IN-DEPTH GUIDE SECURITY AND COMPLIANCE

Secure a company's site: the complete guide

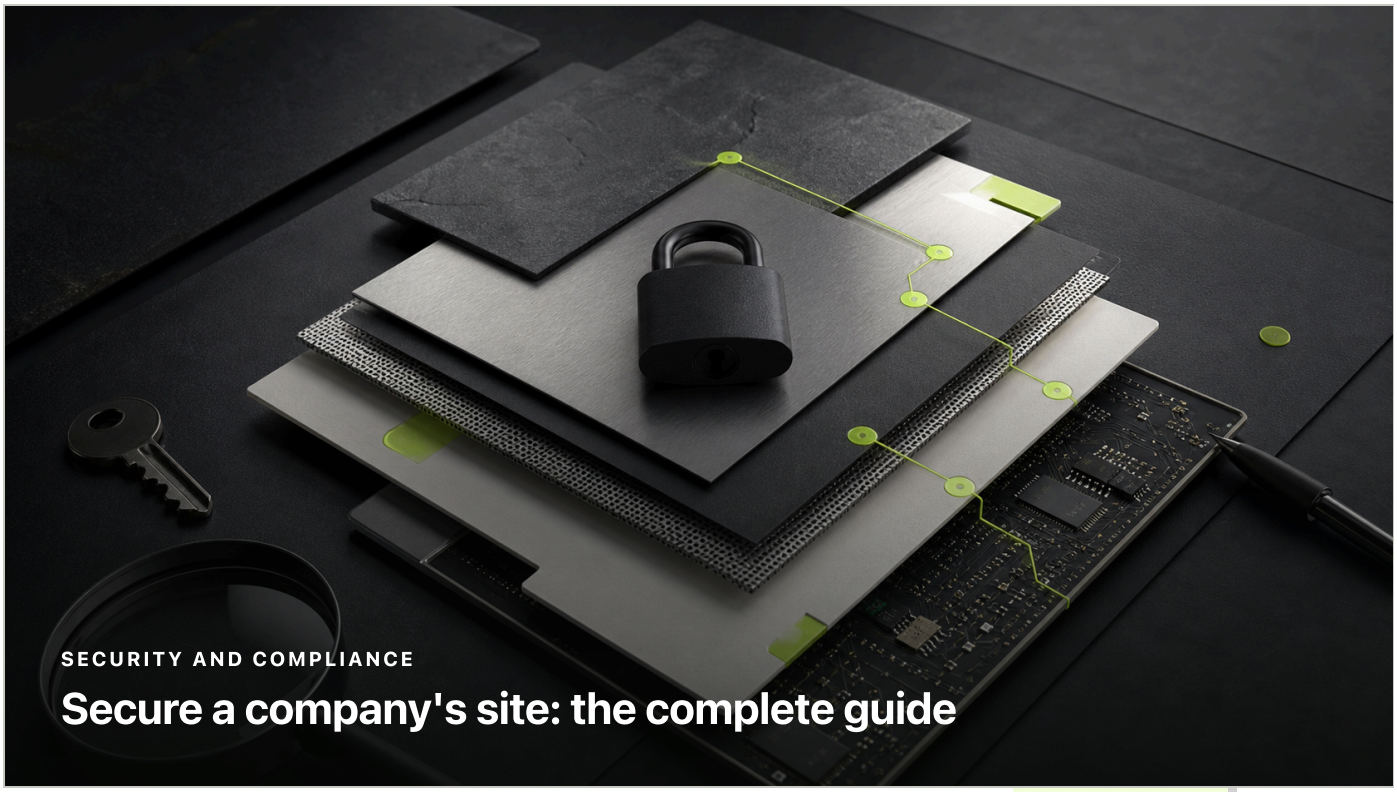
The five layers of protection every business website should have, explained simply, and how to know if you're really protected.

G

GXN
Senior expertise · Digital governance

Quebec First
Quebec business context

July 31, 2026
Updated



SECURITY AND COMPLIANCE

Secure a company's site: the complete guide

TL;DR

The answer in one minute

A well-protected business site is based on five layers, not one. Accesses and who can connect, updates applied regularly, a firewall that filters known attacks before they reach the site, surveillance that quickly detects problems, and backups that have actually been tested. Remove a single layer weakens the whole, regardless of the strength of others.

01 · BACKGROUND GUIDE

Why there's no perfect security, and why it's okay

No site is completely secure, and anyone who promises perfect security is selling an illusion. What really exists is the ability to significantly reduce risk, quickly detect when something is wrong, and be able to recover properly in the event of an incident. The gap between a neglected site and a well-protected site is immense, although neither is perfectly invulnerable.

