NordLayer®

Handling objections

Objection categories

01

Business value

02

Daily value

03

Organization fit

04

Alternatives consideration

Objection categories

01

Business value

02

Daily value

03

Organization fit

04

Alternatives consideration

Objection handling

Business value

OBJECTION:

What is the business value for this solution?

HANDLING

In the context of accelerating business migration to cloud and with the increasing scale of remote work, it is essential to take measures to protect business data and to avoid:

- Potential losses due to fines by regulators in case of data breach
- Customer claims in case of compromised data
- Paused services and lost revenue due to accidents
- Wasted employees' time due to poorly functioning VPN (on average costing 4.45 million dollar, IBM)

Not having clear measures in place is also likely to keep a business from external investments, partnerships or sales to larger corporate clients with increased security requirements. Cybersecurity measures and data protection becomes an increasingly important factor for gaining customer trust and ensuring business continuity.

More on business value

Objection handling

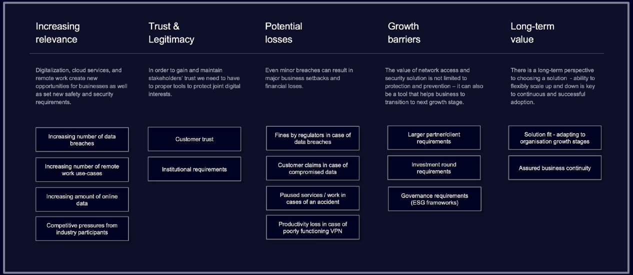
Business value

OBJECTION:

Is it worth the investment?

HANDLING

On average data breach costs 4.45 million dollars for small to medium enterprises and this number is increasing every year due to bigger scale and handling complexity. Network security and access solutions costs up to 10 dollars per user per month which equals to the amount spent for slack, Trello and other similar work tools.



Increasing relevance	Trust & Legitimacy	Potential losses	Growth barriers	Long-term value
Digitalization, cloud services, and remote work create new opportunities for businesses as well as set new safety and security requirements.	In order to gain and maintain stakeholders' trust we need to have to proper tools to protect joint digital interests.	Even minor breaches can result in major business setbacks and financial loses.	The value of network access and security solution is not limited to protection and prevention – it can also be a tool that helps business to transition to next growth stage.	There is a long-term perspective to choosing a solution - ability to flexibly scale up and down is key to continuous and successful adoption.
Increasing number of data breaches	Customer trust	Fines by regulators in case of data breaches	Larger partner/client requirements	Solution fit - adapting to organisation growth stages
Increasing number of remote work use-cases	Institutional requirements	Customer claims in case of compromised data	Investment round requirements	Assured business continuity
Increasing amount of online data		Paused services / work in cases of an accident	Governance requirements (ESG frameworks)	
Competitive pressures from industry participants		Productivity loss in case of poorly functioning VPN		

More on business value

Objection categories

01

Business value

02

Daily value

03

Organization fit

04

Alternatives consideration

Objection handling

Organization fit

OBJECTION:

Do we need such a solution if we don’t work in a sensitive data industry?

HANDLING

Even though media features only large-scale cyber attacks such as the data breaches at Facebook, Netflix, and such financial institutions as JP Morgan, the frequency of small to medium businesses' data breaches is equally high making up 43% of total cyber-attacks (small biz trends, 2019).

Also, contrary to popular belief, industries that are facing higher risks in terms of data breaches are not limited to healthcare, finance or governmental sectors. Manufacturing, professional and business services, energy, retail and wholesale, transportation, education and media companies are also facing significant risks too.

Chances of accidents and attacks also increase if your organization employs remote or hybrid work models. Accident frequency might be even higher in cases where employees are not properly trained and lack the necessary tools to secure their network and be aware of potential risks.

Finally, it's worth taking a second thought if you think that your organization does not have anything sensitive to protect. If you are storing clients' records, financial information, employees’ personal data or intellectual property of any kind, you might become a target.

Objection handling

Daily value

OBJECTION:

Don’t we need a VPN only while traveling? What if we only work from office or home?

