Godrej Industries Group Unified Its Cyber Defenses

The global conglomerate modernized its cyber defenses and achieved near 99.9% uptime with Akamai's integrated security portfolio

Eliminated downtime

Unified protection

Eased IT management

A legacy business continually modernizes

Godrej Industries Group, one of India's most diversified conglomerates, operates across 16 countries in sectors ranging from real estate and chemicals to agribusiness and finance. As the group modernized its operations and applications, its attack surface expanded rapidly. To secure critical infrastructure, digital assets, and customer data across hybrid environments, Godrej turned to Akamai. With Akamai Guardicore Segmentation, Akamai App & API Protector, and Akamai API Security, the organization unified its cyber defenses, reduced disruptions, and effectively protected hundreds of applications and servers.

Building security for a digital-first enterprise

With a 128-year legacy and a footprint spanning 1.1 billion customers, Godrej Industries Group has evolved into a digitally connected ecosystem. From ERP and CRM to Industry 4.0 tools and mobile apps, technology drives every part of the business.

As Godrej moved forward on its digital transformation journey, cybersecurity became central to its strategy. "Cybersecurity is not just an IT function — it's integrated into the business," explained Satyavrat Mishra, Head of Corporate IT and CISO.

Cybersecurity at Godrej is guided by a multilayered defense model based on National Institute of Standards and Technology (NIST) and ISO 27001 standards. With Akamai, that strategy evolved into a unified, resilient framework spanning network, cloud, and application layers. The first step was securing east-west traffic.

Location

Mumbai, India
godrejindustries.com

Industry

Business Services

Solutions

Akamai Guardicore Segmentation

API Security

App & API Protector

From limited control to constant disruption: The challenges of legacy microsegmentation

According to Mishra, a traditional firewall cannot stop the spread of attacks that occurs when a hacker gains access to an internal application or server. "That's why microsegmentation is so important," he explained.

Godrej's first microsegmentation tool fell short. Mishra's team struggled with limited scalability and complex maintenance. Needing detailed analysis of lateral (east-west) traffic, the team had to manually define granular rules to address all scenarios. That included how and when applications talk to one another, while accounting for the multiple protocols and various services that enabled communications among systems.

"It was challenging to manage all those rules. Plus, the solution sometimes misread services as threat actors and shut them down, resulting in unplanned downtime," recalled Mishra.

In addition, the solution depended on the operating system's firewall, turning policy enforcement into a major challenge. It also lacked the flexibility to assign role-based access, making it impossible to prevent administrators and application owners from viewing or modifying rules outside their own application boundaries.

Gaining real-time control and protection at scale with Akamai Guardicore Segmentation

After evaluating numerous vendors, Godrej selected Akamai Guardicore Segmentation for its granularity, intuitive dashboards, and rapid protection mode.

Akamai Guardicore Segmentation:
- Provides fine-grained visibility and control over east-west traffic
- Delivers real-time microsegmentation with customizable policy rules
- Minimizes lateral movement and simplifies compliance reporting

"We liked Akamai's approach," Mishra said. "The solution provides seven layers for defining rules and uses its own enforcement engine for both Windows and Linux."

Godrej runs workloads across multiple platforms, including Nutanix on-premises and major public clouds. Akamai Guardicore Segmentation was deployed across Godrej's hybrid environment — including Azure, AWS, and private clouds — protecting more than 600 servers. Agents on every server enable continuous control, monitoring, and traffic protection across the environment.

"Akamai Guardicore Segmentation integrated easily with our ecosystem to enforce a least-privileged model, prevent lateral malware movement, and protect critical assets. As soon as we implemented the solution, it went into protect mode," Mishra said.

"

Thanks to Akamai's seamlessly integrated solutions, our critical servers and applications are continuously secured and working.

— **Satyavrat Mishra**
Head of Corporate IT and CISO, Godrej Industries Group

The difference was immediate. "Akamai Guardicore Segmentation solved our most pressing challenges: analyzing east-west traffic at scale and making all those service disruptions go away."

Protecting 300+ applications with Akamai App & API Protector

Building on the success of Akamai Guardicore Segmentation, Godrej deployed Akamai App & API Protector to defend against web exploits, distributed denial-of-service (DDoS) attacks, and malicious bots.

