> **End users have shared that they love that they log in to their PC and it just works, whether they are in one of the office locations, at home, or traveling.**

Milan Baria
Founder and CEO, Blueclone Networks

Improving client cyber resilience after ransomware by replacing VPNs and RDP with SASE

In a ransomware attack, a company's network security approach—especially regarding remote access—can mean the difference between one system being infected and the entire organization. One global manufacturing company learned this lesson when its traditional approach to remote network access led to a full-scale ransomware breach. Having gone through three IT service providers already, their CEO knew he needed to turn to Blueclone Networks as they began dealing with an incident response firm in the aftermath.

Modernizing infrastructure with SASE

Milan Baria, Blueclone's founder and CEO, and his team looked over the existing infrastructure and immediately identified several areas to improve. The manufacturing company was using **four Remote Desktop Protocol (RDP) servers hosted in Azure** to connect global and remote users to the headquarters network. Those servers were **open to public IPs** and authenticated via OpenVPN. Somehow, the **company's three previous MSPs missed the security risks and ramifications of this setup** and struggled to incorporate the company's other non-standard IT needs.

When Blueclone jumped in to help, they knew Todyl SASE would be the ideal solution to this issue.

"**With Todyl SASE, we were able to block all traffic into Azure and cut out the VPN and RDP setup entirely.**" Baria continued, "The client loves it, not only because they don't have to log into a VPN, but because it's helped them reduce costs. There's no OpenVPN license ($1800/year), no Azure servers ($4500/year), backups, or egress bandwidth charges. **We helped them save upwards of $6k a year, and because of that, they're very happy.**"

Beyond that, Blueclone has seen **tickets from the client around VPN and remote access issues disappear**. Their employees' systems are also **running much better since removing the previous MSP's security software**. They don't have to deal with VPNs and their servers, and their network drives and ERP system are always available with no connection issues.

After Baria and his team resolved the networking vulnerability, **they won the client's trust and became their full-time MSP**.

$6K
yearly cost savings by eliminating VPNs and RDP servers

15 hours
a week saved by reducing helpdesk tickets

Zero
ransomware incidents since turning to Blueclone and Todyl

todyl

How Blueclone saved the day

Client experiences ransomware attack

The system the client had in place to enable remote work was exploited by adversaries to infect end users and infrastructure alike with ransomware. The client's current IT providers couldn't find the root cause of the issue nor help them with proper incident response reporting.

They turned to Blueclone because:

- They had gone through 3 MSPs prior to the attack
- Their remote work access process was compromised, and they couldn't report properly for IR
- They had worked with Blueclone in the past and trusted their expertise and guidance

Blueclone acted fast to help:

- Immediately shut down all ingress and egress traffic to the client
- Identified weak VPNs and exposed RDPs being used to access Azure
- Determined a need for an overarching network security solution

Blueclone knew that SASE was the only logical path forward

Through SASE, Blueclone blocked all traffic into and fully cut out existing firewalls, VPNs, and RDP ports. To do so, Blueclone relied on Todyl SASE to create streamlined, secure access to network resources.

How Todyl's SASE helped Blueclone support their client

Todyl SASE allowed Blueclone to remove the need for VPNs and hardware firewalls at headquarters and satellite offices altogether. Thanks to the Secure Global Network™ (SGN) Cloud Platform backbone, the client could frictionlessly connect remote users to their resources. From Blueclone's perspective, it all happened through Todyl's single pane of administrative glass for SASE, SIEM, Endpoint Security, and more.

Client completes IR audit and moves forward from ransomware attack

Thanks to Blueclone, the client was able to the ransomware attack behind them and ultimately come out with a better security posture. Blueclone uses Todyl across all its clientele, providing the same best-in-class support and service to any business in need of security and compliance assistance.

About Blueclone

Blueclone Networks is an MSP based out of Princeton, NJ, USA that provides small and medium-sized businesses with computer services, cloud app expertise, VoIP, 24/7 helpdesk, cybersecurity, and more. They also offer co-managed IT services to larger organizations and enterprises worldwide, serving clients in the finance, legal, insurance, pharmaceutical, healthcare, and manufacturing industries.