

CASE STUDY

Building trust in the age of AI-powered threats

Profile

- Company: Aegisys Cloud Solutions
- Website: www.aegisys.com
- Location: Greater Sudbury, Ontario, Canada
- Specializations: Managed IT services for healthcare, municipal government, law enforcement, and finance

Challenges

- **Sophisticated cyberattacks are becoming widely accessible:** Threat actors are leveraging AI to chain together complex exploits, creating pressure to deliver 24/7 proactive defense.
- **Strict data residency requirements:** Highly regulated sectors, such as healthcare and law enforcement, require sensitive data to remain within the country, even when delivering advanced automation to stop machine-speed threats.

Solutions

Barracuda Email Protection and Barracuda Managed XDR: Aegisys built its 'strategic architecture of resilience' by mastering the Barracuda stack. Barracuda's solution countered sophisticated attacks from lateral movement and account takeovers.

By integrating Barracuda Automated Threat Response (ATR) with Barracuda Firewalls, the team was able to automate routine remediation tactics such as brute force attack mitigation, freeing up time to focus on strategic priorities. To solve the data residency puzzle, they use Barracuda Cloud-to-Cloud Backup, ensuring client data remains encrypted and stored within Canada to meet strict regulatory mandates.

Results

- **Proactive protection:** By moving from a break-fix model to security-as-a-service, Aegisys helps customers shift from "We hope nothing bad happens" to "We'd know immediately if it did."
- **Rapid response:** Using AI-driven Automated Threat Response rules, response times for critical threats such as firewall breaches have dropped from hours to mere minutes.
- **Massive scale:** A lean team of 19 now manages more than 300 clients while maintaining 24/7/365 coverage that rivals much larger firms.
- **Compliance at its core:** Aegisys achieved SOC 2 Type 2 certification — a status held by only 5% of MSPs worldwide — by using Barracuda's infrastructure to prove continuous operational integrity by using Barracuda's infrastructure to prove continuous operational integrity.





Aegisys Cloud Solutions combines 27 years of expertise with Barracuda's digital labor to deliver high-impact security outcomes.

In the world of managed services, trust is the most valuable currency, but it's also the most fragile. "A really bad day could undo 20 years of trust," says Rick Beyers, President of Aegisys Cloud Solutions. Based in Greater Sudbury, Ontario, Aegisys doesn't just see its 300 clients as accounts; they're "friends and family."

To protect that family in an era where AI-driven attacks can chain separate exploits together in seconds, Rick and his team have moved beyond traditional antivirus. They've built a defense-in-depth strategy that continuously adapts to an evolving threat landscape, combining AI-powered detection, automation and human expertise to stay ahead of increasingly sophisticated attacks.

That strategy begins with preventing attacks before they gain a foothold. By combining Barracuda Email Protection with Managed XDR, automated response and resilient backup services, Aegisys delivers multiple layers of protection that work together rather than relying on any single security control.

Turning minutes into seconds with automation

For Aegisys, the secret to serving 300 clients with just 19 employees is what they call digital labor. By leaning into the Barracuda Managed XDR platform and automation capabilities, the firm has automated the drudgery of tier 1 and tier 2 workflows.

When a brute force attack hits a client's firewall at 3 a.m., the system doesn't wait for a human to wake up. It identifies the signal, triggers a rule and neutralizes the threat instantly. "We count on Barracuda so we can wear our superhero capes," Rick explains. This proactive approach ensures that by the time a client starts their day, the threat has already been neutralized.

The same philosophy applies to email security. As phishing attacks grow more sophisticated and AI-generated messages become increasingly convincing, Aegisys relies on Barracuda Email Protection to identify malicious emails, suspicious links and dangerous attachments before they reach users. "Email continues to be one of the biggest attack vectors for our clients," Rick says. "Barracuda Email Protection has evolved tremendously over the years and gives us confidence that we're stopping more threats before they become incidents."

Automation also extends beyond threat detection. By integrating Barracuda Managed XDR's ATR capabilities with its firewall environment, Aegisys can automatically generate and deploy security rules within minutes, rather than relying on engineers to manually respond to every event. That allows the team to spend less time reacting to alerts and more time helping clients strengthen their overall security posture.



Solving the Canadian residency puzzle

One of the biggest hurdles for Aegisys' municipal and healthcare clients is the fear that moving to the cloud will mean their data crosses international borders. Rick uses Barracuda's global infrastructure to demonstrate that it can be done without risking non-compliance.

By using Barracuda's dedicated Canadian data centers for cloud-to-cloud backup and email protection, Aegisys ensures that sensitive data stays in-country. This helps ensure that clients meet the rigorous standards of PIPEDA (Personal Information Protection and Electronic Documents Act) and provincial health acts. It allows Aegisys to act as the "gatekeeper of insurability" for their clients, making complex regulatory compliance feel easy.

Cloud-based backup has also transformed the level of resilience Aegisys can deliver. Automated synchronization to secure offsite locations and immutable backups give clients enterprise-class protection that was once difficult or cost-prohibitive for many organizations to implement.

> *"We count on Barracuda so we can wear our superhero capes."*
>
> Rick Beyers, President
> Aegisys

Success through transparency and empathy

While the technology is advanced, the Aegisys philosophy remains grounded in human empathy. They've transitioned from flat-rate contracts to a subscription-based model that itemizes every layer of protection. This transparency helps clients see exactly where their investment goes, from immutable backups to 24/7 SOC monitoring.

Clients also gain visibility into the multiple layers working behind the scenes, including advanced email protection, immutable backups, managed detection, automated response, and continuous security monitoring. Instead of viewing cybersecurity as a collection of individual products, Aegisys helps customers understand how each layer contributes to a more resilient security strategy.

As they look toward the next decade, Aegisys continues to reinvest their growth into operational maturity. By mastering every layer of the Barracuda stack, they've broken the cycle of reactive IT and emerged as a strategic partner that doesn't just manage tickets but secures futures.

Barracuda
Your business, secured.

About Barracuda

Barracuda is a leading global cybersecurity company providing complete protection against complex threats for all sized businesses. Our AI-powered BarracudaONE platform secures email, data, applications, and networks with innovative solutions, managed XDR and a centralized dashboard to maximize protection and strengthen cyber resilience. Trusted by hundreds of thousands of IT professionals and managed service providers worldwide, Barracuda delivers powerful defenses that are easy to buy, deploy and use.

US 1.0 • Copyright 2026 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com
Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.