5 Critical Steps for Ransomware Prevention and Mitigation

1. Discover & monitor every asset

Asset discovery featuring automated network scans is an important service. With ongoing scans, you can quickly find and monitor new devices as they join the network and then understand each device's health.

2. Software patching

A remote monitoring and management (RMM) tool helps with continuous patching, enabling you to automatically deploy updates to endpoints and ensuring your patching never falls behind. You should also be sure that your anti- virus and anti-malware solutions are set to automatically update and run regular scans.

3. Regular data backups

Integrated backup and disaster recovery (BDR) solutions provide more streamlined service management with far less chaos. It's also crucial to secure your backups. Make sure they are not connected to the computers and networks they are backing up or else they could become infected in the event of a ransomware attack.

4. Deploy an endpoint protection tool

Endpoint detection and response (EDR) solutions help protect endpoints such as servers, laptops, desktops, mobile devices, and more to quickly identify malicious activity, as well as automatically taking remediation actions such as restoring unsafe files to an acceptable previous state.

5. Enhancing your cybersecurity toolset

When it comes to cybersecurity, there is no such thing as too secure. Here are a few examples of tools and services you should consider adding to your cybersecurity tech stack:

- ✓ Risk assessment software
- ✓ Email monitoring
- ✓ Security information & event management (SIEM)
- ✓ Threat intelligence feeds