Akamai App & API Protector:

- Combines web application firewall (WAF), DDoS defense, and bot mitigation in one solution
- Offers AI-driven dashboards for visibility and threat detection
- Scales to secure web applications globally

"In just six months, we protected more than 300 applications," Mishra said. "Before that, we had no visibility into who was accessing our apps or from where. Now we have complete dashboards showing attacks by geography and bot activity."

That visibility also translated into stability. "We achieved nearly 99.9% uptime with most of our applications," Mishra said. "Ultimately, security is about keeping applications online and keeping threat actors out, and Akamai delivered exactly that."

Unifying visibility and protection with Akamai API Security

Having already adopted App & API Protector, Godrej wanted a seamlessly integrated API protection layer.
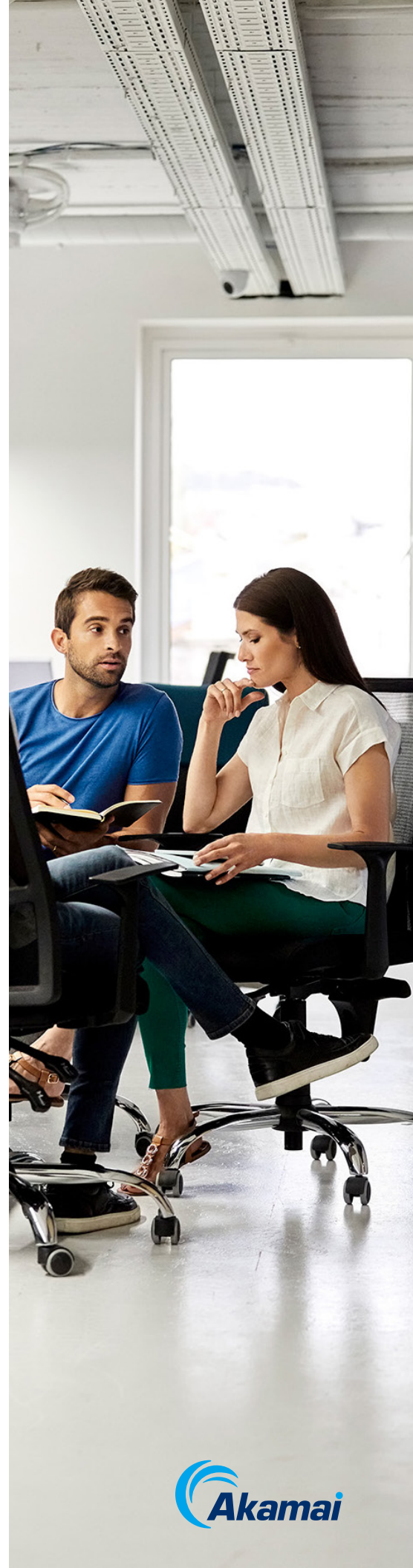
"APIs are one of the most critical components of a digital infrastructure framework, enabling integration with financial institutions and supply chain partners, among others," Mishra said. "But if not properly protected, they can become entry points for attackers."

Akamai API Security:

- Discovers and inventories all APIs across environments
- Detects vulnerable or shadow APIs in real time
- Prevents abuse and attacks through unified policy enforcement

"API Security was an extension of what we were already doing," Mishra said. "It provides a unified dashboard for web and API protection, which is critical for day-to-day management."

As Mishra explained, his team conducts frequent red team exercises to test the security of the organization's applications. "In all those exercises, API Security has successfully stopped malicious actors," he said.

API Security also provides real-time alerts and is backed by strong support. "We haven't experienced any major downtime or escalations, but if something goes wrong, Akamai provides local support and quick resolutions," he added.

Strengthening trust through cyber resilience

For Godrej Industries Group, trust and simplicity go hand in hand. Protecting customer data in real time is non-negotiable, and Akamai's unified suite of cybersecurity solutions makes that possible.

According to Mishra, Akamai has proven to be a trusted security partner and a one-stop shop for protecting Godrej's applications and APIs. "Akamai gives us everything we need in one reliable, easy-to-manage platform. Plus, its unmatched threat intelligence helps stop attacks at the edge," he said.

With fewer disruptions, reduced operational pressure, and continuous protection, Godrej's team can focus on enabling business growth. "Thanks to Akamai, our critical servers and applications are continuously secured and available. Akamai gives us peace of mind and our customers the confidence that we are protecting their experiences and data," Mishra concluded.

At the Godrej Industries Group, we are privileged to serve more than 1.1 billion consumers globally through our businesses with market leadership positions in the consumer products, real estate, agriculture, financial services, and chemicals industries.