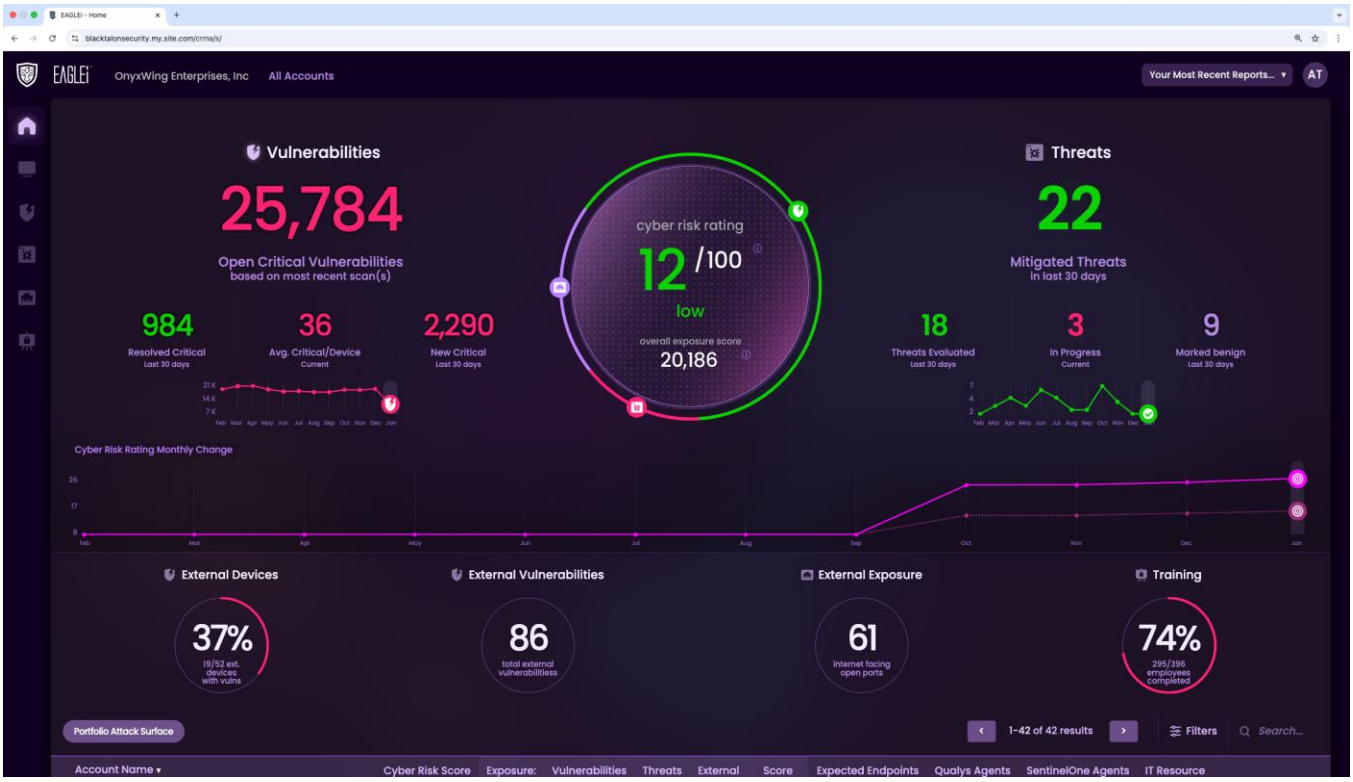
Frequently Asked Questions About EAGLEi

Clear Answers About EAGLEi for Your Business

Our FAQ section is designed to help you understand how EAGLEi strengthens your cybersecurity posture. From proactive vulnerability management to real-time threat response, get straightforward answers about our platform, automation capabilities, and the benefits for your IT team.

– What is a Cyber Risk Score Rating and what kind of data does it include?

EAGLEi Cyber Risk Rating Score is a combination of telemetry data from internal and external vulnerability scans, threat detection, and external exposure for ports and services. Telemetry data is continuously monitored and updated every 6 hours. The Cyber Risk Rating also includes healthcare specific, EAGLEi cybersecurity awareness training academy.



Having a cyber risk score is helpful, but can it tell us how we compare against similar healthcare organizations?

Yes, EAGLEi will allow you to benchmark and compare your organization risk score and overall cyber risk management against 2,000 plus EAGLEi customers securing over 50,000 devices.

– What is "Autonomous Remediation" and why is it important?

