advanced network systems

Fully-managed, next-generation endpoint security

In today's workplace, the devices your employees use have become the biggest attack vector.

Protect them against the most dangerous security threats with next-generation protection along with expert remediation and incident response. Our Endpoint Security Program provides the foundational security services you need including monitoring network endpoints, detecting and stopping malicious threats and correcting vulnerabilities to proactively protect against future attacks. This effective and affordable solution is designed to stop active threats and minimize the crippling effects of a cyberattack on your organization. It includes the right combination of both proactive and remediation services.

Next-gen threat protection, detection and remediation.

Cyber criminals target small and mid-sized organizations the same way they do large corporations and federal agencies; leveraging many of the same tactics. We provide a program designed for smaller organizations that scales protection to meet the needs of your operations. This includes implementing best practices, along with the right solutions and staff needed to deal with real threats. Plus, you can add our advanced patented threat ID technology that detects both known and unknown threats. It leverages the latest behavior-based technology to fully protect user devices for Windows, Mac and Linux, regardless of where they are (office, home, airport, café, hotel, etc.).

Take the cost and complexity out of cybersecurity.

Leverage our advanced security solutions without the need for in-house expertise. Our easy-to-deploy endpoint protection program provides the tools and expertise you need, while eliminating the cost and technical challenges associated with managing your own cybersecurity.

Managed Endpoints Protection Program

Get the essential security services needed to protect your employee devices from cyber threats:

- Device patching
- Anti-virus
- DNS protection
- Dark web monitoring
- Advanced device security profiling
- Employee security awareness training
- Help Desk

BASIC PROGRAM FEATURES

Device Patching: A large number of cyberattacks take advantage of known software vulnerabilities. Operating system and application patches are critical part of basic preventative maintenance necessary to keep machines up-to-date, stable, and safe from malware and other threats.

Anti-virus Protection: is a foundational element of endpoint security. Anti-virus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware. New and updated malware is released daily, so it is important that you always have the latest updates protecting your devices.

Domain Name System (DNS) Protection: provides an additional layer of protection between an employee and the internet by blacklisting dangerous sites and filtering out unwanted content. By using secure DNS protection both at home and at work, employees can avoid unnecessary risks and the potential for malicious attack.

Security Awareness Training: Some of the greatest threats to information security come from your employees. Security awareness training teaches users what cyber threats are, their potential impact and the steps required to prevent cyber-crime from infiltrating their workspace.

Dark Web Scanning: helps organizations detect cyber threats that expose stolen email addresses, account passwords and other sensitive information circulating on the dark web. Gaining this knowledge enables you to take precautions immediately to protect your data.

Network and Security Operations Center Support: expert teams act as the central point of collaboration in a coordinated effort to continuously monitor and improve your security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

	Managed Endpoints: **Threat Protection, Detection and Response**
Basic Program Features	Essential security protections including device patching, anti-virus, DNS protection, advanced device security profiling/risk scoring, and dark web monitoring. An employee security awareness training program is also included. Covered devices are fully supported by our Network Operations and Security Operations Centers; including monitoring, alerting and remediation services.
Advanced Program Features	**Advanced Endpoint Security** that provides non-signature based, AI protection from viruses and zero-day threats and includes OS rollback capabilities.
	AND/OR
	Level 1 and 2 Help Desk support for your employees available during business hours, or with 24x7 coverage. Our U.S.-based Help Desk provides easy access to professional support for hardware and software issues through chat, email and phone.

advanced network systems

Improve Your Endpoint Security With Managed Threat Detection and Response

Can your organization afford to bear the crippling effects of a cyberattack?
Don't wait to get the critical protection you need.
Act now to get the right level of cyber expertise and technology to
have confidence in your security stance.

Get started with a cost-effective program by contacting Advanced Network Systems at **800.639.6757** for a no-risk, no-obligation consultation.

355 Rio Road West, Suite 201
Charlottesville, Virginia 22901

☎ 434.973.4747

✉ contactus@getadvanced.net

🌐 getadvanced.net