SUCCESS STORY / HEALTHCARE

ALYN Protects Hospital Networks from Browser-borne Threats with Ericom Shield Remote Browser Isolation (RBI)

Ericom Shield insulates ALYN endpoints and network from browser- borne ransomware and malware that can slip past defensive security solutions

Customer profile

ALYN Hospital Pediatric and Adolescent Rehabilitation Center

Product

Ericom Shield®

Industry

Healthcare

Background

ALYN Hospital is one of the world's leading facilities for active and intensive rehabilitation of children with physical, respiratory and developmental disabilities. The hospital provides inpatient and outpatient rehabilitation services through a wide range of multidisciplinary clinics and support programs. As a highly specialized tertiary care center, ALYN treats children from a wide geographic area.

Technology in the Service of Rehabilitation

ALYN's medical teams and therapists are experts at leveraging technology to maximize patients' capabilities, social integration and overall well-being. In keeping with this collaborative, technology-forward approach, all medical records are digital; medical staff and therapists use web-based resources extensively; patient teams collaborate with primary medical teams, families and teachers in remote locations via web technologies; and centralized systems enable staff to access patient data from any device or location.

"ALYN professionals closely coordinate at every step with patients' primary physicians and therapists, so sharing patient data with third parties is essential," explained Dr. Maurit Beeri, Director General of ALYN. "Our physiotherapists, occupational therapists, speech therapists, psychologists, social workers, nurses and doctors use the Web constantly, for research, to access resources for patients, and to update patients' families, teachers and local medical teams."

ALYN's small, but highly skilled and dedicated IT team is completing deployment of an entirely new hospital system that integrates highly advanced web infrastructure – cluster and data duplication, disaster recovery, application firewalls, NAC protection, endpoint protection and malware detection, WAF, and email traffic protection and sanitization.

Security First

Technology contributes immeasurably to patient care, but also places ALYN at risk of cyberattacks – risk that Uri Inbar, Director of IT, is adamant to guard against: "ALYN Hospital has zero tolerance for malicious attacks that can cripple hospital systems, threaten patient wellbeing, and expose private information. It's crucial for us to have all relevant protective layers against cyberattacks and other disasters, well beyond those required for our ISO certification."

Wary of the unending cat-and-mouse games between hackers and "patchers," which too often allow room for zero-day threats and malware to sneak in under the radar, ALYN's IT department initially blacklisted large swathes of the Web, and set up isolated workstations which could be used to access Web-based content received from remote colleagues.

Challenge

- Secure ALYN networks from browser-borne threats
- Integrate smoothly and seamlessly with existing ALYN security ecosystem

The Convenience Conundrum

ALYN doctors, nurses and therapists literally wear running shoes to get through their days. With a patient population of children who are seriously ill or disabled, caregivers have no time – and less patience -- to struggle with inconvenient security barriers.

"We need a solution that works seamlessly for every member of our staff, on every device and every operating system they might use, from wherever they are, with absolutely no hassle," explained Inbar.

ALYN needed a secure browsing solution that would protect against browser-borne threats, while providing a completely natural, high quality Internet browsing experience.

The Solution

> *"Web isolation and file sanitization were the final missing pieces of our defense-in-depth puzzle.We were searching for a solution that would integrate smoothly and seamlessly with existing ALYN security solutions, support group-based policy definition for users and domains, and be centrally managed. Ericom Shield ticked all those boxes, and is pre-integrated with Votiro file sanitization."*
>
> **Uri Inbar,**
> Director of IT

Based on a detectionless, patch-free approach to secure browsing, Ericom Shield brings a powerful layer of protection to ALYN's existing cybersecurity portfolio. It dramatically reduces the risk of malware infiltrating ALYN endpoints and network via browser-executable code that can slip past defensive cybersecurity solutions. The solution is transparent to ALYN users, who use the Internet as usual, on any device and browser they choose, in every treatment room, with almost no degradation in performance.

While users experience websites naturally, on their device browsers, each browsing sessions is actually executed on a remote virtual browser that is isolated in a disposable container, located in a remote "safe zone" of the ALYN network DMZ. Far from the endpoint device, the session is rendered in real time and streamed to the user's local browser. A new container is allocated for every remote browsing session and tab, and discarded once that session or tab is closed to prevent accidental leakage.

Browser-executable code, including malware, never reaches the endpoint, yet the user browsing experience is completely secure and totally seamless. In addition, ALYN's IT staff have consistent, centrally managed control over file download and upload permissions based on Active Directory users and groups, while ensuring that downloaded files are automatically cleansed before use.

Ease of use is important not only for the medical staff: With over 200 fixed stations and 50 mobile devices – many of which reside in the 380 users' pockets -- IT administrators needed a centrally managed solution that would be quick to set up and easy to manage. Ericom Shield requires no endpoint installation and is compatible with all devices and operating systems.

Within less than two hours, Ericom Shield was fully integrated with ALYN's existing security frameworks, including anti-virus solution, endpoint security, firewall, URL filtering and file sanitization solutions. As a centrally managed, client-based solution, Ericom Shield inherited existing ALYN organizational policies and Active Directory settings, and no installation was needed on user devices, enabling full testing and roll-out to be completed in weeks.

Results

- Secured ALYN endpoints and networks from browser- borne malware, ransomware and other browser-borne threats
- Empowered physicians, therapists and administrative staff to browse, leverage Internet resources, and download external files seamlessly and safely, for therapy, research, communication and consultation with families and primary medical teams
- Minimized IT overhead related to secure browsing via clientless installation, quick integration with existing solutions, and centralized, policy-based management of individuals and groups

The Impact

"Ericom Shield is crucial for our work at ALYN," said Dr. Maurit Beeri, Director General of ALYN. "The ability to access any site from any computer or tablet, and download any file without putting our network at risk, increases staff productivity and allows us to provide the best care for our patients."

> *"With Ericom Shield, we feel much more confident with users accessing the black pit that the web is today, since we know that every bit of code is executed only remote from our endpoint is executed only remote from our endpoint and networks, and cleared even from there within minutes."*
>
> **Uri Inbar,**
> Director of IT

Conclusion

As a premier rehabilitation hospital for children, ALYN depends on the most advanced technology to maximize the potential and well-being of the kids in their care. Ericom is proud to provide equally cutting-edge technology to enable the professionals who do this outstanding work to securely and easily leverage the digital resources they need to get the job done.

About Ericom Software www.ericom.com

Ericom Software provides businesses with secure access to the web and corporate applications, in the cloud and on-premises, from any device or location. Leveraging innovative isolation capabilities and multiple secure access technologies, Ericom's solutions ensure that devices and applications are protected from cybersecurity threats, and users can connect to only the specific resources they are authorized to access.

Americas:
T +1 (201)767-2210
E-mail: info@ericom.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: ukinfo@ericom.com

Worldwide:
T +972-2-591-1700
E-mail: info@ericom.com

Follow us