us signal

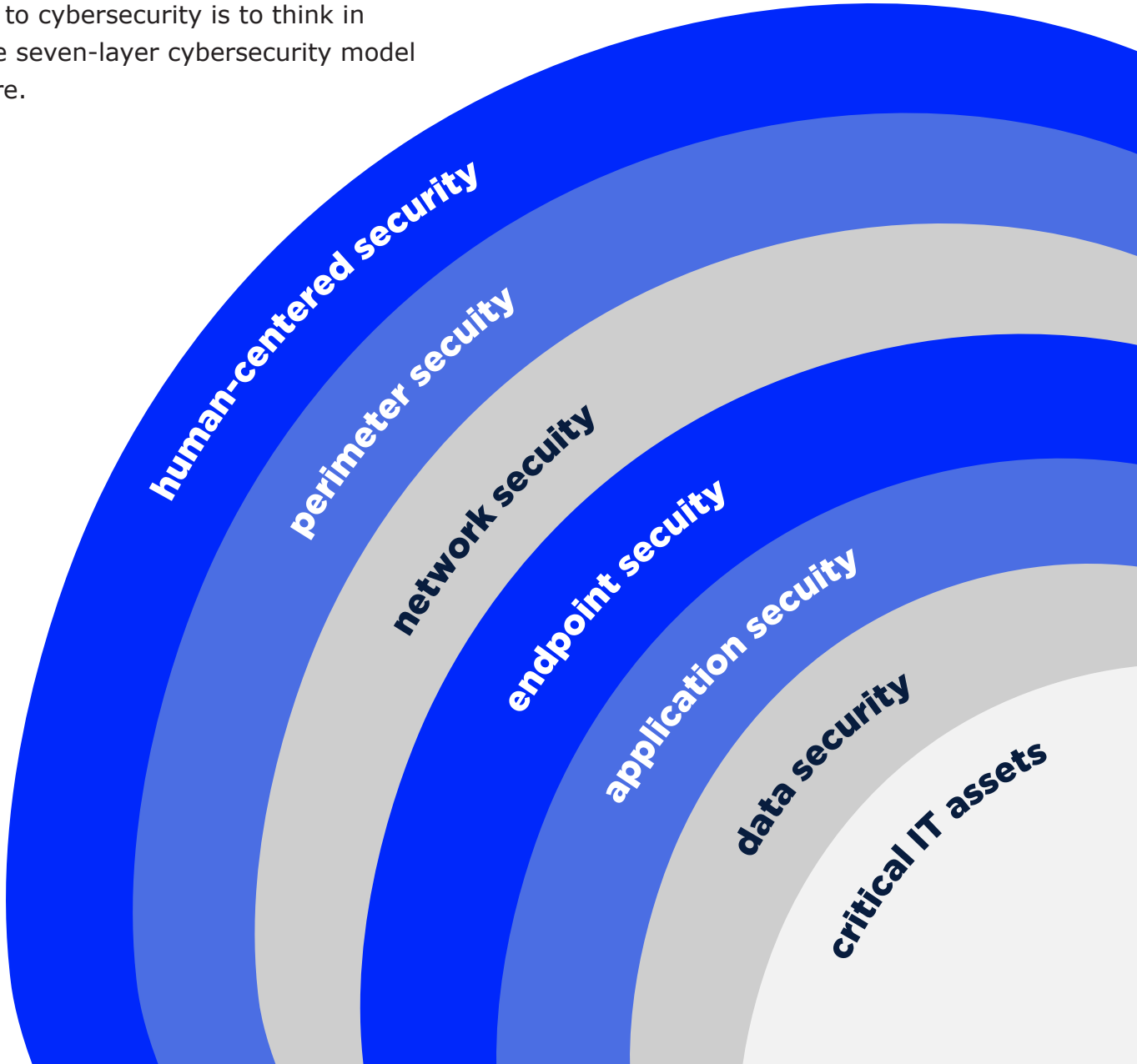
the seven-layer approach to cybersecurity

a cybersecurity strategy whitepaper

A multi-layered cybersecurity strategy is just what is sounds like: a strategy that employs multiple layers of defense mechanisms, security protocols and other measures to protect IT assets. There are various ways to approach this kind of security strategy. (The ISO Open Systems Interconnection – OSI – model is a good one.)

However, one of the easiest and most effective approaches to cybersecurity is to think in terms of the seven-layer cybersecurity model outlined here.

