SANGFOR | Sangfor Athena MDR

Sangfor Athena

Managed Detection Response (MDR) for Educational Institutions

Preserving Education’s Mission in a World of Rising Cyber Threats

Preserving Education’s Mission in a World of Rising Cyber Threats

In 2025, educational institutions globally face an unprecedented escalation in cyber threats. According to 2025 research, the education sector leads all industries in being targeted, averaging 4,388 cyberattacks per organization per week in Q2 2025, a 31% year-over-year increase[1]. Meanwhile, seasonal spikes such as the “back-to-school” period have seen overall attacks per educational organization jump to 4,356 per week, marking a 41% YoY increase[2]. On the other hand, APAC’s education sector recorded the highest average weekly attacks of 7,869 per week in the first half of 2025[2].

These numbers reflect more than just growing threat volume; they expose critical gaps in the education sector’s security posture. Schools, colleges, and universities hold large volumes of sensitive data (student records, faculty information, research, etc.), yet often operate under constrained cybersecurity budgets, limited staff, and stretched infrastructure. As connectivity, cloud use, and remote/hybrid models become more prevalent, attack surfaces multiply, and traditional defenses like firewalls and simple endpoint protections are no longer enough.

This brochure presents a business case for why **Managed Detection & Response (MDR)** services are not merely optional but essential for educational institutions. We examine how MDR addresses the security challenges faced by schools, colleges, and universities by providing comprehensive and effective cybersecurity controls to detect threats, reduce downtime, and meet compliance and stakeholder demands. We also outline the quantifiable benefits for institutions and show how MDR delivers these outcomes in a cost-effective way.

By the end of this brochure, it should be clear: to protect learners, maintain educational activities, and build operational trust, MDR is a strategic shield that education can no longer afford to do without.

The Impact of Cyberattacks on Educational Institutions with Real-World Examples

According to a Bitsight TRACE study, the education sector was ranked as the top industry targeted by Known Exploited Vulnerabilities (KEV), representing 54.3% of all recorded cases[3]. Beyond statistics, the consequences of these intrusions run deep, disrupting not only IT systems but the very mission of education: enabling uninterrupted learning and safeguarding the trust of students, parents, and faculty.

When educational institutions are compromised or repeatedly targeted, the impacts can be seen across various critical dimensions:

1 Disruption of Learning Continuity

Ransomware and web attacks (e.g., defacement or compromise) can disable online learning platforms, examination systems, and classroom technologies. Extended downtime then translates into missed learning hours, delayed examinations, and disrupted academic calendars.

Example: Maastricht University (Netherlands, 2019)

*Source: Shutterstock

On 23–24 December 2019, Maastricht University was hit by a major Clop ransomware attack that encrypted 267 Windows servers, encrypting critical systems (including email and file servers)[4]. The university took nearly all systems offline on 24 December to contain the breach, leaving students unable to access learning materials or prepare for upcoming assessments. Teaching was suspended, exam schedules had to be reworked, and a special leniency arrangement was created for students whose preparation time had been disrupted. Although major services resumed by 6 January, the outage caused significant disruption to learning and academic planning[5].

2 Exposure of Sensitive Data

Schools and universities hold large volumes of valuable data, from sensitive personal information to research and intellectual property, which makes them attractive targets for cybercriminals.

Personal Information: Personal information held by higher education institutions includes financial information, personal identifiers, and even medical records. This data can be exploited for identity theft, fraud, and traded on the dark web. Private and independent schools are especially appealing because parental payment records can include full banking information. Compromised data belonging to young adults is particularly valuable because it can be reused over longer time horizons, including for future social-engineering attacks (e.g., impersonation scam calls using valid personal details).

Example: University of Siena (Italy, 2024)

*Source: Shutterstock

In early May 2024, the University of Siena was hit by a ransomware attack attributed to the LockBit 3.0 cyber-criminal group, which targeted the university's virtualization infrastructure. According to the university's official data breach notices, the incident led to unauthorized access and exfiltration of about 500 GB of data from its virtualized systems[6].

