NETWORK VULNERABILITY MONITORING

An inspection of the potential points of exploit in a network to identify lapses in security in order to patch them before criminals attack them

TriCorps

WHAT IS NETWORK VULNERABILITY MONITORING?

Network Vulnerability Monitoring is an automated, subscription service that routinely checks your network perimeter to find any vulnerabilities, configuration issues, or patches that have failed to apply, which could leave your company vulnerable to attack or breach.

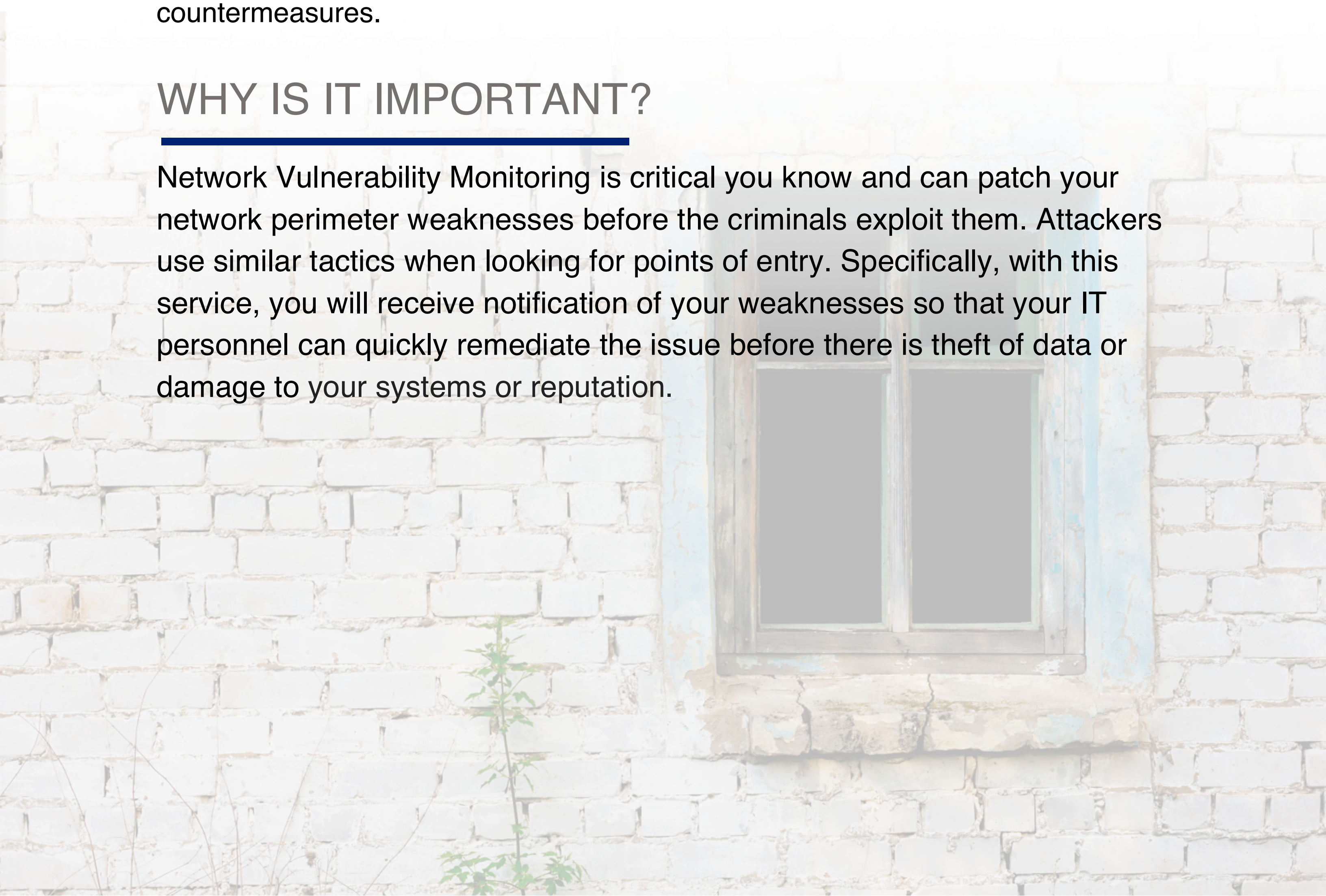
Essentially, it functions like a guard doing a perimeter check of a bank, office building or warehouse, inspecting every door and window to make sure none of them are open, old, or damaged and requiring repair (patching).

Network Vulnerability Monitoring compliments services provided by intrusion detection (e.g. alarm systems) by continuing to monitor weaknesses in the perimeter.

This routine, automated scan is external, meaning there is no trusted access to the network and sees the network the way a threat actor or criminal would. This monitoring detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

WHY IS IT IMPORTANT?

Network Vulnerability Monitoring is critical you know and can patch your network perimeter weaknesses before the criminals exploit them. Attackers use similar tactics when looking for points of entry. Specifically, with this service, you will receive notification of your weaknesses so that your IT personnel can quickly remediate the issue before there is theft of data or damage to your systems or reputation.