At the core of this model are your mission-critical IT assets, which constitute layer 1. These assets are then surrounded by a data security layer (layer 2), an application security layer (layer 3), an endpoint security layer (layer 4), a network security layer (layer 5), a perimeter security layer (layer 6) and a human-centered security layer (layer 7).

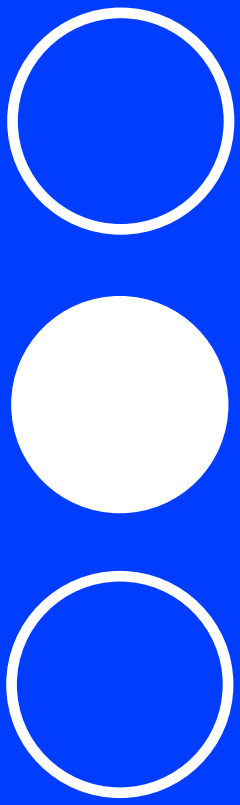


know your threats

Some of the cyberthreats are the same or similar across layers. Others are unique to specific layers. For example, malware is a common threat at the human-centric layer, as well as at the endpoint layer. Distributed denial of service (DDoS) attacks, HTTP floods and SQL injections are threats specific to the application layer.

Some of the same kinds of security solutions or protocols can be used in multiple layers. Case in point: encryption works at both the network and data security layers.

The specific solutions that make the most sense for each layer will vary based on your organization's IT system architecture, current security systems and protocols, compliance needs, and other factors. What's important is to make sure you understand the various threats that can exist at each layer and implement tactics to prevent them, detect them if they do break through, and respond to them in ways that mitigate potential damage.



know your layers

Use the following layer descriptions to create your own seven-layer approach to cybersecurity for your organization.

layer 7: human-centered

This idea here is to make sure that anyone who can access your systems is trained to identify, resist and report phishing attacks, social engineering schemes, and other incidents that could put your IT assets at risk. Mechanisms must also be put into place to ward off security issues that can arise due to human error, negligence and misuse of privileged access.

In addition to frequent, up-to-date training, security components for this layer may include strong password policies and multifactor authentication, implementation of a zero-trust policy, and the use of insider threat monitoring, detection and mitigation tools.

layer 6: perimeter security

Security solutions in this layer are meant to protect the network by controlling incoming and outgoing network traffic based on an organization's established security policies. Common security mechanisms here can include spam filers, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and VPNs to create a barrier between a secure internal network and external networks such as the internet.

layer 5: network

This layer employs solutions to protect the communication between applications and devices on a network. Among them: a robust network architecture, secure protocols like HTTPS, and network segmentation to separate sensitive parts of the network from less sensitive ones. It's also helpful here to employ anti-malware and antivirus software to monitor and analyze network traffic for malicious activity and unauthorized access.

layer 4: endpoint security

The focus in this layer is on protecting the endpoints — individual devices like smartphones, tablets and computers that connect to the network and can serve as entry points for malware and other threats. Antivirus programs and firewalls are important solutions. Other security mechanisms can include managed detection and response (MDR) solutions that monitor, detect, and block malicious activities and threats on endpoints. Even if a device is compromised, MDR solutions help mitigate the threats and prevent them from moving through the network.

layer 3: application security

Security solutions in this layer are intended to keep software and devices free of threats and to eliminate or at least reduce potential vulnerabilities. Security measures may include vulnerability scanning and applying patches and software updates (making sure to prioritize so the most important ones get implemented). Other measures include using solutions like web application firewalls (WAFs) to defend against threats such as cross-site scripting (XSS) and SQL injection.

layer 2: data security

This layer is about ensuring the privacy, integrity, and availability of data. Security measures include data encryption, employing backup solutions and establishing robust access controls to safeguard data from loss, exposure, and unauthorized access.

layer 1: mission-critical

These are the IT assets — data, IT infrastructure, etc. — that are crucial to your organization's operations and business continuity. Protection strategies here involve implementing layered defenses like firewalls, intrusion detection and prevention systems, and robust access controls. For instance, regularly updating and patching mission-critical applications ensures that vulnerabilities are addressed, minimizing the risk of exploitation and ensuring the uninterrupted functionality of essential

strategize with US Signal

US Signal offers a broad portfolio of IT security solutions and advisory services to help you create and implement a multi-layered cybersecurity strategy. For a brief overview of what's available, visit:

Security Services

Security Advisory Services

Better yet, talk to us. Our solution architects will be happy to review your situation and help you devise a cybersecurity strategy to meet your organization's specific needs.