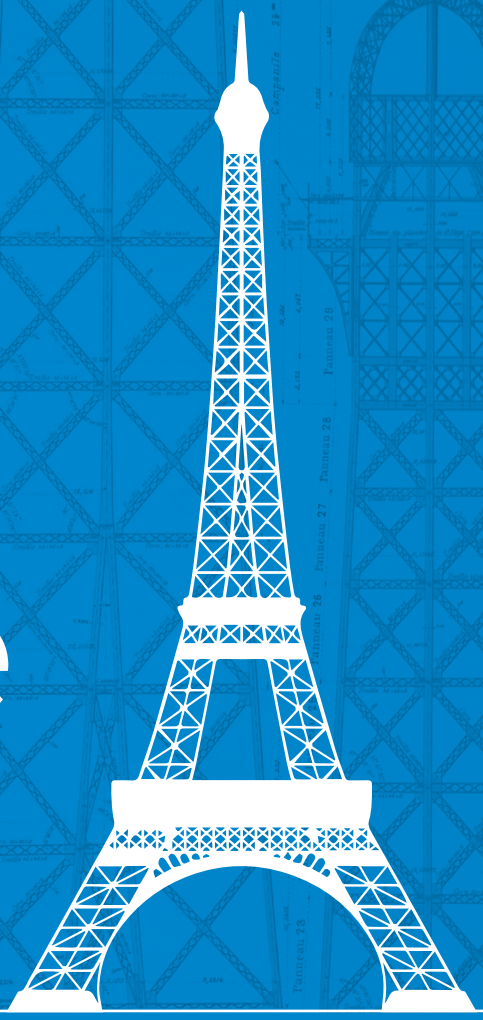
6 Keys to Ensuring Remote Employee Security



There are some amazingly high profile architectural landmarks such as The London Eye, the original Ferris Wheel, the San Francisco Palace of Fine Arts, and even the iconic Eiffel Tower, that were meant to be temporary in nature. Often built for World's Fairs, or similar high profile exhibitions, these buildings were often designed and built in a hurried schedule to meet the arrival of millions of visitors. These structures often pushed the limits of engineering, but given their temporary charter, were built with materials that weren't meant to stand the test of time.

As COVID-19 hit, IT and infosec teams across the globe scrambled to enable remote work for large numbers of employees as quickly as possible. VPNs were dusted off and pushed to their limits. New cloud productivity and collaboration applications were fired up in record time. Endpoint devices were taken home, beyond the safe confines of the corporate perimeter. BYOD was simply allowed where it might not have been before.

