

cyberwhy

SERVICE GUIDE

System Protection

How layered defenses work, what they cover, and how they are kept effective over time.

01 · OVERVIEW

Why it matters

System protection is about reinforcing what you rely on. No single control stops every attack, so protection is built in layers: endpoint protection on devices, firewalls at the boundaries and between networks, intrusion prevention watching for attacks, and monitoring and updates that keep it all current.

Layered protection means that when one layer is bypassed, the next one still stands. It is designed around your environment and requirements, not copied from a catalog.

Typical triggers

- Devices, servers and networks have grown without a common protection design
- Staff work from many locations and devices
- Testing or an assessment found gaps that need controls
- Production, branch or cloud systems connect to central networks
- You run AI workloads or data pipelines that need to be shielded
- A new compliance or customer requirement asks for protective controls

Who benefits

IT manager

Protection that fits the environment and can be run by the team.

Security lead

Controls with clear purpose, coverage and monitoring.

Operations

Fewer surprises and clear routines for updates.

Management

Assurance that the basics are in place and kept up.

In this guide

01 Overview 2
02 What it is, and what it is not 3
03 How it works, step by step 4
04 What you receive 5
05 In practice 6
06 How to prepare 7
07 Questions, references and terms 8
08 How the services fit together 9

02 · SCOPE

What it is, and what it is not

What it is

- + Layered: several controls so no single one has to do all the work
- + Tailored to your environment and requirements
- + Monitored proactively, so problems can be noticed early
- + Maintained: regular updates keep protection current

What it is not

- – Not a product you install once and forget
- – Not a guarantee that nothing gets through
- – Not a replacement for testing, assessments or response
- – Not the same design for every organization

The controls covered

Endpoint protection

Software on laptops, desktops and servers that detects and stops malware and suspicious behavior at the device itself.

Firewalls

Rules that decide which traffic may enter, leave and move between networks. Segmentation limits how far an attacker can travel.

Intrusion prevention

Systems that watch network traffic for known attack patterns and block them.

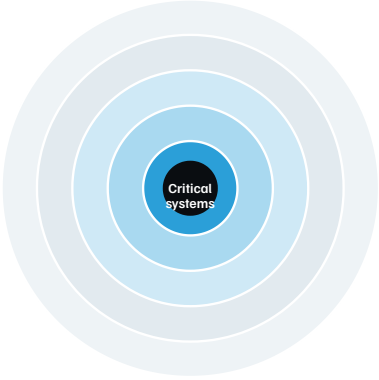
Multi-layered defenses

The combination of controls around critical systems, so each layer covers what the others may miss.

Monitoring and updates

Proactive monitoring of the protected systems and regular updates that keep protection current.

The layers



- Data and backups (often part of the design discussion)
- Identity and access (often part of the design discussion)
- **Monitoring and updates**
- **Network: firewalls, intrusion prevention**
- **Endpoint protection**

Highlighted layers are covered by this service. The outer layers are often discussed in the same design, because the layers work together.

03 · PROCESS

How it works, step by step

A typical engagement, from the first conversation to clear next steps. Exact steps and timing are agreed with you when the work is scoped.

01 Discuss

Understand what you need to protect.

- Talk through your systems, infrastructure and business priorities
- Identify the critical systems and data
- Learn about existing controls, constraints and past issues

YOU PROVIDE
What you need to protect
An overview of your environment

YOU GET
A shared starting point

02 Design

Plan layered protection for your environment.

- Map which layers are needed for which systems
- Choose endpoint, firewall and intrusion prevention controls that fit
- Plan network separation for sensitive systems
- Decide what is monitored and how updates are handled

YOU PROVIDE
Requirements and constraints, such as systems that cannot be changed easily

YOU GET
A protection design for your environment

03 Implement

Put the agreed defenses in place.

- Deploy endpoint protection on the agreed devices
- Configure firewalls and intrusion prevention
- Test that controls work and do not disturb daily work
- Document what is in place

YOU PROVIDE
Access and maintenance windows
A contact for each environment

YOU GET
Defenses in place

04 Monitor

Notice problems early.

- Watch the protected systems proactively
- Look at alerts and unusual activity
- Raise issues with you so they can be handled

YOU PROVIDE
Someone to receive and act on alerts

YOU GET
Systems watched

05 Maintain

Keep protection current.

- Apply regular updates to controls and definitions
- Review rules and coverage as systems and threats change
- Adjust the design when your environment changes

YOU PROVIDE
Early notice of changes to systems

YOU GET
Protection kept current

04 · DELIVERABLES

What you receive

You receive working protection and the documentation that explains it: what is protected by which control, who watches it and how it stays current.

01
Protection design
Layers and controls, mapped to your systems.

02
Implemented controls
Endpoint protection, firewalls and intrusion prevention in place.

03
Segmentation concept
Which networks are separated, and why.

04
Monitoring
What is watched and what happens with alerts.

05
Update routine
How and when protection is kept current.

06
Documentation
A clear record of configuration and responsibilities.

What keeps protection effective

Updates	**Keep current**	Definitions, rules and software are updated so controls recognize today's threats.
Rule review	**Keep lean**	Firewall rules are reviewed so old exceptions do not stay open forever.
Coverage check	**Keep complete**	New devices and systems are brought under protection.
Alert handling	**Keep responsive**	Alerts are looked at, and real issues are handled.

Controls lose value when they are not looked after. These routines are part of the work, with the rhythm agreed for your environment.