The university later confirmed that the compromised dataset included personal data on staff, students, and other stakeholders, such as contact details, login credentials, identity documents, bank and payment details, income and salary information, health and disability data, scans of handwritten signatures, and detailed student-career or professional-career training records[7]. The LockBit 3.0 gang publicized the attack on its dark-web data-leak site, posting sample images of stolen documents and announcing that the full dataset would be made available there at a specific date and time[8]. In its communications to affected individuals, the university warned that this exposure could lead to identity theft, financial fraud, and other misuse of personal data. It urged students and staff to be extremely cautious about unsolicited requests for payments or personal information[6].

Research & Intellectual Property: Beyond personal records, universities also produce research and intellectual property that carry commercial and geopolitical value. State-sponsored or organized cybercrime groups actively target these research assets to gain economic, military, or strategic advantage or to hold them as leverage in ransomware campaigns, directly threatening institutional competitiveness and national interests.

Example: Oxford University (UK, 2021)

*Source: Shutterstock

In February 2021, Oxford University's Division of Structural Biology ("Strubi"), which was conducting COVID-19–related research, was infiltrated by attackers who gained access to internal laboratory systems. Screenshots shared by the intruders showed they could access and manipulate lab equipment. Investigators believed the attackers were financially motivated and attempting to sell stolen research data on underground markets9. The Government warned that hostile actors were "95%" likely trying to hack vaccine research10. Oxford contained the breach before clinical trial data was taken, but the attack exemplifies how universities at the cutting edge of research are targeted for valuable intellectual property.

3 Financial and Operational Strain

Beyond the direct costs of ransom payments, data theft, and remediation, cyber incidents impose significant indirect costs through downtime that disrupts teaching, research, and administrative processes. Institutions also frequently incur unbudgeted spending on legal counsel, regulatory fines, and urgent security upgrades.

Example: Lincoln College (USA, 2021)

*Source: Wikipedia

A small Illinois college (157 years old) became the first U.S. college to shut down permanently after a ransomware attack. Already strained by COVID-19, the college was hit in late 2021 by ransomware that paralyzed admissions, retention systems, and fundraising data for months[11]. Even after paying a ransom (reportedly under $100k), the prolonged downtime meant the college couldn't recover enrollment and finances in time – it announced closure in May 2022. This dramatic case shows how a cyberattack's operational disruption and recovery costs can push an institution over the financial brink.

4 Reputational Damage and Loss of Confidence

Trust is foundational in education, and a major breach places that trust at risk. When stakeholders perceive that an institution cannot protect its data, reputational damage can quickly follow among students, parents, donors, and industry partners. Loss of confidence can reduce admissions demand, limit funding opportunities, and erode long-term standing.

Example: Western New Mexico University (USA, 2025)

*Source: Shutterstock

In April 2025, Western New Mexico University (WNMU) experienced a cyberattack that temporarily shut down key online services and disrupted operations for nearly two weeks. During a Board of Regents meeting on September 11, 2025, the university reported that Fall 2025 enrollment dropped by about 10%—roughly 365 fewer students—resulting in an estimated $3.3 million reduction in annual revenue[12]. The university stated that this decline was largely due to the cyberattack, highlighting the financial consequences tied directly to reputational and operational damage from a breach.

5 Regulatory and Compliance Risks

Many education systems in Europe and the United States, including private schools, must comply with data-protection laws such as the GDPR, the Higher Education Act, FERPA, and internal audit requirements or local equivalents. Non-compliance resulting from a breach can lead to penalties, loss of accreditation, and reduced public funding — particularly for private institutions.