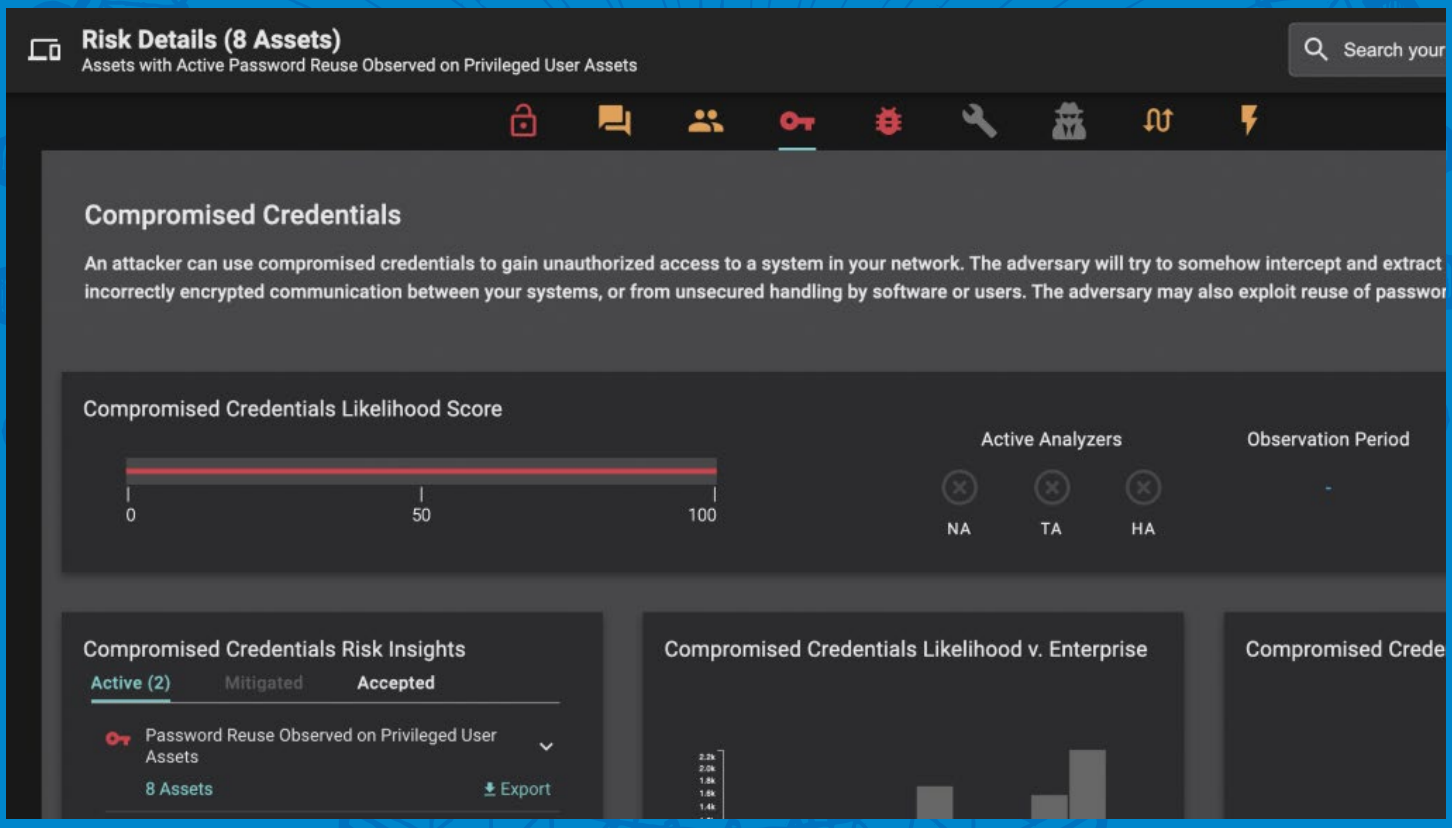
You can't help but applaud the heroic efforts of the teams putting this temporary infrastructure in place. Now however, remote work has become popular enough to become permanent for many. Here are 6 best practices to help ensuring the security of a remote workforce.

Balbix®

1. Avoid password reuse

According to Balbix's 2020 State of Enterprise Password Use Report, 99% of users reuse passwords between work and personal accounts. The implication? When that consumer cloud service gets breached, the bad guys are also getting their hands on that user's work password(s) as well. It's no wonder that 80% of breaches are the result of compromised, weak, or reused passwords.

Balbix can identify reuse of passwords, ensuring that you're focusing on those users at highest risk for compromise via password reuse.

