Data is everything.

Each day, the 18,000+ people at UST Global are solving significant, next-generation problems for Fortune 500 companies. Working in the areas of IoT, API economy, augmented intelligence, and cognitive computing, this Company is an innovation partner for enterprises seeking to accelerate their digital transformation. And to support operations of this magnitude, UST Global has an infrastructure build that spans across continents. An infrastructure that handles data, not just for itself, but also its customers. But, where there is data, threats are inevitable.

The Company’s network is constantly fighting threats. The IT security team has to tackle possible threats like unauthorized access to data center assets, policy violations, and botnets used by organized criminals and hackers for phishing and stealing intellectual property, to name a few.

And, adding to its security concerns, malicious activity can originate not just from outside, but through compromised hosts inside the organization as well. UST Global quickly realized that it had to put strong security in place, and came up with a robust strategy to protect the infrastructure and its systems from all layers. It needed a solution that could continuously analyze file activity across its extended network, quickly detect and contain threats, while also providing a detailed trajectory of the malware movement in the network to quarantine affected systems.

“We needed to increase our security posture, to protect our assets from cyber threats, and the way to do this was with multiple layers of next-generation, automated protection systems across all locations,” says Praveen Raveendran, Director & Global Head, IS Infrastructure Team, UST Global.

The threats stop here.

A network that’s intelligent enough to accurately identify, classify, and stop or block malicious traffic in real time. That’s what UST Global needed. An intrusion prevention system that worked as an additional layer of defense on the perimeter layer, against known and zero-day attacks.
In December 2016, the order was placed for Cisco’s Intrusion Prevention System. A month later, the solution was deployed and configured across UST’s data and development centers in India, the US and the Philippines. Cisco Network-based IPS sensors and the central Firesight Management Console provided the exact solution to safeguard high value information from cyber threats.

“Our existing single-switching network was behaving like a bottleneck to the deployment of Cisco IPS and working around the bottleneck was difficult to replicate across geographies. Further, it would have created an operational nightmare for our troubleshooting team,” says Chandranhari Nair, Lead IT Security.

But UST Global’s security operations team, in collaboration with Cisco, had a better idea.

They worked extensively to create a ‘redundant’ switching layer that a) connected all devices on the perimeter of the network b) separated the external network from the intranet c) placed the Intrusion Prevention System right at the center. All, so that UST Global could inspect all traffic going out and coming in.

When Cisco’s Intrusion Prevention Solution started proving effective within a few weeks of its deployment, UST Global knew it had made the right choice. The dashboard showed up possible attacks being blocked by the sensors.

“Collaborating with Cisco - the industry leaders in security, helped us adopt best practices. Cisco brought extensive knowledge and experience with it while deploying the product in our heterogeneous environments,” says Praveen Raveendran.

While UST Global’s security posture has certainly become more robust, this has directly translated to more secure network infrastructure and applications. The Company’s network now has real-time threat and malware intelligence, as well as, complete visibility into applications, users, devices, operating systems, services and processes, and user network behavior patterns across the organization.
“We observed Cisco Next-Generation IPS was setting a new standard for advanced threat protection, integrating real-time contextual awareness, intelligent security automation, and unprecedented performance. We believed no other solution could offer the visibility, automation, flexibility and scalability to protect UST Global’s dynamic environments against everyday increasingly sophisticated threats.”

Sunil Kanchi, Chief Information Officer & Senior Vice President, UST-Global

The UST Global and Cisco partnership

UST Global compared several products in the market, and was looking for a solution with a great history. It wanted a solution with proven consistency of performance, ease of use, APIs, the ability to extend to other threat intelligence sources, and the ability to integrate with third-party products. Not to mention, good pricing and support as well.

The Company chose Cisco as its partner of choice having evaluated it on all these parameters.