Example: GeniusU EdTech (Singapore, 2022)

*Source: GeniusU

In Singapore, where the Personal Data Protection Act (PDPA) applies to private education entities, the company GeniusU (an education platform) was fined S$35,000 in 2022 for a breach exposing the personal data of approximately 1.26 million users[13]. The breach occurred after a developer accidentally exposed access credentials on a public GitHub repository, allowing an attacker to use those keys to enter GeniusU's cloud environment and retrieve a staging-database copy containing user information. The attacker accessed and exfiltrated names, email addresses, location details, and last-sign-in IPs. The PDPC ruled that GeniusU had failed to implement reasonable security measures, particularly around credential management and protection of replicated production data, and imposed a financial penalty along with required remediation steps[13].

Education Sector Threat Landscape in Numbers

- ✓ The education sector experienced an average of 4,356 cyberattacks per organization per week in H1 2025 — a 41% year-on-year increase[1].
- ✓ APAC was the hardest-hit region, with education organizations seeing an average of 7,869 weekly attacks in H1 2025[2].
- ✓ USD $3.8 million is the average total cost of a data breach in the education sector over the past 12 months[14].
- ✓ In 2024, ransomware attacks successfully encrypted data in 77% of higher-education incidents and 85% of lower-education (K–12) incidents[15].
- ✓ The education sector spends an average of 7% of its IT budget on cybersecurity — below the industry average of 8%[16].

Understanding the Challenges Behind the Numbers

The education sector’s vulnerable security posture can be summarized into two core factors: a large and expanding attack surface and budget and resource constraints.

01. Large Attack Surface

Expanding Digital Footprint:

The education sector’s digital footprint has expanded rapidly. Online learning platforms, collaboration tools, cloud services, and remote access have enhanced the learning experience and flexibility. However, they’ve also created a fast-growing, interconnected web of accounts, apps, and integrations. This expansion multiplies the number of entry points that attackers can exploit.

Unmanaged Devices:

The attack surface is enlarged with unmanaged personal laptops, phones, and home networks accessing campus systems. Because these devices aren’t institution-managed, they often lack consistent controls and create blind spots for security teams, where one compromised device can enable lateral movement. Given limited resources, fully securing this fragmented environment is unrealistic for most institutions.

Human-layer Exposure:

The human layer adds to the risk. Education runs in a highly collaborative environment where staff and students routinely share files and click links from known contacts. That convenience-first culture lowers suspicion and gives phishing and credential theft reliable delivery paths.

Net effect

> **“ Education has a broad, fast-changing, and hard-to-govern attack surface.**

02. Budget and Resource Gaps

Educational institutions typically operate with tight cybersecurity budgets — in some cases cybersecurity receives **<1% of IT spend**[17]. This has two direct consequences:

① It limits the ability to hire qualified cybersecurity personnel. The World Economic Forum's Global Cybersecurity Outlook 2025 report also recognizes that educational institutions are disproportionately affected by the shortage of cybersecurity professionals.

② It restricts the ability to refresh aging technology fast enough to keep pace with modern threats.

On the technology side, there are two kinds of legacy at play, each with a different risk:

- **Legacy Security Technology:**

  Older firewalls without full WAF capability, legacy email gateways and IAM, limited endpoint telemetry, etc. When security controls are outdated, successful exploitation becomes more likely because threats aren't blocked or detected in time. Microsoft's Cyber Signals Issue 8 highlights this as a key driver behind recent ransomware and phishing success in schools[18].

- **Legacy Educational/Administrative Systems:**

  Legacy SIS/ERP, older attendance and grading platforms, and unpatched file servers often contain exploitable vulnerabilities that increase breach impact and enable longer attacker persistence.

Net effect

> **Institutions lack the resources, people, and replacement capacity to continuously manage and correct a widening attack surface.**

Preserving Education’s Mission with Sangfor Athena MDR

Evident from the above, the education sector has become one of the most attractive targets for cybercriminals for various reasons and loopholes. With vast amounts of sensitive and high-value data spread across increasingly complex digital environments, universities and schools face mounting risks from ransomware, data breaches, and disruptive attacks.