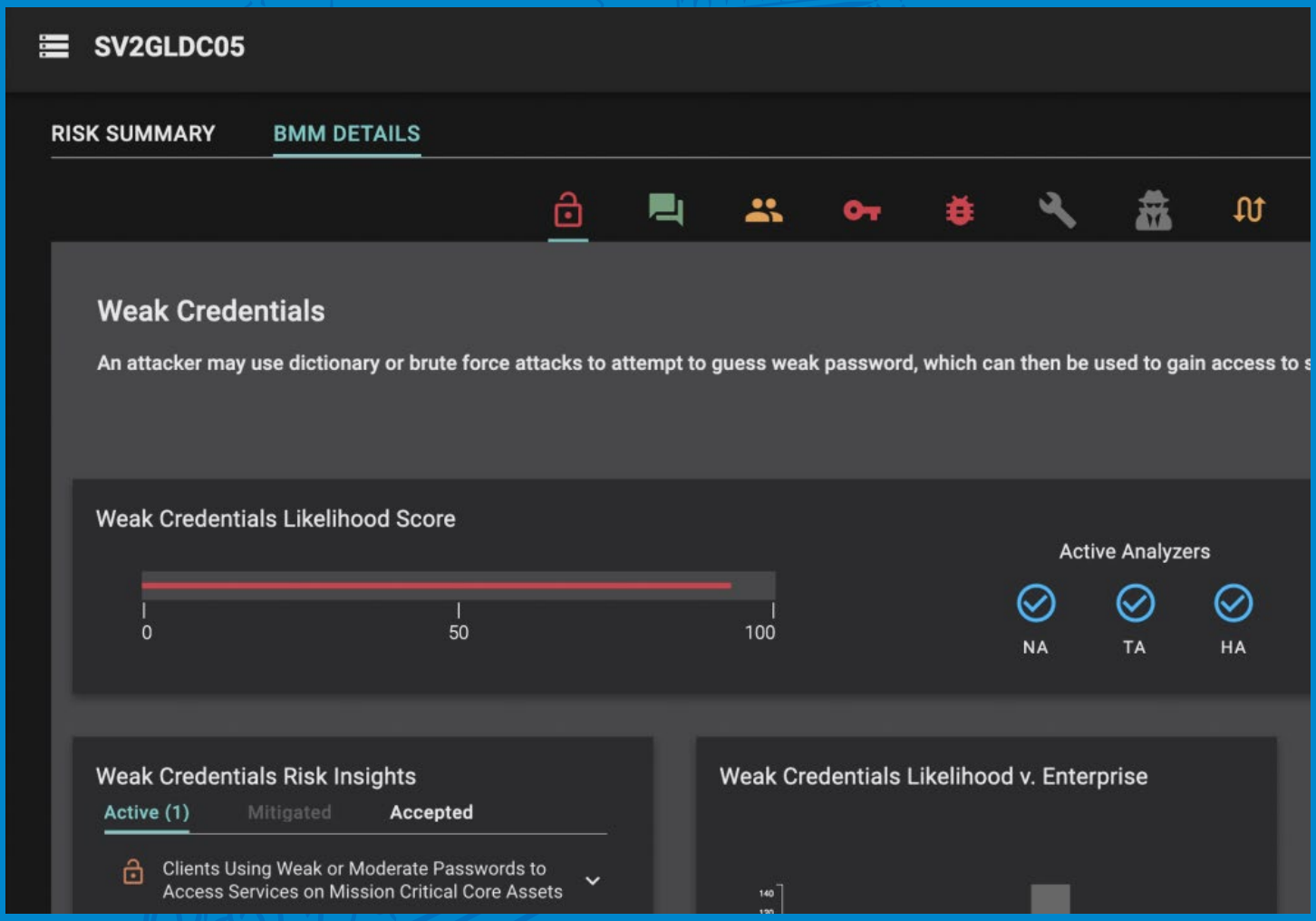


Identifying Risk of Compromise from Password Reuse

2. Strengthen identity

Closely related to password reuse, weak credentials also represent significant risk to the enterprise. In this case, it's best to build and enforce a corporate identity policy that requires the use of multifactor authentication, a password manager, and NIST recommendations on password complexity.

Identifying weak credentials is fast and simple with Balbix's natural language search capabilities:

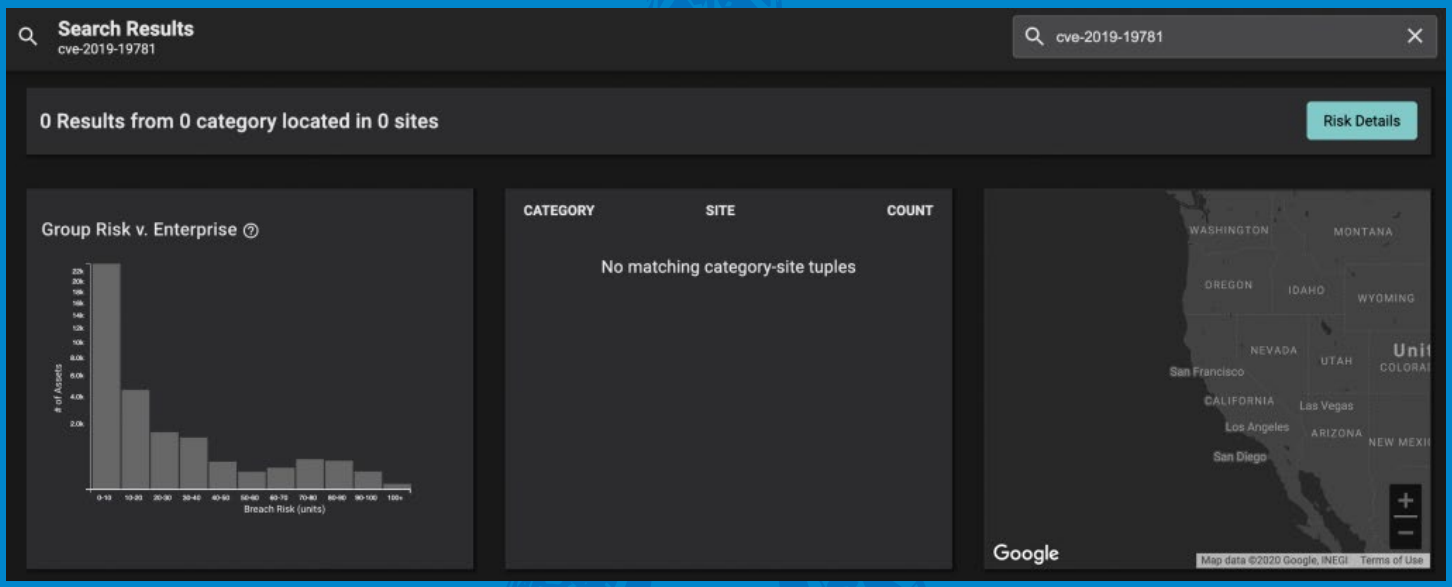


How to identify weak credentials with Balbix's natural language search capabilities

3. Require an always-on, updated VPN

With the speed at which quarantine measures were put in place, many teams focused on VPN capacity. Unfortunately, there were a number of severe vulnerabilities targeting highly deployed VPNs from Citrix and Pulse Secure that predictably became very popular with attackers around that same time.

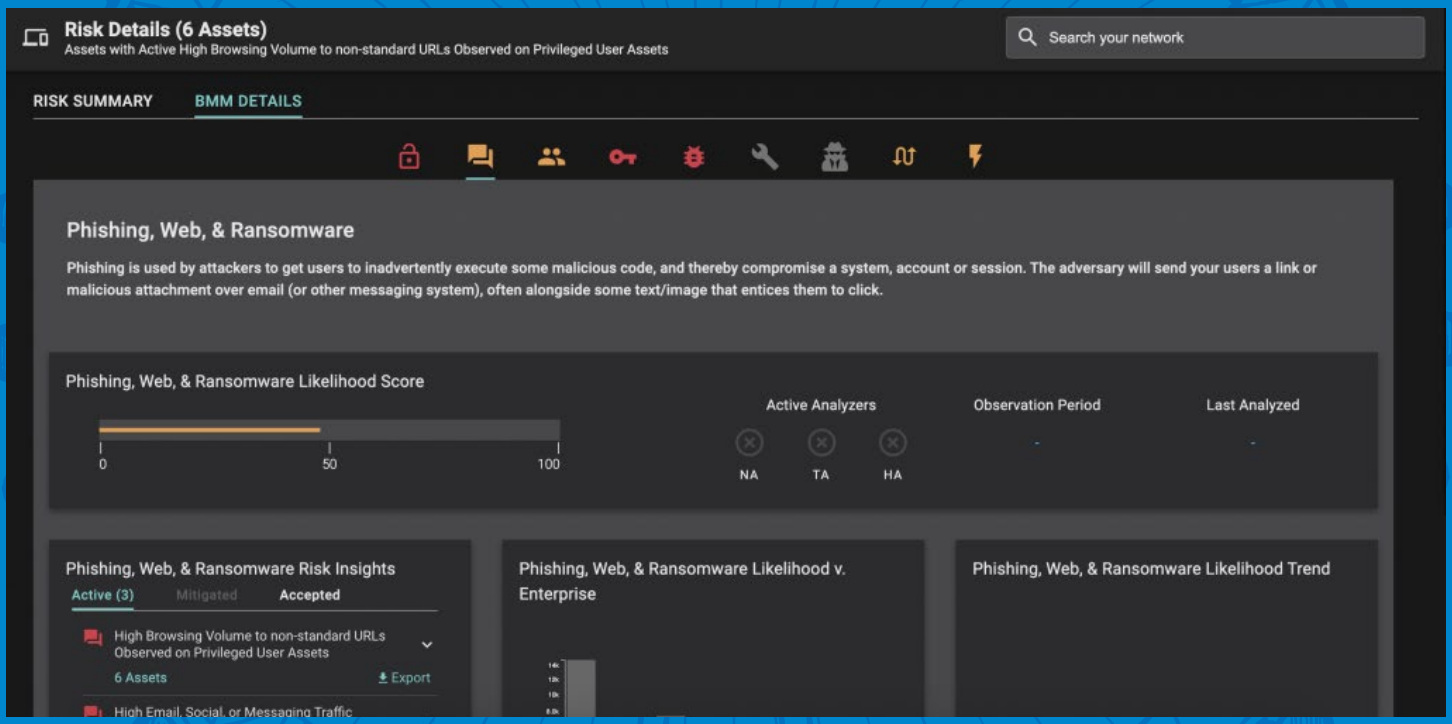
Search across your entire attack surface for these types of vulnerabilities at any time using the Balbix platform. Looks like this organization is keeping up!



