What to Expect When You First Enable the Arctic Wolf Managed Risk™ Service

PRODUCT DOCUMENTATION

Overview

Executing continuous vulnerability scans is a cornerstone of your organization's cybersecurity program. However, the myriad types of single-scan approaches that only offer a point-in-time view of your network can make understanding your risk profile a daunting task.

Unlike single-scan alternatives that rely on automated methods that make assessing vulnerabilities difficult, the Arctic Wolf Managed Risk™ service enables you to continuously scan your networks and endpoints, and quantify risk-based vulnerabilities. Leveraging Arctic Wolf's Concierge Security Team™, Arctic Wolf Managed Risk provides real-time understanding of your cyber risks so you can take prioritized action to improve your cyber risk posture. It complements Arctic Wolf Managed Detection and Response™, which provides the most comprehensive security operations center (SOC)-as-a-service in the industry.

The Managed Risk scanner provides a continuous view of your vulnerabilities. Constantly updated with the latest threat information, it automatically detects when devices enter and leave your network. It provides comprehensive visibility into the risk your organization faces.

The vast majority of hosts on a network experience no impact when a vulnerability assessment is conducted. Some older systems—such as consumer-grade printers or network IoT devices—may have denial of service vulnerabilities that are revealed when scanned. This document describes some of those instances, and how they can be effectively managed when the Managed Risk scanner is deployed.

The Managed Risk scanner uses similar methods that bad actors use to identify vulnerabilities and map your attack space. For that reason, issues that occur during a scan are equally exploitable by a bad actor to cause a denial of service condition on your network. If you have a device that experiences problems during a scan, we recommend consulting the vendor for an appropriate patch or workaround. Other strategies that can be deployed for such systems are outlined below.

What should I do if I see an issue?

There are three possible mitigation strategies we recommend. Each issue is slightly different, so consider the following options carefully when deciding which technique to employ:

Whitelisting the scanner IP

Various devices have intrusion detection system (IDS) features, typically around port scan detection and failed login monitoring. The Managed Risk scanner regularly conducts port scans to identify open services and tries known or default usernames/passwords on them. In these situations, the preferred solution is to whitelist the Managed Risk scanner IP within the IDS feature/product to eliminate false alerts.

Scheduled scanning of the host IP

The Managed Risk scanner can be configured to schedule scans within a specific timeframe. We recommend scheduling scans outside of typical business hours to minimize disruptions if the impact of scanning certain hosts creates an inconvenience.

Blacklisting the host IP on the Managed Risk scanner

This is often referred to as the "hammer" approach. Adding an IP to the Managed Risk scanner blacklist will prevent scanning that host entirely. From the Managed Risk dashboard/scanner perspective, the host no longer exists in your network. This option is available as a last resort, when the impact of scanning outweighs the benefits of visibility into the risks present on the host.

What to Expect When You First Enable the Arctic Wolf Managed Risk™ Service

What types of issues are typically observed?

Each situation is unique, but here are some general observations and recommendations for the different circumstances you may encounter:

Temporary account lockouts

Some applications temporarily disable a user account after observing a number of failed login attempts. This can be an inconvenience if a user needs to connect to the application while the temporary lockout is active. In these situations, whitelisting the scanner IP is the preferred solution. The next best option is to schedule a scan of the affected host at a time when the temporary lockout is more convenient.

Antivirus endpoint software

Some antivirus endpoint software alerts the user when it detects a port scan. Since scans occur regularly, we recommend whitelisting the Managed Risk scanner IP address in the endpoint software to prevent repeated nuisance alerts to end users.

Printers

Some network-attached printers accept unvalidated input on specific ports as print data, and consequently print garbage pages, wasting toner and paper. The Managed Risk scanner attempts to detect printers and prevent this from occurring. If you still observe this issue, however, we recommend backlisting the printer.

Note: Some specialty industrial printers have particularly expensive materials that could be inadvertently damaged under such circumstances. We recommend blacklisting those printers and—as a security best practice—limiting access to them through network segregation techniques.

Consumer-grade devices

Many different consumer-grade network devices such as Wi-Fi access points, UPnP devices, IoT devices, etc., are prone to issues when scanned. This is typically due to poor error handling in the network stack when unexpected data is received on a listening port. If you observe minor issues on one of these devices, we recommend scheduling the scan at a time when the impact of the nuisance is minimized. If the impact is more severe, we recommend blacklisting the device IP address.

