

Security Solutions

A sound security strategy has multiple layers.

External:

- > Firewalls
- > DDoS Mitigation
- > Content Filtration
- > CDN (Content Delivery Network)

Internal:

- > Endpoint Security
- > Intrusion Prevention and Detection Services (IPDS)
- > Vulnerability Scanning
- > Penetration Testing
- > Security Systems

Cloud:

- > Software-defined Perimeter
- > Retainer Services
- > Dark Web Threat Management
- > Application and Data Security
- > Analytics
- > Threat Intelligence



At minimum, you should have the following in place:

Endpoint Security (required)

Endpoint security is the process of securing endpoints on an organization's network. All devices (mobile, laptops, desktops, servers) are considered endpoints and provide an entry point for threats. With the rise of BYOD and remote workforces, the need for endpoint security has increased significantly.

Firewalls (required)

As the first required building block for an overall network security posture, a firewall is designed to monitor incoming and outgoing network traffic and block unauthorized traffic from penetrating the network. Maintaining a firewall requires a lot of time from IT resources, and the majority of businesses with a firewall don't actively view the logs. A Managed Firewall is a realistic system for all businesses to have in place. The system gives a simplified view for easy filtering by ingress and egress traffic.

Intrusion Detection and Prevention (recommended)

These are applications layered on top of a managed firewall solution. If your IT staff does not have security expertise, it is recommended to outsource these services.

- **Intrusion Detection System (IDS):** Provides alerts when suspicious activity is detected and logs activity as an audit trail (does not take any actions to stop attack).
- **Intrusion Prevention System (IPS):** Provides an increased layer of protection that helps to automatically defend against threats and attacks identified by the IDS.

Vulnerability Scanning (required)

A vulnerability scan is an automated scan that looks at a user's entire network, pings all machines tied into it, and generates a report of all problems (like a building inspection). The report can include hundreds to even thousands of problems. It's recommended to perform a vulnerability scan on a quarterly basis. Some organizations may be required to do this because of compliance.