At the same time, budget constraints, legacy systems, and limited cybersecurity expertise leave institutions struggling to establish effective defenses, aside from basic security tools and processes.

This is where **Sangfor Athena MDR** (Managed Detection and Response) makes a difference. By combining advanced security technology with expert human oversight, Athena MDR delivers purpose-built protection for education. We monitor, detect, and stop threats before they disrupt learning, ensuring sensitive data stays safe and institutions remain resilient.

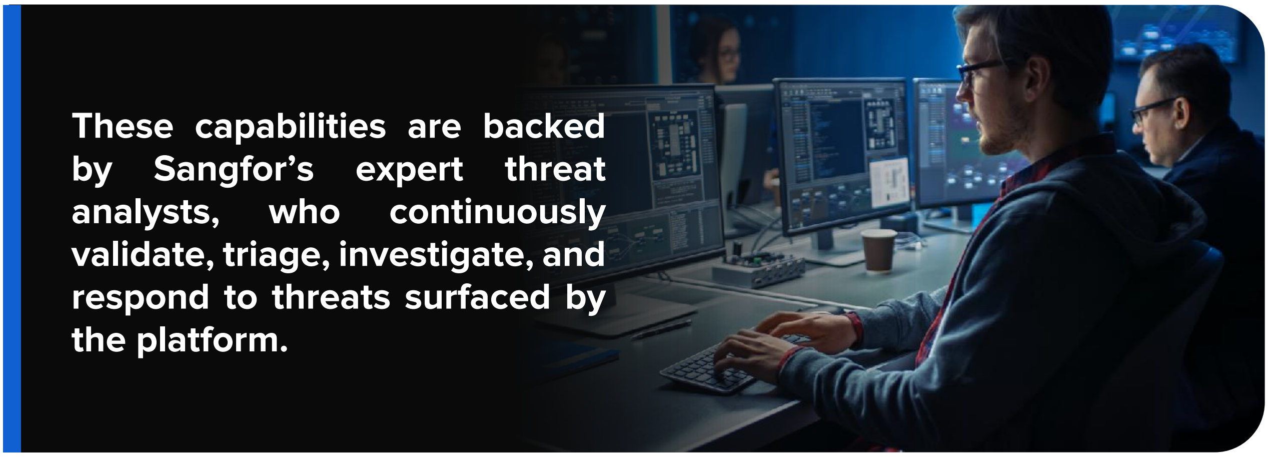
With Athena MDR, schools, colleges, and universities don’t need to become cybersecurity experts themselves — they can focus on what matters most: enabling students to learn, grow, and succeed in a secure digital environment.

How Athena MDR Addresses Education's Cybersecurity Challenges

Sangfor Athena MDR resolves the security operation challenges outlined above by combining advanced technology with 24/7/365 human expertise. It supports educational institutions' security without requiring additional cybersecurity headcount or capital expenditure.

1 Managing the Expanding Attack Surface

- **Covers the Large Digital Footprint:** Sangfor's MDR platform is powered by proprietary XDR technology that ingests telemetry from every major surface — network, endpoint, cloud, and email — and unifies that data into a single correlation engine. Sangfor also provides the native components/sensors required to collect this telemetry, including Athena NGFW, Athena EPP, and STA network sensor, ensuring rich first-party data capture. By aggregating these multi-layer signals into one detection fabric, the MDR platform can connect malicious activity across the environment that would otherwise appear unrelated when viewed independently. Detection accuracy is further enhanced by Sangfor's GenAI security suite, Security GPT, which provides high-fidelity correlation analysis with low false positives.

