Case study

Third-party security: Avoiding a breach through your outsourcing partner

The recent breach of India-based outsourcing giant Wipro has proved that insecure third-party firms can be a conduit for compromise of their clients and partners.

Avoid the Wipro breach scenario

In April 2019, one of the largest IT outsourcing and consulting giants Wipro was breached following a phishing attack and several of their customers' networks targeted by leveraging Wipro's privileged vantage point into their network. Phishing emails successfully targeted several Wipro's employees which lead to access to their corporate network and by using site-to-site VPNs between Wipro and its customers, attackers later breached the client networks. In Wipro's example, the attackers' goal was to carry out a mass gift card fraud. The attack was discovered when Wipro's clients noticed malicious activities originating from Wipro's network. This breach has proved the danger that third-party firms with insufficient security practices can be effective pivot points into a customer's network and cause major damage.

The problem

Breaches originating from third-party vendors and suppliers are among the fastest growing risks to an organization's sensitive data and reputation. Despite the major risks, companies continue to rely on third-party providers and share confidential and sensitive information with site-to-site VPN setups. The lack of centralized control and network segmentation, the complex nature of third-party relationships make it complicated to mitigate risks.
On average, companies don't know if the third-party's security practices are enough to prevent a potential breach. Moreover, only less than half of all companies prioritise managing third-party risks.

Traditional solutions provide remote access which exposes all corporate network and increases breach risks.

Third-party risks for companies:

- Increased attack possibilities.
- Often third-party vendors don't have sufficient security practices.
- Third-party companies can be compromised and their systems used to launch attacks on partners or clients.

Trust and verify isn't enough.

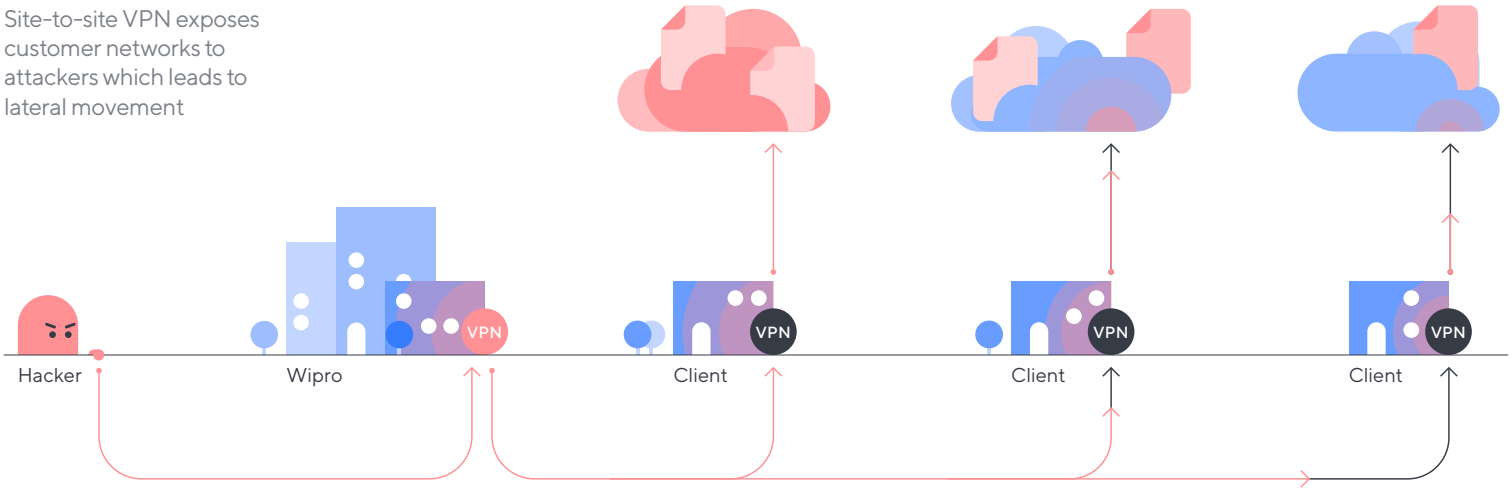
60% of companies vet third-party security practices

59% of companies experience a data breach due to suppliers

16% of companies effectively mitigate third-party risks

22% of companies didn't know if they had a third-party data breach in the last 12 months

Site-to-site VPN exposes customer networks to attackers which leads to lateral movement



Fyde solution

Fyde enables app and identity-driven segmentation to prevent full network exposure and continuously monitors access to prevent breaches such as Wipro.

In the age of increasing number of supply chain attacks, Fyde protects organizations from third-party breaches so you can focus on productivity and efficiency.

Granting only the necessary and least privileged amount of remote third-party access to enterprise resources is critical to ensure enterprise security.

To avoid third-party originated breaches such as the Wipro case, Fyde has built a software-defined remote access and security solution, to mitigate third-party risk to businesses by providing application centric segmentation, visibility and control while improving security and IT operations. Fyde's modern VPN alternative, enables secure, reliable and fast access to sanctioned apps and services in your network from any device, network and location. It's easy to set up, monitor and manage. Fyde solution is designed to improve the security posture of unmanaged devices, protecting user identities on-the-go, and preventing against phishing and account takeover attacks.

- Strengthen third-party and supply chain security
- Don't just rely only on employee awareness training to spot phishing
- Gain visibility into IT outsourcer activities
- Avoid reputational damage
- Prevent from phishing attacks

Fyde limits third-party access to authorized user identities, devices and continuously monitor access requests