Liquid Web

Ebook

Your cybersecurity blueprint

Practical steps to build a secure, resilient business

Table of contents

Introduction

It's never been easier to launch and grow a business online—or harder to protect it. Every connection, transaction, and customer record you manage is part of a larger digital ecosystem. And while that connectivity fuels growth, it also creates opportunity for cybercriminals.

If you think your business is too small to be a target, think again.

According to Accenture's Cost of Cybercrime study, **43% of cyberattacks target small and midsize businesses, yet only 14% are prepared to defend themselves.** That gap puts many companies at serious risk—and most never see it coming. The most common threats include:

Ransomware

Attackers encrypt your data and demand payment to unlock it

DDoS attacks

Floods of fake traffic that crash your website or server

Phishing scams

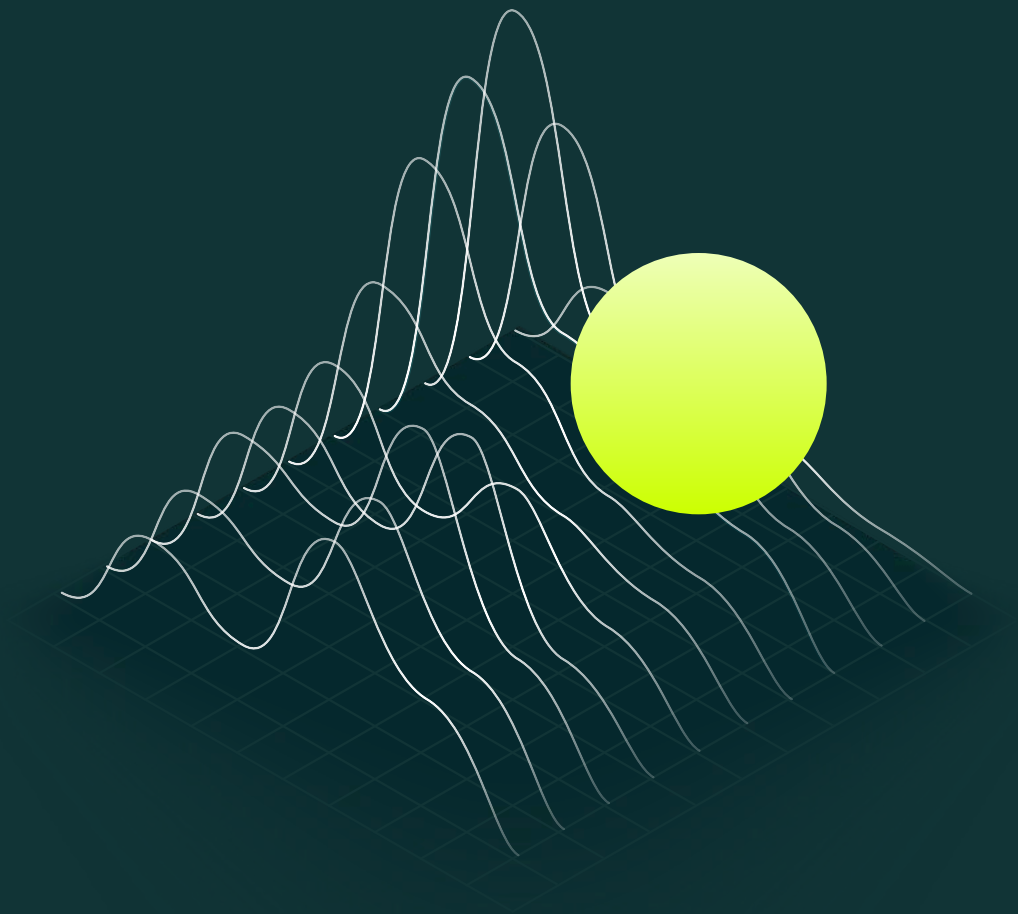
GFraudulent emails or messages that trick users into sharing credentials or financial information

The cost of a single breach can go far beyond money. **Lost trust**, **downtime**, and **data exposure** can threaten the business you've worked hard to build. The good news? You can reduce your risk with a thoughtful, layered approach to security—and the right partner by your side.

This blueprint will walk you through the essentials of building a strong security foundation, from scanning for vulnerabilities and protecting your systems against attacks to training your team, testing your backups, and planning for recovery. You'll also find a simple checklist and practical next steps to help you keep your business secure and resilient over time.

