Pine Gate Renewables: Defeating Ransomware and Advanced Persistent Threats in Just Four Months

Pine Gate Renewables faced the dual challenge of scaling operations while defending against the sophisticated threats increasingly targeting the energy sector.

INDUSTRY
Renewable Energy

EMPLOYEES
+500

HEADQURTER
Asheville, North Carolina

47% More
Ransomware resilience

64% More
Ransomware resilience

23% More
Overall Resilience

Executive Summary

The key success factor was Reclaim's ability to rapidly analyze Pine Gate Renewables' environment, deploy tailored security policies, and deliver measurable results from day one accumulating 47% ransomware resilience improvement and 64% APT protection enhancement over four months while saving 587 hours of manual work, all with zero business disruption.

Key Results

+47% improvement
Ransomware resilience

+64% improvement
Advanced Persistent Threat resilience

+23% improvement
Overall threat resilience across all threat categories

587 Hours Saved
$117K operational efficiency value

Zero Business Impact
Safe remediation with no productivity disruption

$400K+ Annual Potential
Ongoing savings identified

> "We knew we had gaps in our Microsoft security stack, but fixing them manually would've meant pulling my team off everything else for a year. Reclaim showed us exactly where we were exposed to threats, then actually fixed it without breaking anything. Four months in, we've improved our Ransomware resilience nearly in half and saved my engineers hundreds of hours they'd have spent researching configs and testing changes."
>
> **L.C. Williams, CISO, Sr Director Security & IT Operations, Pine Gate Renewables**

The Challenge: Critical Infrastructure Under Siege

As a rapidly growing renewable energy company operating critical grid infrastructure, Pine Gate Renewables faced the dual challenge of scaling operations while defending against the sophisticated threats increasingly targeting the energy sector. The challenges included:

- **Overwhelming Manual Effort:** Analyzing thousands of settings across various security tools to identify exposures, and then countless hours researching the right solution, ensuring it won't have any negative business impact, and validating its effectiveness over time.
- **Configuration Complexity:** Difficulty optimizing existing security tools to maximize protection against threats while maintaining business operations. Hundreds of thousands of security findings required analysis, prioritization, and tailored remediation strategies.
- **Resource Constraints:** While their security team possessed deep expertise, they were responsible for protecting expanding digital infrastructure while supporting rapid business growth leaving little capacity for the extensive manual security engineering required.
- **Time Pressure:** Traditional manual approaches would take 12-18 months to properly analyze behaviors, create tailored policies, test configurations, and deploy changes all while maintaining zero business disruption.

PIPE™: The Technology Behind Safe Automation

Reclaim's patent-pending PIPE™ (Productivity Impact Prediction Engine) is what makes truly automated remediation possible. Unlike traditional approaches that recommend changes without understanding business impact, PIPE™ uses behavioral data analysis to learn how each organization actually operates, then simulates every security change to validate it won't disrupt productivity.

For Pine Gate Renewables, PIPE™ delivered:

- **Automated behavioral analysis** of Pine Gate's operational patterns using historical data eliminating the typical 6-8 weeks required for manual behavioral analysis and stakeholder interviews.
- **Pre-deployment simulation** of every configuration change to predict exactly which users and workflows would be affected.
- **Prediction accuracy** on business impact, enabling confident automation without the fear of operational disruption.
- **Continuous validation** confirming each policy's effectiveness and accumulating threat resilience improvements from day one.

The Solution: Business-Aware Security Automation

Reclaim Security's preemptive approach compressed what would typically require 12-18 months of manual work into a focused 4-month engagement requiring just 2-4 hours per month of the team's time freeing them to focus on strategic initiatives while improvements began from day one.

Rapid Initial Assessment

- **Seamless API integration** with Pine Gate's Microsoft security stack, completed in minutes.
- **Comprehensive analysis** of thousands of settings across their environment automated assessment that would require 8-10 weeks manually.
- **Intelligent correlation** of hundreds of thousands of findings into 67 actionable exposures, prioritized by impact on threats resilience.
- **Clear dashboard** delivered within showing progressive improvement paths.

Security Domains Optimized

- **Email Security (Microsoft Defender for Office 365):** Common Attachment Filters and Anti-Phishing policies with User Anti-Impersonation protection deployed across all mailboxes.
- **Operating System controls** deployed across all workstations.
- **Endpoint security (Microsoft Defender for Endpoint) optimization** preventing lateral movement and persistence.
- **Identity protection (Microsoft Entra ID):** deployed across all user accounts defending against credential compromise.

Focus on optimization of existing Microsoft investments rather than adding new tools maximizing ROI on security spend already made.

Progressive Implementation

- **Continuous deployment** throughout the 4-month period with built-in guardrails ensuring zero business disruption.
- **Progressive validation** confirming each policy's effectiveness and accumulating threat resilience improvements from day one.
- **Near real-time validation** of all deployed configuration changes.
- **Automated confirmation** that would require weeks of manual security testing.

Ongoing Protection: Adaptive Security Posture

Building on the initial 4-month success, the ongoing partnership with Reclaim Security continues to provide Pine Gate Renewables with:

- **Continuous threat monitoring** across Pine Gate's renewable energy business ecosystem, validating deployed configurations in near real-time.
- **Business-aware recommendations** ensuring zero disruption to critical operations while progressing toward additional improvement potential.
- **Automatic configuration adaptation** to handle security drifts, keeping the progressively deployed improvements current as threats evolve.
- **Ongoing optimization roadmap** to deploy additional improvements achieving remaining threat resilience enhancement and security stack optimization potential, delivering $400K+ in annual value.

Key Takeaways for Security Leaders

Pine Gate Renewables' 4-month engagement demonstrates that organizations can:

1. **See results from day one with minimal team involvement:** 47% ransomware improvement and 64% APT enhancement progressively accumulated over four months requiring just 2-4 hours per month of team time vs. 12-18 months of intensive manual work for traditional approaches.
2. **Eliminate hundreds of hours immediately:** 587 hours of manual work eliminated through the initial 4-month engagement, freeing security talent for strategic initiatives.
3. **Deploy progressively without sacrificing quality or safety:** Automated behavioral analysis and PIPE™ technology deliver superior results faster than manual approaches while ensuring zero business disruption.
4. **Deliver measurable value within a quarter:** Demonstrate concrete security improvements and realized cost savings ($117K) in four months.

About Pine Gate Renewables

Pine Gate Renewables is a leading developer, owner, and operator of utility-scale solar energy projects, dedicated to accelerating the transition to clean, renewable energy across the United States.

About Reclaim Security

Reclaim Security is a preemptive exposure management platform founded by former Microsoft Defender executives. Our patent-pending PIPE™ (Productivity Impact Prediction Engine) technology predicts business impact with accuracy before deploying security changes, enabling safe automated remediation. Recognized by Gartner in multiple 2025 reports on preemptive cybersecurity, we help security teams implement and maintain optimal security configurations across their technology stack, reducing mean time to remediate exposures, improving team operational productivity, ensuring security stack consistency, and maximizing return on existing security spending, all with zero business disruption.

See Results Like Pine Gate's

Request a complimentary 10-day proof of value to see your own ransomware resilience score and identify high-impact, zero-disruption remediation opportunities.