

STACK THE SECURITY DECK

in your favor

Security always involves risk.

Make sure you **reduce risk** across

THREE DIMENSIONS:



Know the signs of a **vendor** that takes

SECURITY SERIOUSLY:

- Strong tech investments
- An organizational culture of security
- Security personnel (for example, a security team on call with a clear escalation policy)
- A published trust or resource center



Avoid companies with:

- Anything “off” about their website (for example, out-of-date copyrights in the footer)
- Missing security features in the products during trials (for example, no multifactor authentication)

Your security **MUST BE STRONGER** than that of your customers.

Take the following steps (at least):

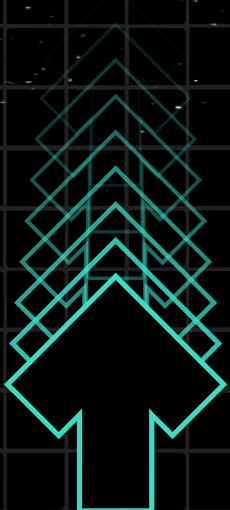
- **Write down** internal business processes
- Use secure, up-to-date, non-legacy tools
- Employ strong endpoint protection driven by **AI and machine learning**
- Track what’s on the network and reduce your attack surface via asset management
- Follow **strong onboarding and offboarding policies** (and use identity and access management tools to help, if needed)
- Enable **multifactor authentication**
- Enforce strong network access controls
- Have a good **VPN** for anyone working remotely
- Deploy a **password manager** to enforce credential best practices

While some customers may be cost-sensitive, it’s better to set a

BASELINE of security layers:

- **Endpoint protection** (preferably an AI-driven endpoint detection and response tool) to prevent new endpoint threats
- **Email protection** to prevent email threats, like phishing, spam, and business email compromise
- **DNS filtering** that uses AI recognition to keep users off unsafe sites
- **Cloud/SaaS security** (especially configurations and credential management) to protect cloud services
- **Vulnerability scanning** to find potential issues like unpatched software or misconfigurations
- **Backup** to bring people back up and running in the event of ransomware or another data deletion
- **Phishing simulations** and **security awareness trainings** to keep end users vigilant against threats

LEVEL UP
your security



Get the **protection, support, and education** you need to own the risk conversation with your customers.

n-able.com/lp/where-security-happens