Here's how to build your foundation.

Building resilience through layered protection



Vulnerability scanning

Before you can fix security gaps, you need to find them. Vulnerability scanners automatically map every device connected to your network—from laptops and printers to servers and switches—and identify potential weak points.

A good scanner checks for outdated software, open ports, and default logins that could let attackers in. It then compares your environment against a current list of known vulnerabilities and recommends patches or updates.

If you work with a managed hosting provider like Liquid Web, these scans and updates happen automatically. Our teams identify and resolve vulnerabilities before they become problems, keeping your infrastructure strong and your data secure.

Pro tip

Run scans regularly—not just once. Schedule them monthly (or more often for critical systems) and patch immediately when issues appear.

DDoS protection

Distributed denial-of-service (DDoS) attacks overwhelm your website or server with massive amounts of fake traffic until it slows or crashes. Sometimes it's just malicious chaos. Other times, it's a distraction for a larger breach attempt.

Either way, downtime costs money and reputation. DDoS protection tools monitor network traffic in real time, filtering out bad traffic before it reaches your site.

Ask your hosting provider what level of protection they include—and make sure it scales with your business. With Liquid Web, advanced DDoS protection comes standard on every plan, keeping your sites available and your customers connected no matter what's happening in the background.

Antivirus and firewalls

Antivirus software and firewalls form the backbone of your digital defense. Each plays a different but equally essential role in keeping your systems secure.

Antivirus tools scan your files, directories, and systems to identify, quarantine, and remove threats before they can spread. Today's versions go beyond simple virus detection. They use real-time monitoring and behavior analysis to stop malware, ransomware, and trojans before they cause damage.

Firewalls act as your network's gatekeeper. They inspect incoming and outgoing traffic, blocking suspicious activity before it ever reaches your systems. Think of them as a digital bouncer, checking IDs, spotting trouble, and keeping your data safe inside.

For small and midsize businesses, having both layers in place—and keeping them updated—is non-negotiable. A strong antivirus and properly configured firewall can prevent most common attacks from ever getting off the ground.

Cybersecurity training, policies, and procedures

The vast majority of hosting companies fall into this category. This is the least expensive option, often starting at $10 a month. For that amount, you'll receive a very small portion of a server and share the server with thousands of other websites.

Start with training. Teach employees how to spot phishing attempts, fake invoices, and other social-engineering tactics. Use real-world examples, run internal phishing tests, and make security part of everyday awareness, not just an annual checkbox exercise.

Create clear policies and procedures.

- Require strong, unique passwords and regular updates.
- Set two-step approval limits for vendor payments or fund transfers.
- Limit each employee's system access to only what they need to do their job.
- Revoke credentials immediately when someone leaves the company or a vendor contract ends.
- If your team works remotely, require a secure virtual private network (VPN) for any connection to company systems.

Make security a shared responsibility. Employees should know exactly what to do—and who to contact—if something looks suspicious. When everyone's alert and informed, your people become your first line of defense instead of your biggest vulnerability.

Ongoing human oversight and management

Even the strongest security systems still need human attention. Firewalls, scanners, and automated alerts are powerful, but they're only as effective as the people managing them.

Security isn't a "set it and forget it" process—it's ongoing.

Systems need updates, patches need applying, and alerts need interpretation. Whether you manage everything in-house or partner with a hosting provider, consistent oversight is what keeps your defenses strong.

For many small and midsize businesses, that means making an honest assessment of internal resources. Do you have the expertise and time to monitor vulnerabilities, manage updates, and respond to threats around the clock? If not, a managed hosting provider can help fill that gap.

At Liquid Web, our security experts monitor and maintain the core infrastructure that keeps your hosting environment stable, secure, and always on. With managed hosting, you get a reliable foundation backed by 24/7 support, so your team can focus on growing the business, not maintaining servers.

Protection and remediation planning

Even with strong defenses in place, no system is completely immune. That's why every business needs a clear backup and recovery plan, one that lets you bounce back quickly if the unexpected happens.

Start by backing up ***everything*** that keeps your business running:

- Files and databases
- Operating systems and applications
- Configuration settings and virtual machines
- Cloud-hosted infrastructure and on-device data

Follow a few core principles:

- **Back up daily** whenever possible.
- **Store copies offsite** to protect against natural disasters or local outages.
- **Keep historical versions** for at least six months.
- **Encrypt your backups** to prevent them from becoming a new point of vulnerability.

