Alpha Tech

"News about IT Technologies that can help your business prosper"

Millbury, MA

The Modern Security Stack

In today's war against cybercrime, anti-virus software is not enough. You need a multi-dimensional, layered approach to security to protect your company's data.

Our Approach

Here at AlphaNet, we have focused on a core set of vendors to provide our security platform. These are all significant vendors, focused on supporting companies like ours in supporting companies like yours. We evaluate our security stack every 6 months at a minimum, sometimes more often when something significant has happened in the area of cybersecurity.

To go over the modern security stack, we are grouping technologies into one of 6 areas of concern. We will explain the area of concern, then the specific technologies in that group. Note we will not be addressing specific products, but functionalities.

Tip of the Spear

This group covers the heart of our protection, the endpoint security elements. These include:

Anti-Virus/Anti-Malware/Anti-Ransomware—The traditional first line of defense.
Exploitation Mitigations—these are defenses for known vulnerabilities.
Privilege Access Management—this allows us to have an admin user present on a PC only when it's needed. Most malware piggy backs off the security level the user has when doing their job, or elevate security. With this in place, this isn't possible.

Protecting the Perimeter

This is the traditional firewall's domain. Today's technology makes an old-school firewall look like a horse and buggy. Items here include:

Unified Threat Management (UTM) Appliance—this is what has made the firewall a dinosaur. The UTM doesn't just grant or deny access, it follows the allowed resource around your network to make sure it doesn't mis-behave.
Home Office Edge Appliance—for a small or home office (less than 5 users), this appliance is an extension of your UTM, providing it's benefits without any extra management burden.

Head on a Swivel

These technologies keep our end users alert and help reduce effectiveness of phishing attacks. This includes:

Annual Cybersecurity Awareness Training—this covers some regulated compliance requirements, such as most state's privacy laws. It is also often mandated by insurance companies these days.

Weekly reminders to stay vigilant—watch a quick video, answer some questions, don't get hacked!
Simulated Phishing Attacks—to keep your users on their toes.
Dark Web Monitoring—we monitor the Dark Web for any mention of credentials including your company's domain(s). If something shows up, we notify you and your effected end user so they can change their passwords.
Employee Productivity Monitoring—keep an eye on what your employees are doing, especially the remote ones.

Lock It Up

What happens if your device falls into the wrong hands?

Hard Drive Encryption—by encrypting your hard drive, we prevent someone from getting around your password and MFA. It's also seamless to your users, as the successful login unlocks the encryption.

For additional protection:
Network Access Control (NAC) – NAC verifies PCs the way 2FA verifies your users. With NAC, we review a device trying to connect to the network by verifying that it meets our requirements for connection. This usually involves making sure that the company-approved security stack is installed and operating on the computer.
Multi-Factor Authentication (2FA or MFA)—by adding this to any login you can, you dramatically reduce the chances of someone getting on your device or in your cloud app. We recommend this for Windows Login and Microsoft 365 at a minimum.

Keep an Eye on It

The price of security is vigilance.
Items here include:

Remote Monitoring & Management (RMM)—this allows us to monitor your network, and address issues.
Secure Remote Control—an extension of the RMM, this allows us to actually connect to your PC.
Penetration Testing—we periodically recommend having a third party perform a penetration test on your network.

For a stronger defensive posture:
Managed Detection & Response—A third party Security Operations Center (SOC) is watching your network, determining if intrusions are individual and random or part of a concerted attack.

Back It Up

When things go wrong, nothing beats a good backup. We recommend 3 different standard backups:

Backup of Servers to a local appliance and the cloud
Backup of Critical Workstations
Backup of M365 to store critical files on the cloud to keep them safe and easily accessible to your entire team

Want to learn more? Contact us using the information printed below and we can get started.

Want Help Now?

Call us at 508-471-3155 or email us at info@alphanetsolutions.com

Alpha NetSolutions, Inc.
3 Silver Fox Dr, Fl 1, Millbury, MA 01527