02 · BACKGROUND GUIDE

The first layer, access

The majority of security incidents start with mismanaged access, not a sophisticated attack. A weak password reused elsewhere. A former employee account never deactivated. Access shared between several people without traceability. The most cost-effective first line of defense is simply knowing who has access to what, and removing what is no longer needed.

DECISION CARD

The four angles to keep together

01

Why there's no perfect security, and why it's okay

02

The first layer, access

03

The second layer, updates

04

The third layer, the application firewall

GUIDE READING GRID

Angle	Dimension to examine	Use in the decision
01	Why there's no perfect security, and why it's okay	Setting the Context
02	The first layer, access	Identify dependencies
03	The second layer, updates	Compare options
04	The third layer, the application firewall	Preparing for the next step

The second layer, updates

Every piece of non-updated software represents a publicly known vulnerability, which automated attackers actively seek out at scale. Putting off updates for fear of breaking something is understandable, but it accumulates risk that grows over time. Best practice is to test updates before applying them to production, not to avoid them indefinitely.

INTERACTIVE TOOL

Set your decision

Select the dimensions that describe your situation. The result is to organize the next conversation, not to replace an analysis.

WHAT CONCERNS YOU NOW

- 01 **Why there's no perfect security, and why it's okay**
- 02 **The first layer, access**
- 03 **The second layer, updates**
- 04 **The third layer, the application firewall**

Urgent decision 5

Current control level 5

RECOMMENDED ANALYSIS

Several dimensions must be treated together

Avoid an isolated decision. Map out the dependencies and agree on an intervention order.

45 / 100

The third layer, the application firewall

A filter placed between the Internet and your site, which blocks known attack attempts even before they reach your platform. It is the equivalent of a guard at the entrance that refuses suspicious visitors before they enter the building. This layer alone blocks a significant proportion of automated attempts that affect all sites without exception, continuously.

05 · BACKGROUND GUIDE

The fourth layer, surveillance

Detecting a problem in hours rather than weeks completely changes the magnitude of the consequences. Continuous monitoring observes suspicious changes, site availability, and signals of possible compromise. Without this layer, an incident is often only discovered when a customer reports it, which is the worst way to find out.

06 · BACKGROUND GUIDE

The fifth layer, the truly tested backups

The most neglected layer, despite its capital importance. A backup that exists in theory but has never been restored for real is not a guarantee, it's a hope. The only test that really matters is a successful full restore, performed periodically to confirm that everything is working as expected.

07 · BACKGROUND GUIDE

How to know if you are really protected

Some concrete checks that you can do yourself. Ask anyone who manages your site when the last major update took place. Ask if an application firewall is active, and on what basis it is configured. Ask who has access to the site at this time, and if this list has been recently revised. Ask to see proof of a successful backup restore, not just confirmation that a backup exists somewhere.

- If these questions remain unanswered, a vulnerability probably exists, even in the absence of any visible incident at this time.

08 · BACKGROUND GUIDE

What I see on the ground

In twenty years of cleaning up compromised sites, almost all of them shared the same basic profile. No updates for a long time, forgotten accounts, no backup ever checked. The attack itself was almost never sophisticated. It was accumulated neglect that opened the door, year after year, until someone found it.

09 · BACKGROUND GUIDE

When this guide does not fully apply

If your site is purely informative, without any information gathering or transactional role, the level of protection required may be smaller than for a site that processes customer data or payments. Core layers remain relevant, but the intensity of monitoring can be adjusted downwards.

Frequently asked questions

01 **WordPress is reliably secure.**

Yes, well maintained. The vast majority of compromised WordPress sites were neglected sites, not victims of faults impossible to correct.

02 **How much does serious protection cost.**

03 **How often should we test our backups.**

04 **Is my small business really a target?**

EDITORIAL METHOD

In-depth guide prepared by GXN based on real business situations. Recommendations remain independent of brands and suppliers.

OFFICIAL SOURCES

References to be checked according to your situation

These references support the external rules and frameworks cited in this guide. They are not a substitute for legal or professional advice tailored to your organization.

Canadian Center for Cyber Security

Basic Cybersecurity Controls for Small and Medium Organizations ↗

G

ABOUT THE PUBLISHER

GXN

Senior expertise directly accessible, supported by specialists when the project requires it.

Discover GXN ↗

NEXT STEP

You want to know where the security of your site really is.

The free assessment covers just this aspect, without unnecessary jargon.

No call required. No sales sequence.