The goal is simple: ensure your business can recover without losing critical data or momentum. Whether it's a server failure, ransomware attack, or simple human error, reliable backups mean you can restore operations fast and minimize downtime.

Liquid Web's managed hosting includes automated backups and disaster recovery options, so your data stays protected even when the unexpected strikes. Because real security isn't just about prevention—it's about preparation.

Testing your backup and recovery strategy

Backups only matter if they work when you need them. Testing your recovery process is the best way to make sure your systems—and your team—are ready when something goes wrong.

Schedule regular tests to confirm your data can be restored quickly and completely. Aim to simulate real-world conditions: server outages, corrupted files, or accidental deletions. Testing helps you uncover weak points, measure how long recovery actually takes, and refine your plan over time.

Schedule regular tests to confirm your data can be restored quickly and completely. Aim to simulate real-world conditions: server outages, corrupted files, or accidental deletions. Testing helps you uncover weak points, measure how long recovery actually takes, and refine your plan over time.

If your infrastructure supports **automatic failover,** test that too. Failover systems are designed to shift traffic to a healthy node when another goes down, keeping your business online with minimal disruption. Conduct

tests during low-traffic windows and document your acceptable recovery times so everyone knows what “normal” looks like in an emergency.

And remember, testing isn’t one-and-done. Your systems, software, and data change constantly, so your backup strategy should evolve too. Make testing a routine part of your operations, not an afterthought.

When you host with Liquid Web, our team helps ensure your backups and failover systems are configured, tested, and ready to perform, so you can stay focused on running your business, not recovering from disasters.

Teams

Keeping your business secure takes more than technology. It takes people who know how to use it. Cybersecurity is a team effort that requires planning, oversight, and quick action when threats arise.

If you manage security in-house, make sure you have the right roles in place and that responsibilities are clearly defined. Even in a small business, assigning ownership helps prevent gaps in coverage.

Common security roles include:

Chief information security officer (CISO)

Oversees your company’s overall security posture, policies, and response strategy. This role sets direction and ensures the right safeguards are in place.

Network administrator or engineer

Designs, maintains, and secures your network infrastructure. They manage day-to-day operations and ensure your systems stay patched and protected.

Infrastructure manager

Keeps hardware running smoothly—from switches and routers to servers and cables—and ensures physical security aligns with digital protection.

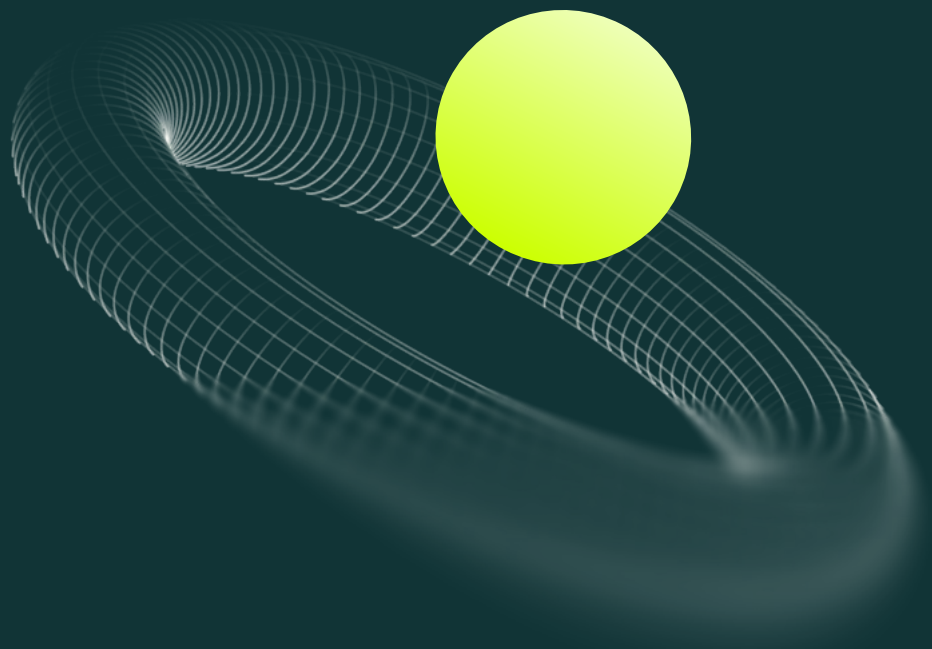
Recovery or incident response team

Activates your backup and recovery plan during an outage or breach. This team should know exactly what to do, who to notify, and how to minimize downtime.

