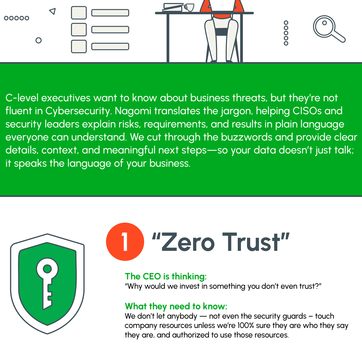
nagomi

10 Security Buzzwords that Get Lost in Translation



C-level executives want to know about business threats, but they're not fluent in Cybersecurity. Nagomi translates the jargon, helping CISOs and security leaders explain risks, requirements, and results in plain language everyone can understand. We cut through the buzzwords and provide clear details, context, and meaningful next steps—so your data doesn't just talk; it speaks the language of your business.

1 "Zero Trust"

The CEO is thinking:
"Why would we invest in something you don't even trust?"

What they need to know:
We don't let anybody — not even the security guards – touch company resources unless we're 100% sure they are who they say they are, and authorized to use those resources.

2 "Holistic"

The CEO is thinking:
"Is this some kind of zen wellness approach?"

What they need to know:
Everything in our security stack works well together. There are no major gaps or disconnects that force us to piece together fragmented data.

3 "Defense-in-depth"

The CEO is thinking:
"I guess that's better than a shallow defense…"

What they need to know:
Our security strategy uses multiple tools, techniques, and policies to protect our data and prevent downtime.

4 "Real-time monitoring"

The CEO is thinking:
"Wouldn't it have to be?"

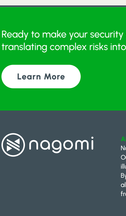
What they need to know:
Our security tools are always on, scanning our traffic and environment for potential threats.

5 "Single pane of glass"

The CEO is thinking:
"How many panes do we need?"

What they need to know:
Our analysts can see alerts and the health of multiple security tools on one screen without having to switch back and forth between multiple dashboards or monitors.

6 "Comprehensive"



The CEO is thinking:
"OK. I'm with ya. That sounds good."

What they need to know:
We don't have huge areas out there where threats could be getting in without us knowing it.

7 "360-degree"

The CEO is thinking:
"Wouldn't that leave us right back where we started?"

What they need to know:
Our tools and analysts can see any threat coming at us from every direction.

8 "Resilient"

The CEO is thinking:
"Resilient"? Are we preparing for a cyber-zombie apocalypse?"

What they need to know:
We have tools in place that back each other up—and—should a cyberthreat or attack take down one of our assets, we can shift things around so that the business never shuts down.

9 "Cutting-edge"

The CEO is thinking:
"In other words: we're not sure this is going to work?"

What they need to know:
Our old stuff wouldn't cut it. This new stuff might do the trick.

10 "End-to-end security"

The CEO is thinking:
"That's good. I'm gonna use that one!"

What they need to know:
We're in good shape — our data, devices, and applications are all being monitored and protected by effective security controls wherever users log in and use company resources.

Ready to make your security strategy business-friendly? Contact us today to start translating complex risks into data-driven results that everyone can understand.

Learn More

nagomi