How ThreatWatch helps a leading healthcare provider improve the effectiveness of its vulnerability management program without compromising on data security and privacy

threatwatch

About ThreatWatch

ThreatWatch is a next generation Threat Management platform that finds and prioritizes potential cyber threats and security weaknesses affecting any attack surface, early and without using scanner appliances or bulky agents.

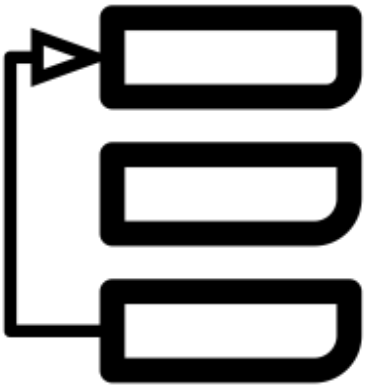
This case study with one of our healthcare sector customer delves into some of the more universal and unique challenges faced by organizations in charge of protecting patient privacy and preventing data breaches.

Challenges

Increased risk from third party agents for asset discovery

Privacy and data security are of utmost importance to any healthcare provider as was in this case. So, while running an effective vulnerability management program, patient data privacy was always going to be a risk due to the need to deploy third party agents for asset discovery. This was especially important for certain classes of asset being used exclusively for certain projects using sensitive patient information.

Vulnerability backlog



Privacy and data security are of utmost importance to any healthcare provider as was in this case. So, while running an effective vulnerability management program, patient data privacy was always going to be a risk due to the need to deploy third party agents for asset discovery. This was especially important for certain classes of asset being used exclusively for certain projects using sensitive patient information.

Cloud asset sprawl and scanning costs

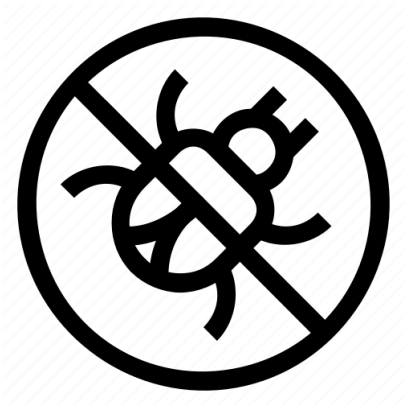
Keeping track of assets on the cloud for vulnerability management was a major challenge because of the elastic nature of cloud where instances come and go. Without effective aging of decommissioned assets, this was creating a sprawl that adds to the complexity and costs of the vulnerability management program.

Approach

No-agent, cloud native asset discovery

ThreatWatch does not believe in re-inventing the wheel when it comes to asset discovery. All major cloud providers allow deep asset discovery using native APIs. This approach eliminates the need for having agents. Instead a simple, open source CLI maintained by ThreatWatch was recommended. This CLI was designed to be easy to use and automate from within the provider network thus also eliminating the need for sharing cloud credentials with a third party service.

Malware context and vulnerability prioritization



Using machine curated threat and vulnerability intelligence provided by ThreatWatch, vulnerabilities identified on assets can be prioritized based on several important factors besides just CVSS scores. By identifying exploitabile, exploited or malware weaponized vulnerabilities the backlog can be significantly reduced and teams can focus on real issues that can cause breaches rather than keeping up with the long tail of vulnerabilities.

Policy based asset aging

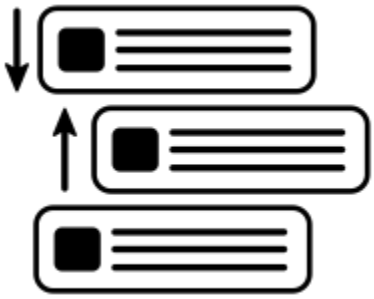
ThreatWatch policies allow decommissioned assets to be aged out and purged automatically. This will reduce the asset sprawl and reduce the clutter in reporting introduced by older assets. This, coupled with ThreatWatch's simple pricing model helps reduce the costs .of the vulnerability management program

Results

Reduced risk from third party agents on critical assets

Using a cloud native no-agent approach, the vulnerability management program was able to track hundreds of assets on cloud without deploying third party asset discovery agents. This also reduced the risk from having to share cloud credentials to a third party service. Risk from compromised agents or shared credentials was eliminated.

Reduced vulnerability backlog with accurate prioritization



Accurate prioritization of vulnerabilities resulted in a **90% reduction in backlog.**
Reduction in backlog meant the high priority vulnerabilities were being patched faster resulting in better cyber hygiene and reduced riisk of attacks.

Reduced VM overheads and costs

Decommissioned assets are now automatically getting purged from the VM program using policies run on set schedule. This resulted in lowering the costs and complexities of the VM program.

Conclusion

Reduced risk, lower overheads, better TCO

ThreatWatch, with its unique approach to proactive security is designed to provide:

- Real time threat and vulnerability intelligence
- No-agent, low overhead threat and vulnerability assessments
- Simple, secure asset discovery and management
- Accurate, machine driven prioritization of threats

These features helped bring a huge improvement in the effectiveness vulnerability assessment program at the healthcare provider while reducing the overheads and costs of running the program.