EAGlEi doesn't just identify vulnerabilities and leave you with a 150,000 line vulnerability report. EAGLEi takes swift action by "Automatically Remediating" as much as up to 70% of your vulnerabilities. This significantly streamlines your remediation effort, automatically patching and fixing known issues, while empowering your team to focus on the most critical security items at hand.

– We are a critical access hospital in rural America and find many cybersecurity solutions are too expensive and resource intensive for a small hospital like ours. Is EAGLEi affordable and a good fit technically?

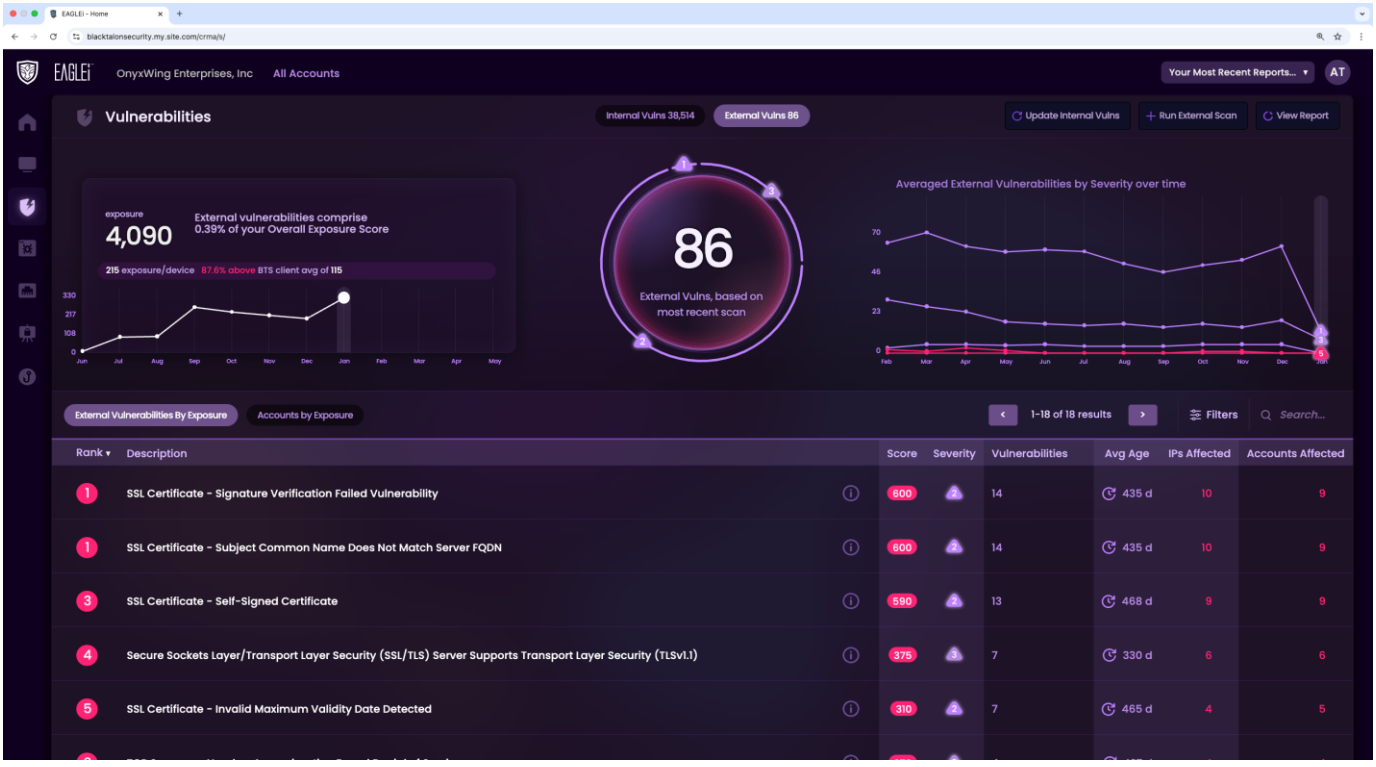
Yes, EAGLEi is an excellent fit both technically and affordable for small critical access hospitals, clinics, dental practices, etc. Pricing is based on a per device license (servers, firewalls, laptops, workstations, etc.) and has no minimum license requirement. EAGLEi does not require additional staff or complex cybersecurity knowledge. In fact, the automatic remediation feature alone will make up for your small staff and increase your effectiveness at protecting your critical access hospital.

Does EAGLEi provide any Managed End Point Detection and Response capabilities and if so, is it 24x7x365?