HOW DOES IT WORK?

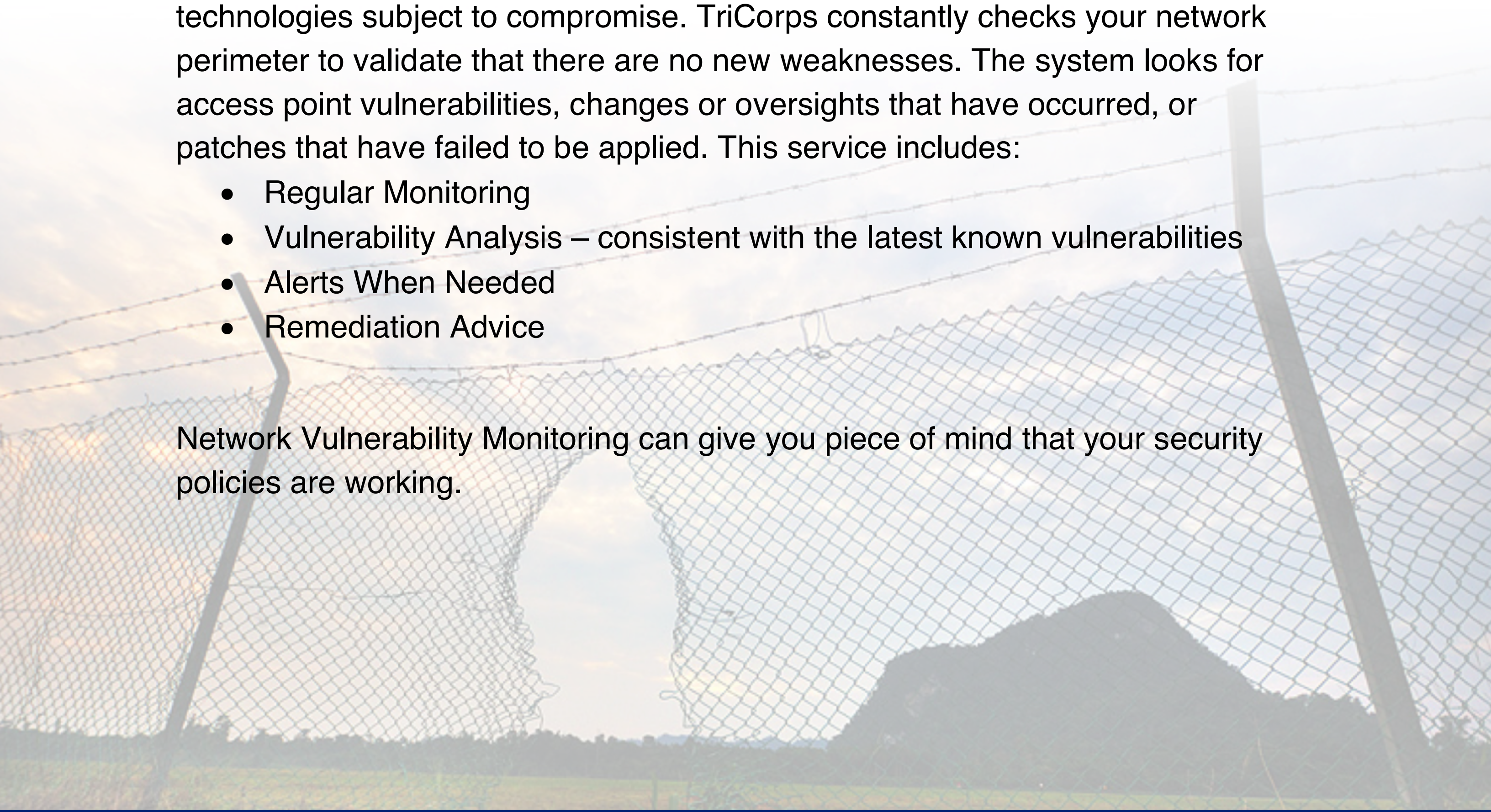
TriCorps has a 24/7 security surveillance center that is staffed with multiple security personnel. We use cutting edge software to continuously monitor your network for issues. If anything abnormal is detected, our team notifies you and offers solutions for remediation. Nothing is required from your team during the monitoring, but, if there's an issue that we feel should be addressed, we will contact you and recommend solutions.

WHAT YOU RECEIVE:

In short: external confirmation that your preventative security measures are working. For most companies, their networks are always evolving with new devices and software being introduced, new data flowing in and out, and aging technologies subject to compromise. TriCorps constantly checks your network perimeter to validate that there are no new weaknesses. The system looks for access point vulnerabilities, changes or oversights that have occurred, or patches that have failed to be applied. This service includes:

- Regular Monitoring
- Vulnerability Analysis – consistent with the latest known vulnerabilities
- Alerts When Needed
- Remediation Advice

Network Vulnerability Monitoring can give you piece of mind that your security policies are working.



For more information, contact us at 405.621.9006
or email us at info@TriCorps.com

TRICORPS

tricorps.com ☎ 405.621.9006 ✉ info@tricorps.com