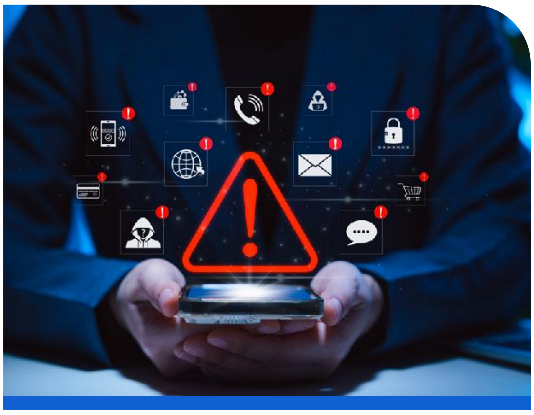


These capabilities are backed by Sangfor's expert threat analysts, who continuously validate, triage, investigate, and respond to threats surfaced by the platform.

This unified telemetry + AI correlation architecture, reinforced by Sangfor's native sensors, expert human confirmation, and continuous operations, collapses the digital landscape into one governed detection plane, negating the risks and challenges of an expanding attack surface.

- **Protects Against Unmanaged Device Threats:** Even without agents on personal or untrusted devices, the MDR platform analyzes network telemetry to detect suspicious activity like lateral movement attempts that could compromise your core assets. It operates continuously, even during non-working hours, and can remotely contain impacted endpoints before threats spread across the environment. This ensures that core IT assets are proactively and consistently protected by an MDR team from risks introduced by unmanaged devices, especially in environments with low access controls that allow BYOD devices to coexist on the same network as core IT servers and staff workstations.

- **Counters Low Security Awareness:** The MDR platform integrates Sangfor Anti-Phishing GPT, which uses GenAI to detect and intercept stealthy phishing, including spoofed messages from trusted contacts. It sends users notifications to warn them of potential phishing attempts and blocks malicious links and attachments, even if a user interacts with them. This counteracts the risks created by attackers exploiting education's highly collaborative sharing culture while reducing reliance on individual user vigilance as a control.



- **Protects Vulnerable Educational Systems:** During service onboarding, the MDR team identifies the most critical and vulnerable systems with the highest exposure, and then prioritizes monitoring and detection on those assets. Athena MDR experts focus on spotting abnormal activity and behavioral indicators associated with vulnerability exploitation on these older systems, ensuring that attacks targeting legacy platforms are surfaced and responded to quickly.

2 Addressing Limited Budgets and Resources

- **Reduces TCO:** By consolidating advanced technology, human expertise, and mature processes into one managed service, institutions get comprehensive protection at a fraction of the cost of building an in-house SOC, with savings of **up to 80% per year**. From a different perspective, the MDR service is 10 times more cost-effective compared to the high capital and operational costs of building an internal SOC, according to **Sangfor's MDR TCO Calculator** (based on protecting 50 servers and 200 non-server assets).

- **Maximizes ROI:** By preventing a single major breach, Athena MDR provides a clear return on investment by protecting revenue and ensuring business continuity. The service costs only a small fraction compared to the alarming average USD 3.8 million in cyberattack damage and penalties on educational establishments. Sangfor's MDR TCO Calculator further shows that, **for every $1 spent** on the MDR service, academic institutions can potentially **avoid $127 in breach-related costs.**

- **Replaces Outdated Security Technologies:** Athena MDR offers cost-competitive bundles that include first-party security components and sensors, including Athena EPP (Endpoint Protection Platform) and the Athena STA sensor. These allow institutions to replace legacy security technologies without breaking the bank while maximizing the value of the MDR service.

For schools, colleges, and universities, the value of Athena MDR is clear

01 **Always-on protection** that prevents learning from being interrupted by ransomware or system downtime.

02 **Compliance-ready security** aligned with regulatory expectations and industry standards.

03 **Safeguarding sensitive data** such as student records, personal identifiers, and financial details from theft or misuse.

04 **Cost efficiency** through a service model that delivers enterprise-grade protection at a fraction of building it in-house.

05 **Ensures Academic Continuity:** With cybercriminals aware of education's budget constraints, Athena MDR ensures schools can continue teaching and research without being forced into costly ransom payouts or prolonged downtime, thanks to our continuous monitoring and fast resolution process – all with minimal involvement of your own IT team.

