# How Tata Power Maintained 100% Uptime While Blocking 860mn+ Attacks

## OVERVIEW

- **860M+** cyber-attacks blocked across Tata Power's digital ecosystem
- **100% uptime** maintained, even as **~70% of applications** faced **DDoS attacks**
- **60+** critical applications, across 11 ports, 2100+ APIs, and IoT platforms secured
- **$102K+** in SOC operational savings in one year

As Tata Power's digital footprint expanded across applications, APIs, enterprise platforms, and IoT services, scaling application-layer security became a priority. The focus was to protect availability, enhance threat visibility, and enable early risk detection across a complex hybrid environment without adding operational overhead.

Working closely with Tata Power's security team, Indusface's fully managed, cloud-based WAAP operated as an extension of their internal SOC. Indusface took ownership of day-to-day DDoS monitoring, vulnerability prevention, virtual patching, and continuous policy tuning across the digital ecosystem.

The partnership was proven at scale in 2025 during sustained application-layer DDoS and vulnerability-exploit attacks. Indusface helped block **over 860 million attacks** while eliminating alert fatigue and incremental SOC effort, delivering approximately **$102K+ in annual operational savings** and establishing a scalable security foundation for long-term digital growth.

## ABOUT TATA POWER

Tata Power is India's largest integrated power company, with operations spanning power generation, transmission, distribution, and renewable energy. The organization supports critical national infrastructure and serves millions of customers nationally.

Alongside its core energy operations, Tata Power operates a rapidly expanding digital environment that includes enterprise platforms, customer-facing applications, internal systems, APIs, and connected digital services. This includes IoT-enabled offerings under the **EZ Home** smart living brand. Ensuring the **security and availability** of these digital systems is central to both operational reliability and customer trust.

"Even with multiple security tools in place, cyber risks can go undetected due to noise, fragmented visibility, and human fatigue. Indusface functions as an independent '**third eye**', working closely with our internal security teams to continuously monitor and protect our application and API landscape 24×7. Indusface ensures threats are identified and contained early, before they can impact availability, data security, or critical business operations."

- Corp Cyber Security Team, Tata Power

## KEY SECURITY CHALLENGES

1. Hybrid and Evolving Digital Landscape

   Tata Power's applications run across on-prem infrastructure and cloud, spanning both staging and production environments. The landscape includes a mix of legacy systems, modern architectures, and IOT services that continue to evolve.

   Maintaining consistent application-layer protection across this landscape became increasingly complex as scale and traffic volumes have grown.

2. Critical Enterprise Systems on Custom Ports

   Several important enterprise platforms, including SAP and third-party systems, operate on non-standard ports. Most WAAP solutions primarily support only HTTP and HTTPS traffic, which leaves gaps when services run outside these default ports. At Tata Power's scale, any unprotected port directly increases the risk surface.

3. Large-Scale, Adaptive DDoS Attacks

   As digital adoption increased, Tata Power experienced recurring DDoS activity ranging from low-volume probing to sudden, large-scale surges. These attacks were often designed to mimic legitimate user behavior, making it difficult to distinguish from normal traffic using traditional, threshold-based controls.

4. Alert Noise and Operational Pressure

   With multiple security controls already in place, the challenge was not a lack of data, but too much of it. Correlating alerts from internal firewalls, application traffic, and attack telemetry in real time was resource-intensive and difficult to sustain at scale efficiently.

## SOLUTION

1. Fully Managed 24x7 Security Operations

   Indusface's managed SOC continuously monitors application traffic and applies core security policies and virtual patching to defend against both known and emerging application-layer vulnerabilities.

   AppTrana blocked **260+ open vulnerabilities** across legacy and third-party systems at the **WAF layer**, virtually patching them through a combination of **core and custom security policies**. This approach reduced downtime risk caused by technical debt and saved Tata Power **$52K+ in patching effort**, while providing continuous protection during extended remediation cycles, where code-level fixes for legacy and third-party components can take up to six months. By shielding business-critical systems throughout this window, Indusface helped Tata Power minimize exposure without forcing rushed changes or disrupting stable operations.

In 2025, over **620 million attacks** were blocked through finely tuned security policies for TATA Power's application landscape.


*Attacks blocked by core rules in 2025*

From Dec 2 to 27, attackers failed with DDoS attempts. When they switched to vulnerability exploits, Indusface combined AI detection with human SOC response to block the surge from Dec 28 to 31, preventing a serious breach with no business disruption.


*Vulnerability exploit surge blocked between Dec 28 and Dec 31, 2025*

## 2. Behavior-Based DDoS Mitigation with 100% Uptime SLA

Instead of relying on static thresholds, Indusface leverages **AI-ML models** to understand normal traffic behavior and detect anomalies during attacks. This capability proved critical during large-scale DDoS incidents in August when traffic surged **400x above normal levels** and once more in December 2025 when traffic surged over **600x the baseline**.


*DDoS attack surge in August and December 2025*

Using behavioral DDoS, malicious traffic was stopped without affecting legitimate users, eliminating the need for emergency manual intervention.

Even during these large-scale attacks, Indusface ensured Tata Power maintained 100% uptime, keeping business operations uninterrupted.

## 3. Comprehensive Coverage Across All Exposed Ports

Indusface extended WAAP protection across all exposed ports beyond HTTP and HTTPS, including those used by SAP, legacy platforms, and internal services. This ensures consistent application-layer security without requiring changes to existing application architecture or workflows.

4. Continuous API Discovery and Protection

   Using **AI-driven traffic analysis**, Indusface continuously identified and protected **over 2100 APIs**, including undocumented and newly exposed endpoints. This ensured API security kept pace with ongoing application changes without manual inventory management.

5. Centralized Security Logs

   With **Security Information & Event Management (SIEM) enabled**, the Tata Power team seamlessly integrates WAF-generated logs with their existing SIEM platforms, gaining centralized visibility into security events along with actionable alerts.

6. Securing IoT and Connected Platforms

   Indusface also extended protection to Tata Power's **EZ Home IoT platforms**. This reflects a future-ready security posture that goes beyond traditional websites and applications to secure connected and emerging digital services.

## RESULTS

- **860.06 million** application-layer attacks blocked across **60+** digital services
- **151.75 million** DDoS attacks mitigated using behavior-based controls in 2025
- **2.4 million** automated bot attacks blocked
- **100% uptime** maintained across customer-facing & enterprise platforms during peak attack periods
- **270+ vulnerability exploits prevented** (via a mix of core and custom rules) by Indusface, reducing exposure during patching cycles with no dev effort from Tata Power's side
- **~$102K+** saved in one year through reduced SOC operational effort (as per SOC & engineering cost in India)
- **~$7.4 million+** in estimated breach risk avoided

## Looking Ahead: Securing the Next Phase of Digital Growth

As Tata Power's digital ecosystem continues to evolve, the security focus is expanding to include AI-driven applications, automated workflows, and growing machine-to-machine interactions across platforms and infrastructure.

Indusface is supporting this next phase through AI-Shield, which extends protection to AI-enabled applications and APIs, strengthens coverage for IoT and smart infrastructure services, and utilizes advanced behavioral analysis to detect AI-driven and automated attack patterns.

Through its ongoing partnership with Indusface, Tata Power has established a resilient and scalable application security model that strengthens protection without adding operational friction. This approach enables the organization to support both current operations and future innovation, while ensuring early risk detection, sustained availability, and uninterrupted digital services.