Not every business can staff these roles full-time, and that's okay. Many small and midsize companies choose to partner with a managed hosting provider to fill the gaps.

At Liquid Web, our dedicated security specialists act as an extension of your team, monitoring systems, responding to threats, and keeping your infrastructure safe 24/7. It's expert support when you need it most, without the overhead of building your own around-the-clock security team.

Cybersecurity checklist for your business



Cybersecurity checklist for your business

Use this checklist to review your current security setup and identify areas that need attention. Strong protection comes from consistent, layered practices, not one-time fixes.

Your security essentials:	Yes	No
Perform regular vulnerability scans and patch any weaknesses right away.	○	○
Set up DDoS protection to keep your sites and systems online during attacks.	○	○
Install antivirus software on all devices and keep it updated.	○	○
Configure a firewall to block suspicious traffic before it reaches your network.	○	○
Provide ongoing cybersecurity training for your team.	○	○
Establish clear policies and procedures for passwords, data access, and vendor payments.	○	○
Back up files, databases, applications, and configurations daily.	○	○
Store some backups off-site and encrypt them for safety.	○	○
Test your backup and recovery plan regularly.	○	○
Assign ownership of security tasks or partner with a managed provider for 24/7 coverage.	○	○

Pro tip

Treat this checklist as a living document. Review it quarterly and update it as your business, tools, and team evolve

Considerations

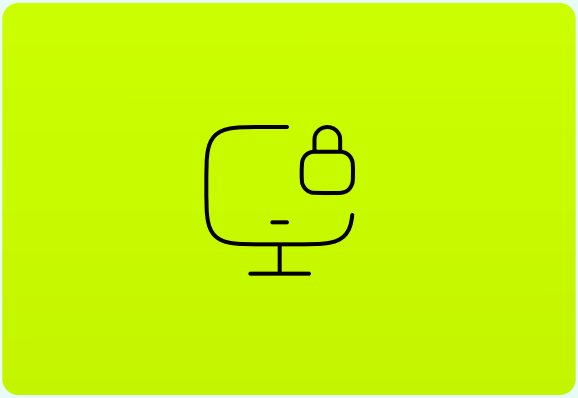
Managing cybersecurity on your own can be challenging and expensive. Many growing businesses don't have the time or staff to monitor systems, apply patches, and respond to threats around the clock.

If security isn't your team's core focus, consider partnering with a managed hosting provider. The right partner can handle the technical side of protection so you can focus on running and growing your business.

With Liquid Web's fully managed hosting, you get enterprise-grade security, proactive monitoring, and expert support—all designed to keep your data, sites, and customers safe.

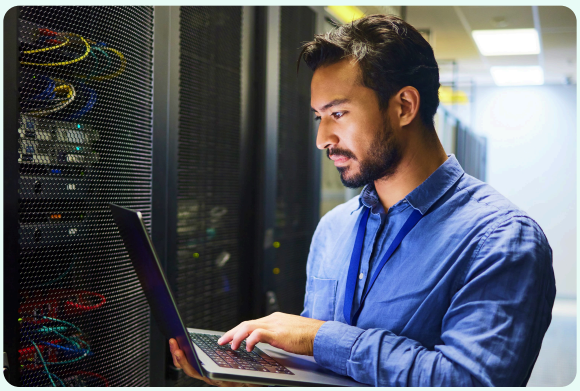
Protect what you've built

Cybersecurity isn't optional anymore. It's a core part of running a successful business. Whether you manage it internally or lean on a trusted partner, protecting your systems protects everything you've built.



Don't wait for a breach to take action. Strengthen your defenses, keep your backups tested, and make security a habit across your entire team.

With Liquid Web by your side, you can rest easier knowing your business is protected by experts who are always watching out for you.



About Liquid Web

About Liquid Web

For more than 25 years, Liquid Web has powered content, commerce, and growth for the designers, developers, and businesses creating online. We've built our reputation on secure, reliable hosting—backed by people who care as much about your success as you do.

Our managed hosting solutions help you move faster, stay protected, and scale with confidence, whether you're running a single site or a complex infrastructure.

When you choose Liquid Web, you get more than a platform. You get a partner dedicated to your uptime, performance, and peace of mind.