DATA SECURITY · FOR DECISION-MAKERS

Your company data in NexaStack – *how safe is that, really?*

Anyone leaving the big subscription platforms today for their own, self-operated software stack rightly asks: is my company data actually safer or less safe on my own server than with Microsoft, Google, or Dropbox?

The honest answer: on a poorly configured server — less safe. On a server set up the way your NexaStack is — considerably safer. And above all, it's clear **where your data lives, who has access, and who is responsible in an emergency.** With a big multi-tenant cloud, none of that is clear.

> *Picture your NexaStack as a company building. To reach the data inside, an attacker would have to clear five hurdles in a row – all five at once and unnoticed, in the same night.*

Inside this building live all your company's data: documents, calendars, contacts, passwords, chats, contracts. Break one hurdle, and the next still stands.

01 The location & the front door

1

HURDLE 1 · THE LOCATION

A secured, audited data center — and a single tenant: you.

The building doesn't stand just anywhere — it sits in a guarded, SOC 2–audited US data center: access controls, video surveillance, fire suppression, backup power. Your NexaStack runs as a **single tenant** — not in a shared multi-tenant pool — so you control who has access, rather than relying on a vendor's internal policy. With the data-center operator there is a written data-processing agreement (DPA) setting out all data-protection obligations, and your data is encrypted at rest and in transit.

2

HURDLE 2 · THE FRONT DOOR

One entrance, and a lock no password can open.

A normal building has many doors, windows, and delivery entrances. Yours doesn't. From the outside there is exactly one entrance; every other wall is windowless and sealed. That's the firewall — a digital firewall that blocks everything not explicitly allowed.

And that single door has no lock you can type a password into. That's deliberate: password login simply doesn't exist. The door opens only when a specific digital key is presented — a mathematically unique code that exists on a single admin device and nowhere else in the world. It can't be guessed, intercepted, or cracked by dictionary. The classic password-guessing that attackers run in loops hits a wall — there's nothing to guess.

Anyone who still tries gets thrown out hard: three failed attempts and the attacker's internet address is fully blocked for 24 hours, with the block automatically extended on repeat. The server's master "super-admin" login is also fully disabled — one of the most common reasons servers get taken over is operators leaving that master key open for convenience.

03 The individual offices inside

3

HURDLE 3 · ISOLATION

A break-in to one application is never automatically a break-in to all.

Suppose, purely hypothetically, an attacker did find a way through the door. What do they find then?

Not one big open room with all the data, but a building full of individually locked offices. Each application has its own office with its own door, its own key, and its own filing cabinet: Nextcloud in its office, OnlyOffice in its office, Vaultwarden in its office, Paperless in its office. Around 50 such offices in total, across 22 separated corridors.

The crucial point: these offices have no connecting doors. Whoever got into the Nextcloud office stands only in front of the Nextcloud files. They see no passwords from Vaultwarden, no documents from OnlyOffice, no invoices from accounting. They don't even see that those other offices exist. Each application also has its own separate cabinet with its own key — so a break-in to one application is never automatically a break-in to all.

In every office there's also a strict digital supervisor. It watches every action the software takes and permits only what the software needs for its actual purpose. If an attacker managed to take over an application and misuse it — copying data, attacking other areas, loading malware — the supervisor blocks it immediately and raises an alarm. On a compromised Nextcloud instance you therefore can't "just look around to see what else is on the server." The attacker is stuck in that one office.

One more thing, invisible but important: every connection from your laptop or phone to the server is encrypted. No one in between — a café Wi-Fi, a hotel connection, a public event — can read which documents are opened or which passwords are entered.

04 The watch service & the fallback

4

HURDLE 4 · THE WATCH SERVICE

The system watches the building — and checks itself every night.

A round-the-clock digital watch service runs on the server with two jobs. **First:** every suspicious activity is logged. Every login, every access, every change to a security-critical file lands in a record that can be inspected and analyzed — so if something unusual does happen, it's fully documented. **Second:** the system checks itself. Every night an automatic control runs to see whether even a single important file was unexpectedly changed, the way a museum guard checks each night that every painting is still in place. Weekly, specialized programs additionally scan for known malware, hidden tampering, and newly disclosed vulnerabilities in the installed software. If something is found, an alert fires automatically.

The point that matters most in practice: **security updates are applied automatically.** The most dangerous server isn't the one under attack — it's the one that hasn't had an update in months and sits online with known, long-closed holes.

5

HURDLE 5 · THE FALLBACK — DAILY BACKUPS

Even in the worst case, nothing is lost.

Assume the worst: despite all four previous hurdles, something bad happens anyway — a hardware failure, a fire in the data center, or a very sophisticated attacker who encrypts all the data and demands a ransom (what the news calls "ransomware"). Even then, nothing is lost. Every night at 4:00 a.m. a complete, encrypted copy of all data, databases, and settings is transferred to a second, physically separate US location. These copies are kept for 14 days — so a rollback is still possible even if a problem only surfaces a week later. Once a quarter it's tested whether everything can actually be restored from these backups — a backup that's never been tested is not a backup, it's a hope. In the worst emergency, the complete NexaStack is running again on a new server within two to four hours. No data loss, just half a working day of downtime.

AND IF SOMETHING HAPPENS ANYWAY?

05 Two written plans take effect immediately

SECURITY INCIDENT RESPONSE PLAN

Defines to the minute what happens in the first 60 minutes, the first 4 hours, and the first 72 hours: who informs whom, which data is secured first, when affected parties are notified under applicable breach-notification rules, and when you, as the decision-maker, are brought in.

OPERATIONS MANUAL & SECURITY CONTROLS

Concrete step-by-step runbooks for every realistic outage scenario — so in an emergency you execute rather than improvise. Backed by a formal security-controls document suitable for SOC 2 / vendor security reviews and customer inquiries.

What it adds up to

Your data doesn't sit "somewhere on the internet." It sits in a guarded US data center, behind a single door that opens only with a non-copyable key, in individual offices with no connections between them, under permanent self-monitoring, and with a daily, encrypted, actually-tested backup at a second location.

WHY WE CAN SAY THIS PLAINLY

This is not theory and not a marketing claim. It is exactly the security level our own production infrastructure runs on — the same environment where our own customer data and business records live. What's good enough for us is good enough for you.

STILL HAVE A QUESTION?

Ask us on a strategy call.

No obligation, no sales script. — nexastack.co/en/strategy-call