YES , EAGLEi provides 24x7x365 Managed End Point Detection and Response services. We currently utilize SentinalOne, but are already working on providing an option to utilize CrowdStrike in Q1 2026.

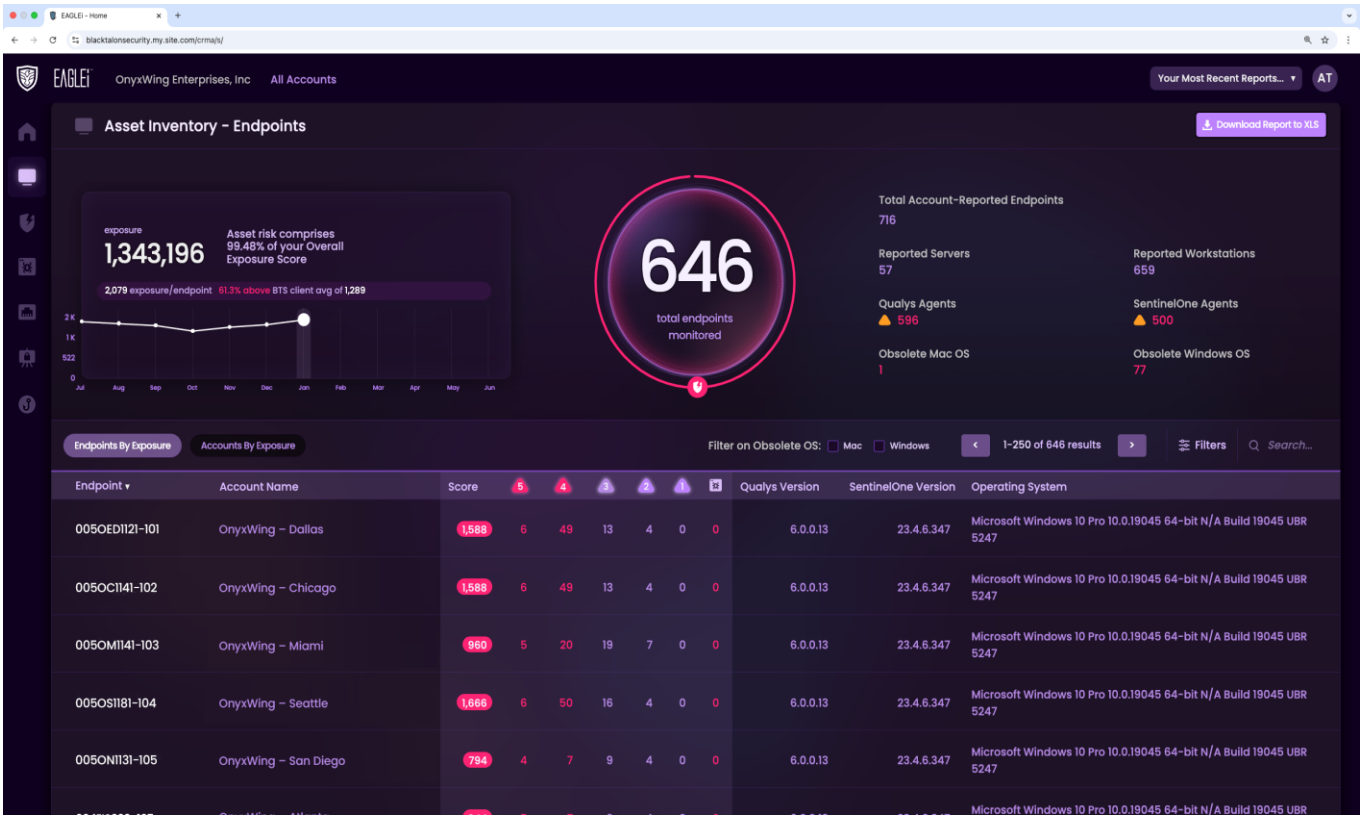
We just onboarded a new facility two months ago, can EAGLEi tell me how the new facility is doing from a risk perspective?

Yes, EAGLEi consolidates internal and external vulnerability data from many different sources to quickly illustrate your risk at an organizational level or allow you to drill down into a specific facility.



