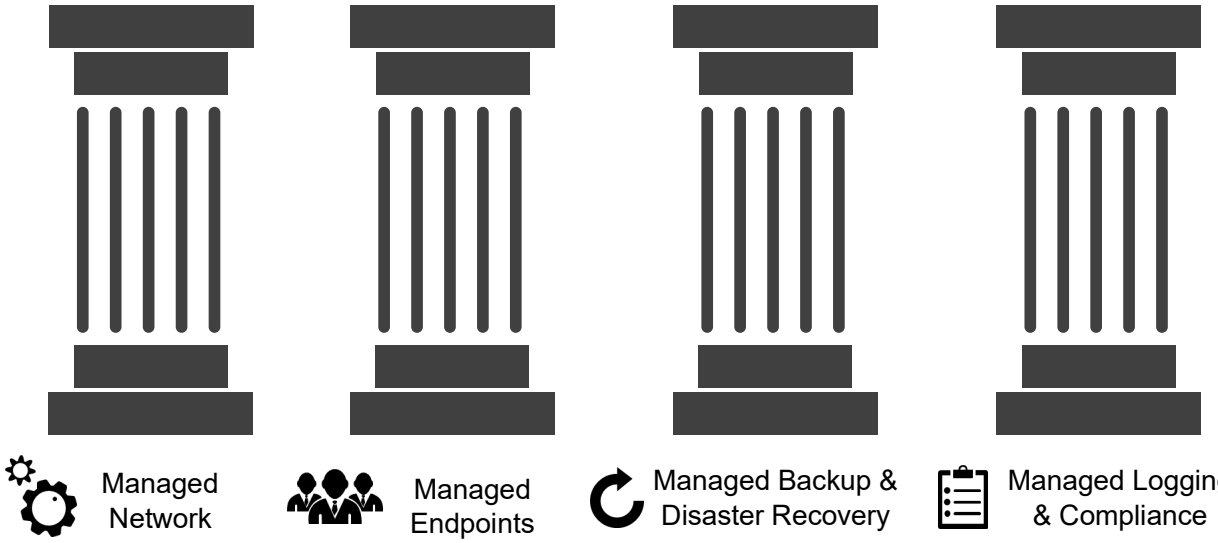
A Four-Pillar Program Approach to Cybersecurity



advanced network systems

"HAVING BETTER CYBERSECURITY DOESN'T HAVE TO BE COMPLICATED.

DEVELOPING A MORE COMPREHENSIVE STRATEGY BECOMES MUCH SIMPLER WHEN YOU FOCUS ON FOUR PILLARS."

Every organization can have the essential services needed to reduce the risk of security threats and support their compliance requirements.

Our 4-pillar program provides a full-spectrum of cybersecurity services and takes the guesswork out of covering the right security measures at each key level of the network.

Each pillar of protection includes the right combination of proactive and remediation services to reduce risk and minimize the crippling effects of a cyber-attack on your operations.

PILLAR 1: Managed Network. Improperly managed core network devices create easy access for targeted attackers. *Nearly 57% of data breaches are attributed to poor patch management. Source: Ponemon*. This foundational program features fully-managed security patching and critical updating of core network infrastructure including servers and firewalls, performed by our Network Operations Center.

PILLAR 2: Managed Endpoints. Employee devices have quickly become one of the biggest vectors for cyber-attacks. *A recent Ponemon Institute study revealed 68% IT security professionals experienced one or more endpoint attacks that compromised their company's data assets or IT infrastructure. Of the successful incidents, 80% were new or unknown, zero-day attacks.* This program offers the right combination of advanced endpoint security protections. This includes AI-based protection from viruses and zero-day threats, dark web monitoring for email addresses and DNS protection. Covered devices are fully supported by our Network Operations and Security Operations Centers; including monitoring, alerting and remediation services.

PILLAR 3: Managed Backup & Disaster Recovery. A sound backup and DR solution are essential elements of an incident response plan for data breaches and cyberattacks. *A 2020 Coveware study reported that the average total downtime for businesses resulting from a ransomware attack was 16.2 days. Aside from suffering the costs of downtime, companies are having to fork over larger ransoms than ever before.* Stop baby-sitting your backups; this program provides fully-managed local or cloud-based backup and disaster recovery services performed by our Network Operations Center. Includes backup validation and advanced ransomware protection.

PILLAR 4: Managed Security Logging & Compliance. Meeting cybersecurity measures mandated by compliance regulations requires analysis of your security logs and a response plan in place. *According to analysts at Gartner Research, having a professionally monitored SIEM solution in place significantly enhances an organization's security posture, by addressing critical security and compliance issues.* This program provides 24x7 monitoring, event alerting, along with the collection and analysis of data activity across all managed devices. A team of security experts along with the latest SIEM technology and threat intelligence, proactively detect, analyze and alert on cybersecurity incidents.

Minimizing security risks is about a lot more than just anti-virus and firewalls. Ask us how we can put a comprehensive, multi-layer strategy in place today, to improve your security posture.

800.639.6757 www.getadvanced.net

advanced network systems