05 · IN PRACTICE

Seeing it at work

What each control does, and does not

CONTROL	HELPS AGAINST	DOES NOT COVER ALONE
Endpoint protection	Malware and suspicious behavior on a device	Attacks that never touch the device, such as stolen passwords used elsewhere
Firewalls	Unwanted traffic between networks, and spread inside a network	Attacks that arrive in allowed traffic, such as a malicious attachment
Intrusion prevention	Known attack patterns in network traffic	New or unusual techniques without a known pattern
Monitoring	Gives early notice of unusual activity	Prevention by itself: someone has to act on alerts
Updates	Known weaknesses that are already fixed upstream	Unknown weaknesses, and systems that are never updated

GOOD TO KNOW

Layers around a critical system

Example

NETWORK LAYER	A firewall rule allows only the traffic the system needs, and the system sits in its own network segment.
DETECTION LAYER	Intrusion prevention watches that segment for known attack patterns.
DEVICE LAYER	Endpoint protection on the server detects malware and suspicious behavior.
PROCESS LAYER	Updates and monitoring keep each layer current and noticed.

FOR AI PROJECTS

Protecting projects that use AI

AI workloads often run on powerful servers that hold valuable data and have broad network access. Keep model servers, data stores and pipelines in their own network segments, allow only the connections they need, and watch outbound traffic, since stolen data and abused keys have to leave somewhere.

06 · PREPARATION

How to prepare

A little preparation makes the work faster, safer and more useful. Here is what helps most.

Before we start

- List your devices, servers and networks
- Name the critical systems and data
- Note systems that cannot be changed or patched easily
- Know your maintenance windows
- Decide who receives alerts and who acts on them
- Share existing firewall, endpoint and network documentation

Typical ground rules

- + Changes are planned and made in agreed windows
- + Controls are tested before they go live
- + Configuration is documented
- + Monitoring covers the systems agreed in scope

Common misconceptions

~~Antivirus is enough.~~	**In practice:** Malware is only one path. Firewalls, segmentation, intrusion prevention and updates cover the others.
~~We are too small to be a target.~~	**In practice:** Many attacks are automated and look for any weakness, not for a particular company.
~~Set it up and forget it.~~	**In practice:** Protection decays without updates and review. Monitoring and maintenance are part of the service.

07 · REFERENCE

Questions, references and terms

Frequently asked questions

Do we need all layers?
Not everything everywhere. The design matches protection to the value and exposure of each system.

Will protection slow our work?
Controls are tested before they go live, with attention to daily work. Sensitive systems are handled with care.

Who handles alerts?
This is agreed in the design: who watches, who is informed and who acts.

Can this work with our existing tools?
Yes. The design starts from what you have and fills the gaps.

How does it relate to assessments and testing?
Assessments and tests show where protection is missing. Protection closes gaps. Response helps when something gets through.

How are updates handled?
Regularly and in agreed windows. The rhythm is agreed for your environment.

Reference frameworks and sources

CIS Critical Security Controls	A prioritized set of practical safeguards.
NIST Cybersecurity Framework 2.0	The Protect and Detect functions describe this area.
NIST SP 800-41	Guidelines on firewalls and firewall policy.
NIST SP 800-94	Guide to intrusion detection and prevention systems.
ISO/IEC 27002	A catalog of security controls, including technological ones.

Terms in plain language

Endpoint. A device such as a laptop, desktop, phone or server.

Intrusion prevention. A system that detects and blocks attack traffic.

Defense in depth. Using several layers so one failure is not fatal.

Firewall. A control that filters network traffic by rules.

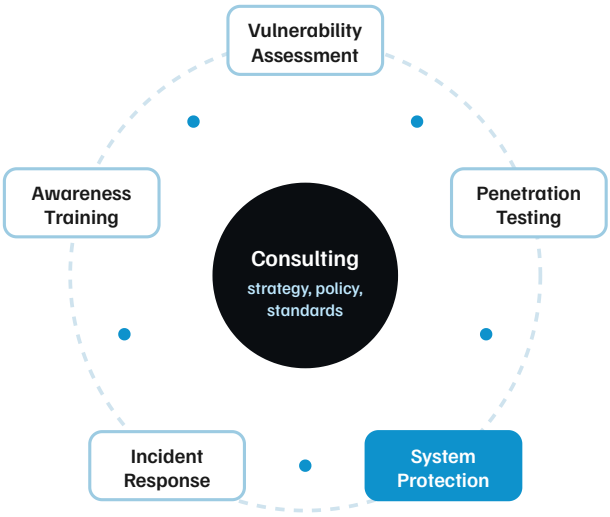
Segmentation. Dividing a network into separated zones.

Egress. Traffic leaving your network.

08 · NEXT STEPS

How the services fit together

Security works best as a cycle: find weaknesses, test them, protect, prepare to respond and keep people alert, all guided by a strategy. You can start with any one of them.



Vulnerability Assessment
Finds known weaknesses across your systems and ranks them.

Penetration Testing
Shows what an attacker can actually exploit.

System Protection (this guide)
Closes gaps with layered, maintained defenses.

Incident Response and Forensics
Acts when something gets through, and learns from it.

Security Awareness Training
Prepares the people who meet threats first.

Cyber Security Consulting
Sets strategy, policy and standards that tie it together.

Talk to a specialist about system protection.

Tell us what you are working on and what you need to protect.

EMAIL
info@cyberwhy.com

WEB
cyberwhy.com/services/system-protection/

This guide describes how work of this kind typically runs. Scope, methods, timing and deliverables are agreed with you for your situation, and nothing in it is a guarantee. References to standards and frameworks are for orientation and do not mean certification. © CyberWhy. All rights reserved.