4. Beware risky activities

With the shift to home work, the lines between personal lives and work lives are blurring like never before. Unfortunately, this might also mean riskier web browsing and other behaviors on corporate assets, let alone the risk of others in the household making use of corporate machines. For privileged users, the stakes are even higher.

Keep tabs on those users (privileged or otherwise) that are driving unnecessary risk into the organization via risky behaviors.

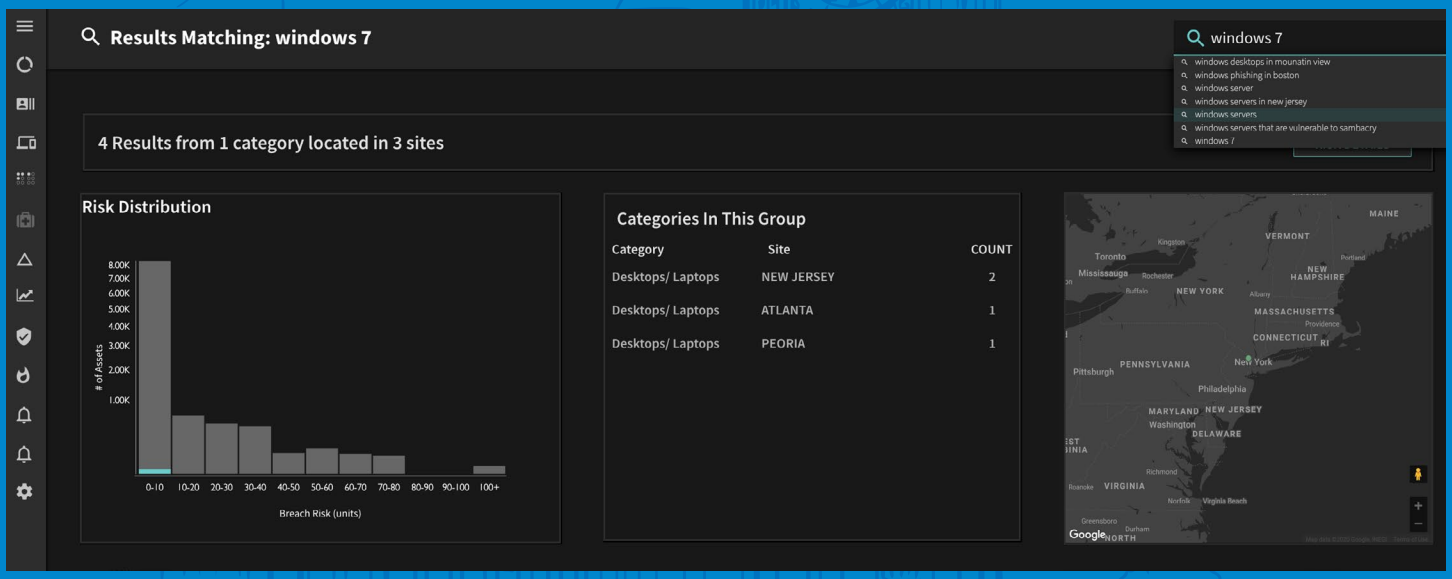


Keep tabs on those users (privileged or otherwise) that are driving unnecessary risk via risky behaviors

5. Minimize remote attack surface by removing unused software

The typical organization wastes 37% of their IT budget on unused software. Identifying this wasteful spend not only helps with cost consolidation and efficiency, but it shrinks the enterprise attack surface significantly.