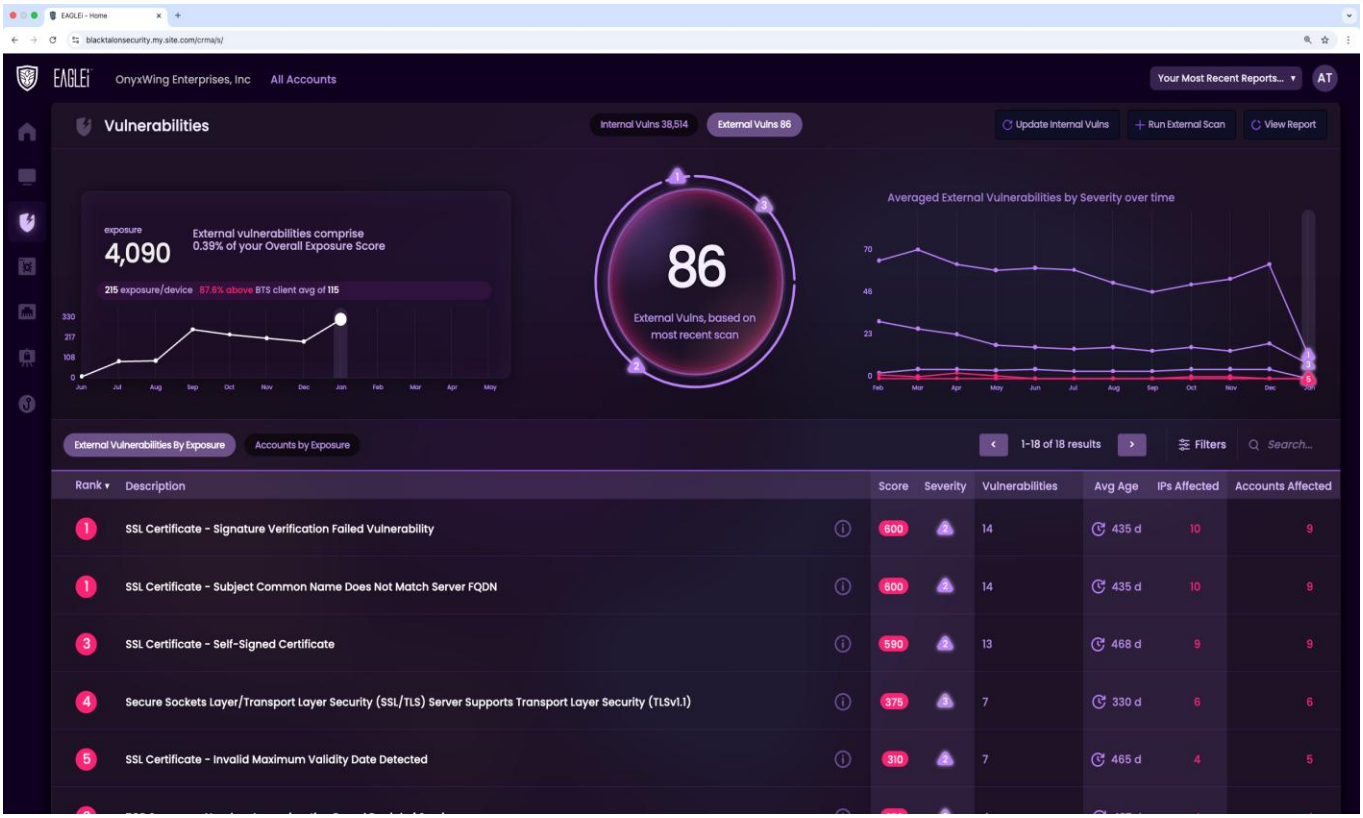
– Can EAGLEi help us create an IT asset inventory, as well as identify which endpoints are at more risk than others?

YES, EAGLEi scans your environment, discovering assets and ultimately creating a comprehensive IT asset Inventory. EAGLEi then assigns an exposure score to all your endpoints, so you can actually filter or sort the devices by exposure, low to high. You will be able to understand exactly what is wrong with a device from a security perspective and more importantly, understand if the device is contributing positively or negatively to your cyber risk rating.



- If my team only has two hours a day to focus on cyber risk, can you help them identify where to start? Too many cyber risk solutions simply provide an overwhelming excel report with 150,000 lines of vulnerabilities and leave them wondering where to start?

Instead of having to log into multiple consoles, and run reports, EAGLEi instantly provides identified threats (internal, external, specific software and device vulnerabilities) for the entire organization as well as down to individual physical locations. EAGLEi automatic remediation begins patching known vulnerabilities, while your team has the necessary information to focus their time and energy on the most severe vulnerabilities.



How can EAGLEi help our organization from a compliance and regulatory perspective if we are audited?

EAGLEi helps with compliance and regulatory audits by showing the proactive steps you've taken, how you're managing risk, and how effective your changes are in addressing cyber threats. This is especially useful if you've had a data breach and need to demonstrate your actions.