Networking equipment

Although very rare, issues have occurred on some networks when a switch/router is scanned. When this happens, it is almost always due to old, end-of-life hardware, or low-end versions of higher-end products. Each of these situations is unique. If you think you see an issue with a piece of networking equipment, please contact us. If the impact is more than a nuisance, you can blacklist the equipment control port IP, or temporarily pause scanning while we help investigate.

Firewalls

Some firewalls have built-in intrusion detection system (IDS) features. We recommend whitelisting the Managed Risk scanner IP address in those features to ensure that the network is fully scanned and that no CPU resources on the firewall are unnecessarily wasted. We are happy to help you investigate any suspected firewall issue.

VPNs

The Managed Risk scanner typically consumes very little bandwidth during a scan. As such, scanning across VPN networks can be effective, as long as the VPN has high-enough capacity for the combination of regular traffic and scanner traffic. VPNs that are rate-limited for VoIP or other low-bandwidth applications should not be scanned as the capacity will likely be exceeded. If you have questions or concerns about how to best deploy the Managed Risk scanner in your network, please contact us.

Special industry-specific concerns

Some industry segments use atypical devices within their networks. In such cases, take extra consideration around cybersecurity in general, as well as network vulnerability scanning specifically. We are happy to discuss network design best practices around device isolation and network segregation for these types of uncommon/special devices.

What to Expect When You First Enable the Arctic Wolf Managed Risk™ Service

Healthcare industry

The continuous advancement of healthcare technology has led to more and more healthcare-specific devices being "network attached" in some form. Doing so has many advantages but can also result in additional risks. For example, a dialysis device vendor may create a network-attached device so that it can be remotely monitored. If the vendor did not invest sufficiently in security and hardening or has never run a vulnerability scan against the device as part of development, unexpected behavior similar to an IoT device or consumer Wi-Fi router may occur during a scan. Unlike a consumer device where the impact is merely a nuisance, a dialysis machine experiencing unexpected behavior may result in serious health consequences for the patient. As such, we highly recommend that devices critical to the health care of a patient are isolated from the network using network security device isolation and network segregation techniques. We also recommend consulting with the vendor about their security practices before initiating a vulnerability scan on that host.

Networked manufacturing devices

As in the healthcare industry, many manufacturing systems are network-connected devices with similar risks. For any system where unexpected behavior could result in possible harm to an operator, we highly recommend first isolating these devices from the network using network security device isolation and network segregation techniques, as well as consulting the vendor about their security practices before initiating a vulnerability scan on that host.

Utilities and SCADA devices

Modern utilities make heavy use of SCADA devices within their networks. These systems are usually isolated into a separate network and the vendors typically invest in security and hardening. However, since unexpected behavior in these devices may seriously impact operations, similar precautions to those used with healthcare devices need to be taken before actively scanning SCADA hosts.

What systems are likely to alert when scanning is enabled?

Intrusion detection systems

Intrusion detection systems (IDS) are designed to detect and alert on the same scanning behavior that the Managed Risk scanner executes continuously. A properly deployed IDS will detect and alert once scanning commences. We recommend whitelisting the Managed Risk scanner IP address in the IDS to prevent false alerts from being a nuisance to your IT staff.

Can I scan through a VPN/firewall?

We recommend deploying multiple Managed Risk scanners at multiple sites instead of scanning through a VPN and firewall.

Note: Generally, if you can ping externally across the VPN, deployment of Managed Risk scanners in this scenario is supported. The bandwidth impacts of scanning across your VPN environment are estimated to be approximately 100Kbps.

Switches that don't like being scanned

Blacklist these switches on the Managed Risk scanner and consider removing them from your network:

- Avaya/Nortel Ethernet Routing Switch 5520-48T-PWR
- HP ProCurve 2530 switches (YA.16.01.0006)

VM requirements

We recommend deploying the Managed Risk scanner VM with 8GB RAM, 20GB HD space, and 4 vCPUs. To scan as many hosts as quickly as possible, the Managed Risk scanner makes heavy use of the CPU. The number of hosts you scan may impact this.

Where do I go for questions/support?

Always feel free to contact the Arctic Wolf Concierge Security Team™ at ask@arcticwolf.com for any assistance, questions, comments, or concerns you have.