



Forcepoint Defends Apollo Hospitals Against Cyberattacks While Protecting Sensitive Patient Data

Forcepoint Web Security and DLP help this leading Chennai, India healthcare provider keep users safe from malicious attacks and minimize the risk of sensitive patient data loss.

Cybercrime is increasing dramatically in a fast-changing threat landscape where malicious websites and hackers can wreak havoc on healthcare organizations, while compromised systems can lead to damaging downtimes. Moreover, stringent data protection laws require organizations to ensure privacy is protected. Patients from across the world depend on leading Indian healthcare provider Apollo Hospitals for exceptional care and, in the process, entrust it with highly sensitive data. In order to keep that personal information safe, Apollo Hospitals relies on Forcepoint Web Security and Data Loss Prevention solutions.

CUSTOMER PROFILE:

India's first corporate hospital and a pioneer of private healthcare in the country.

INDUSTRY:

Healthcare

HQ COUNTRY:

India

PRODUCTS:

- › Forcepoint Web Security
- › Forcepoint Data Loss Prevention (DLP)

The cybersecurity threat landscape is evolving very rapidly, with a steep rise in cybercrime in the last few years. Advanced threats, such as ransomware, propagated via malicious and compromised websites and botnets, can wreak havoc. This is especially true in healthcare—of all the sectors, it's the most targeted by hackers globally. A cyberattack can lead to system downtime, which can mean the difference between the life and death of a patient. In addition, threats such as malicious users or employee negligence can come from inside an organization.

Moreover, in the new digital age, there is rapid growth in the range and volume of patient data available in digital form. This data can help healthcare providers facilitate digital health services that can deliver more accessible, coordinated, and personalized care. However, along with advantages come risks. Sensitive patient data needs to be protected and shared in a safe way in compliance with local laws.

As a foremost healthcare institution in the country, Chennai, India-based Apollo Hospitals was uniquely positioned to take on these challenges. The organization has long been a leader in clinical excellence, affordable costs, modern technology and forward-looking research and academics. It is among the first hospitals to leverage technology to facilitate seamless healthcare delivery and has earned multiple awards for its infrastructure, technology and services, including the 2019 Healthcare Transformation Leader's Award and the CHiME Most Wired Level 8 achievement in 2020.

"We have had a long-term and trusted relationship with Forcepoint. "

NUTAN MOHANTY, IT HEAD, APOLLO HOSPITALS

Because of its focus on looking ahead, the healthcare provider was quick to realize that its security posture needed to be aligned with the changing world of threat vectors, and at the same time, it needed to allay any concerns about data privacy and ensure compliance with stringent regulatory requirements.

"The evolution of the worldwide web has meant that the medium has become increasingly complex and thus digital risks have increased. Cyberattacks have become more frequent and sophisticated and their impact can be debilitating. Unfortunately, such attacks can result in severe consequences for patients," said Nutan Mohanty, IT Head, Apollo Hospitals. "We were looking for more advanced security tools that could protect our users from bad actors and malicious websites. We also needed solutions that minimize the risk of patient data loss and do all of this in a simple and easy-to-use platform."

Protecting against cyberattacks and preventing data loss with next generation solutions

Luckily, when it came time to expand their cybersecurity protections, Apollo Hospitals already had an established cybersecurity partner in Forcepoint. The hospitals had utilized Forcepoint for years and were happy with the solutions.

Still, Apollo Hospitals wanted to be sure it was making the right choice and assessed the top security vendors and tools in the market before choosing to upgrade to the latest version of Forcepoint Web Security and add Data Loss Prevention (DLP). The healthcare provider's focus was on integrated solutions that would not only protect against malicious sites but also address security risks when users work offsite. The choice was guided by several factors, including Forcepoint's ease of integration and access, exceptional security effectiveness and web and data loss protection through a single sign-on system. The updated version of web security protection provides new features such as shadow IT visibility and control for unknown attacks and zero-day protection.



Challenges

Protect users from cyberattacks and prevent risk of data leakage.



Approach

Implement Forcepoint Web Security and Forcepoint DLP.



"It's no wonder that we didn't think twice before making Forcepoint our preferred partner for cybersecurity. It was natural to extend our protection with the latest offerings from the same suite, and Forcepoint Web Security and Forcepoint DLP work very well together," Mohanty said.

Gaining complete visibility over confidential and sensitive patient data

For a robust security posture, complete visibility is needed not only into data at rest but also data in motion. Forcepoint solutions protect Apollo's users against advanced threats, insider threats and data theft. The easy-to-use tools detect and defend sensitive patient data in real time. They also identify the location of critical and sensitive data as well as keep track of its movement. Therefore, there is now complete visibility across users and endpoints, providing a cohesive defense against malicious sites, risky user behavior, and advanced threats. The solutions cover endpoints such as desktops, printers, applications and servers.

"By investing in Forcepoint's solutions, we now have complete visibility into data location and movement. We can also stop the unusual transfer of data," Mohanty said.

According to Mohanty, Forcepoint stood out for its offerings. He pointed out several features that cemented the ongoing relationship and tilted the balance in favor of moving forward with the next generation of Forcepoint solutions:

- Enhanced protection from malicious websites and cyber-attacks
- Improved web security and complete visibility of data movement
- Enabled single sign-on
- Compliance with data protection regulations

The future of Apollo Hospitals looks secure with Forcepoint

Apollo Hospitals is now prepared to address any new threats that develop in the cybersecurity landscape—whether inside or outside the organization. The provider has also been able to allay any concerns about patient data privacy and compliance with local and state regulations. With the help of advanced Forcepoint Web Security and Forcepoint DLP, Apollo Hospitals has taken the next step to becoming a cyber-resilient and regulatory-compliant organization.

"The best part is that Forcepoint has helped us tremendously with charting a roadmap for our cybersecurity strategy," Mohanty said.



Results

- › Enhanced web security against cyberattacks.
- › Enabled single sign-on.
- › Data protection compliance.



"The best part is that Forcepoint has helped us tremendously with charting a roadmap for our cybersecurity strategy."

NUTAN MOHANTY, IT HEAD