# Construct Your District's **Multi-Layered Cybersecurity Fortress**

K-12 cybersecurity is all about having multiple defensive layers. That way, you're well-protected across your entire digital infrastructure — which is expanding all the time.

Think of it like a medieval castle. From the inner keep to the kingdom gates, the crown's most valuable treasures are always under lock and key.

1 INFRASTRUCTURE

Like a castle, the IT infrastructure contains your crown jewels — only in this case, we're talking about sensitive information systems that store student, staff, and financial data.
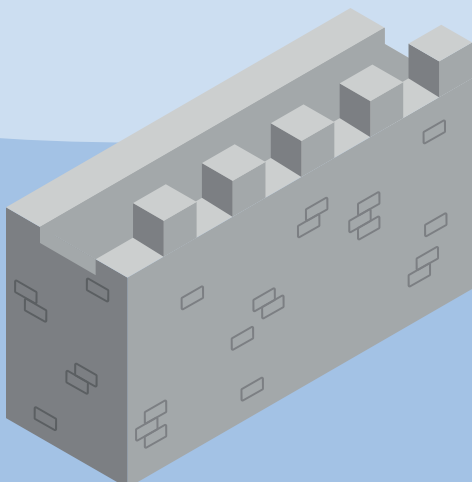
2 NETWORK SECURITY

Firewalls act like moats, protecting your perimeter from unauthorized access. They monitor inbound and outbound network traffic for signs of malicious intent.

3 ENDPOINT SECURITY

Devices, like drawbridges, are how users access your informaation. Endpoint security and antivirus software prevent potential threats from using these pathways to infect your school district.
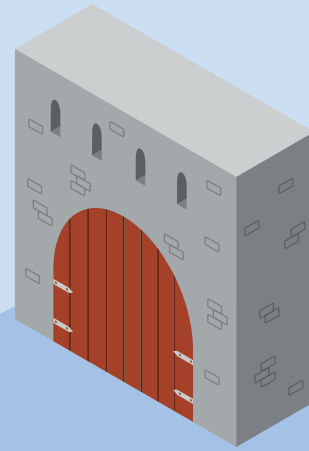
4 IDENTITY AND ACCESS MANAGEMENT (IAM)

Like guards at the kingdom gates, IAM tools use multi-factor and role-based authentication to control who's allowed inside, what they can do, and where they may go

5 CLOUD SECURITY

Imagine a knight in shining armor spotting suspicious activity from the castle's watchtower. That's cloud security, protecting your domain from unseen threats within your castle's walls.

Protecting your digital kingdom is no easy feat, but it's a lot more secure using a multi-layered security strategy. With the above components working together, you can reduce your attack surface, mitigate risk, and keep your district's sensitive information away from criminals.

Want to learn more?
Fortify your defenses by **contacting ManagedMethods today.**

Managed Methods