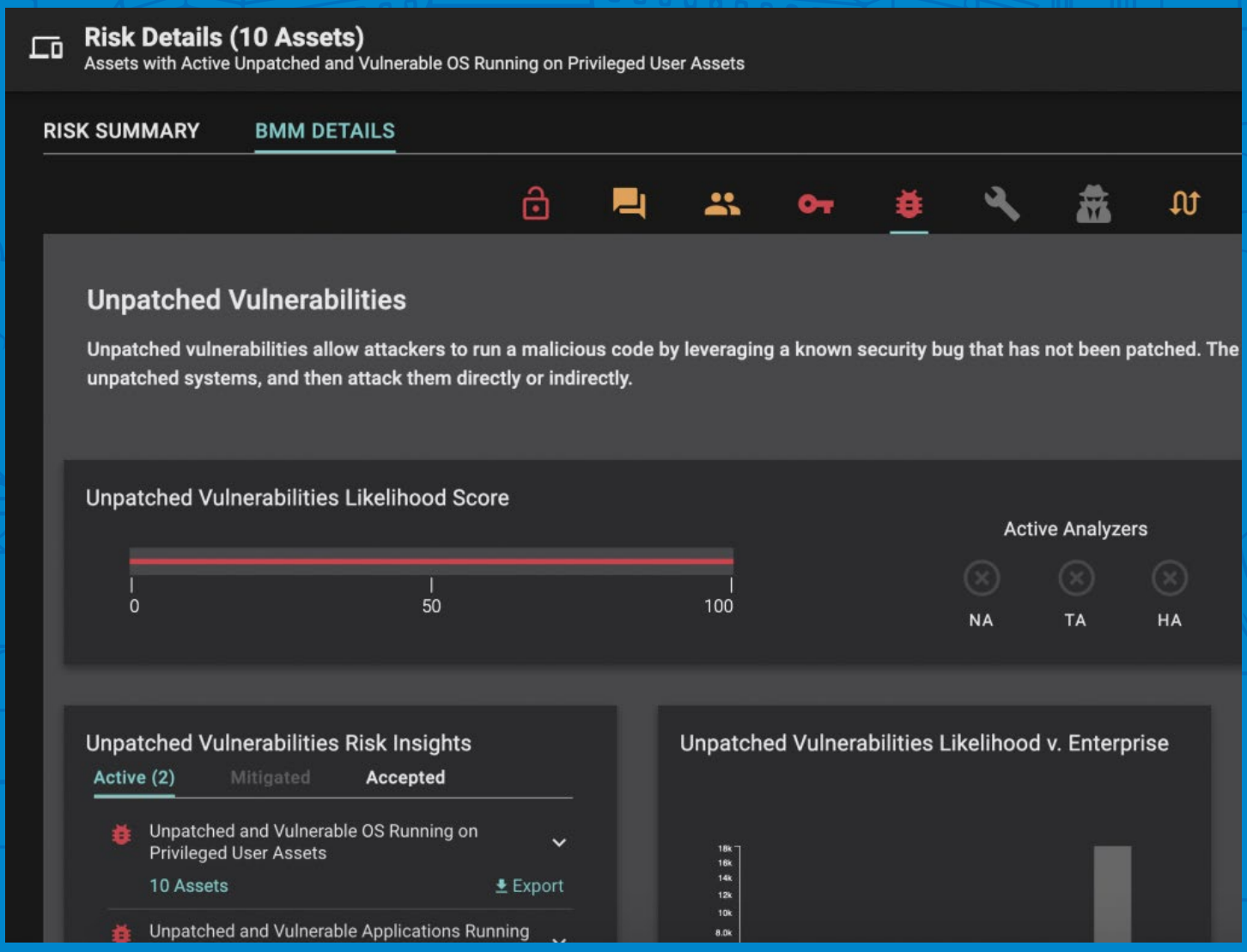
Unused software—find it, eliminate it, forget about it.



6. Keep remote systems patched

Just because a remote machine is more difficult to patch, doesn't mean this is a task to be avoided. Key here is leveraging a risk-based prioritization mechanism rather than simple CVSS severity.

Finding unpatched systems and prioritizing patching efforts can be done in seconds with Balbix:



How to find unpatched systems and prioritizing patching efforts

Request a demo today to learn more about these and other capabilities in the Balbix platform.

LEARN MORE

Balbix®