HANDLING

It is true that VPN is essential while traveling and connecting to public Wi-Fi as it is impossible to identify and control who has access to the same network thus making malicious takeover extremely easy. However, home network can also be easily compromised due to a known location or other users who are using the same network with or without the owner’s knowledge.

Regardless the network location, the risk of other internet threats such as phishing remains relevant and can potentially cause data leakages and increase vulnerabilities.

Objection handling

Daily value

OBJECTION:

What if employees do not want to use it?

HANDLING

There are different models ranging from encouragement to enforcement which can be used to onboard employees and ensure continuous cybersecurity tool usage. In most of the cases, we recommend using a combination of approaches, i.e. implementing strict usage policies and supporting teams and leadership through repeated educational and awareness actions. Since the NordLayer solution is simple and easy to install, it creates a minimal amount of friction and does not disrupt employees workflow.

Objection handling

Daily value

OBJECTION:

Is the deployment going to be complicated and time-consuming?

HANDLING

Instant deployment. NordLayer is extremely simple to setup and test with a limited number of users or the whole organization.

Straightforward security. It takes only one click to safeguard all data traffic on your device. Pick a server or a gateway to connect to, and your connection becomes secure. Worried you'll forget to turn the app on? Switch on the auto-connect feature, and the app will secure your device automatically.

Third-party authentication. No need to create and manage yet another set of credentials. You and your team can connect to NordLayer with Azure AD, Google, OneLogin or Okta accounts.

Objection handling

Daily value

OBJECTION:

How can we be sure that the solution is working and actually protecting our data?

HANDLING

The network security and access tool does not interrupt employees' work, but if a user visits a potentially malicious site, they are notified about the potential danger right away. In addition, an administrator can overview and track the usage of the solution across the organization.

Objection categories

01

Business value

02

Daily value

03

Organization fit

04

Alternatives consideration

Objection handling

Organization fit

OBJECTION:

Will it work with our solutions and infrastructure?

HANDLING

Our product is designed to provide an additional layer to existing hardware or software solutions - there is no need to make any changes regarding your current infrastructure.

Objection handling

Organization fit

OBJECTION:

Will we need all the functionalities? Won’t they overcomplicate the employee experience?

HANDLING

Some features are hard to live without when using a VPN service and others are simply nice-to-haves. It’s a ‘set it up and forget it’ kind of scenario. Once you tailor the VPN service settings to your liking, there is no need to keep coming back to the Settings page.

Objection categories

01

Business value

02

Daily value

03

Organization fit

04

Alternatives consideration

Objection handling

Alternative consideration

OBJECTION:

Wouldn’t a simple VPN be enough?

HANDLING

A personal VPN does not provide centralized control and administration of employees’ devices and, as a result, makes it difficult to ensure proper and continuous usage. Advanced and security-oriented features like dedicated server and single-sign-on are only available with a business VPN.

A personal VPN is primarily intended for personal use and is not regarded a proper network access and security tool.

Objection handling

Alternative consideration

OBJECTION:

Shouldn’t we adapt an advanced fully integrated cybersecurity suite?

HANDLING

Companies should choose solutions that are a good match to their current resources, existing roles and competencies. Utilizing advanced solutions requires specific roles, additional budget and continuous involvement of dedicated teams. Selecting, integrating and launching such solutions require extensive preparation and feature long-term roadmaps. Not having the right setup and a real business need might result in a company wasting considerable resources just to adapt a solution that is going to be utilized only to a fraction of its potential.

NordLayer provides comprehensive security, easily integrates with existing infrastructure and does not require additional planning or preparation.

Objection handling

Alternative consideration

OBJECTION:

Wouldn't the new service pose extra challenges when our business situation changes and we have to rapidly downscale or upscale our team?

HANDLING

With NordLayer, there are no hidden costs and you can change your subscription at any time.

Note: Payment must be made upfront for user and server licenses on an annual subscription plan. To downscale, please get in touch with your Account Manager or contact our 24/7 Customer Support team.

NordLayer®

If you have any questions, contact our tech-minded sales team!

P. (647) 951-4411
E. ictnet@ictnetworksystems.ca
W. https://www.ictnetworksystems.ca/contactus