Athena MDR empowers education providers to focus on their core mission — teaching and innovation — with the confidence that their digital environment is continuously monitored, defended, and resilient against evolving cyber threats.

Athena MDR Service Scope

Sangfor Athena MDR uses proprietary technology to collect only essential security-related data, minimizing exposure to sensitive information. We offer flexible options to tailor the service to your needs, avoiding unnecessary technology costs.

Technology Component Options

Sangfor Athena NGFW	Sangfor Athena STA Sensor	Sangfor Athena NDR
Sangfor Athena EPP	Sangfor Athena XDR	Third-party Tools

For additional details or customization requests, please contact us to discuss how Athena MDR can be tailored to meet your educational institution's unique security requirements.

Athena MDR Services Key Differentiators

1 **Rapid Onboarding:**

Establishes effective security operations in less than 1 month.

2 **Context-relevant Service:**

Ensures service delivery tailored to your environment and pain points.

3 **Human + Machine Intelligence:**

Combines technology efficiency and human instinct and experience to enhance efficiency and accuracy.

4 **Dedicated Service Manager:**

Assigns each customer with a go-to security expert to help them stay ahead of threats and introduce a level of familiarity to enhance service experience.

5 **Threat Intelligence Advisory:**

Helps you make sense of threat intelligence relevant to your environment.

Contact Us Now

to explore how else Sangfor Athena MDR addresses your challenges and requirements to keep your organization safe from cyber threats and attacks at all times.

☎ ✉ 🌐

Sources

1. https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/

2. https://blog.checkpoint.com/research/cyber-attacks-surge-against-education-sector-ahead-of-back-to-school-season/

3. https://www.bitsight.com/sites/default/files/2024-04/bitsight-a-global-view-of-cisa-kev-catalog.pdf

4. https://www.maastrichtuniversity.nl/file/reponseofmaastrichtuniversitytofox-itreportpdf

5. https://www.maastrichtuniversity.nl/cyberaanval-een-overzicht

6. https://www.unisi.it/unisilife/notizie/sample-communication-interested-parties

7. https://www.unisi.it/unisilife/notizie/further-sample-communication-interested-parties

8. https://www.ransomware.live/id/dW5pc2kuaXRAbG9ja2JpdDM%3D

9. https://www.theverge.com/2021/2/25/22301725/covid-19-research-lab-hacked-oxford-university-strubi

10. https://www.gov.uk/government/news/uk-condemns-russian-intelligence-services-over-vaccine-cyber-attacks

11. https://lincolncollege.edu/home

12. https://entertainment.wnmu.edu/wnmu-regents-meet-hear-updates-on-presidential-search/

13. https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/commissions-decisions/decision---geniusu-pte-ltd--180122.pdf

14. https://www.huntress.com/blog/average-cost-of-a-data-breach

15. https://news.sophos.com/en-us/2024/07/11/the-state-of-ransomware-in-education-2024/

16. https://ma.moodys.com/rs/961-KCJ-308/images/Higher%20Education%20Cyber%20Report.pdf

17. https://www.cisecurity.org/insights/blog/report-k12-orgs-concerned-about-security-budget-threats

18. https://www.microsoft.com/en-us/security/blog/2024/10/10/cyber-signals-issue-8-education-under-siege-how-cybercriminals-target-our-schools/

SANGFOR

INTERNATIONAL OFFICES

SANGFOR SINGAPORE

380 Jln Besar,
#08-04/05 ARC 380, Singapore 209000
Tel: (+65) 6276-9133

SANGFOR HONG KONG (CHINA)

Unit 1612-16, 16/F, The Metropolis Tower,
10 Metropolis Drive, Hung Hom, Kowloon, Hong Kong
Tel: (+852) 3845-5410

SANGFOR INDONESIA

Atrium Mulia 3rd Floor, Jl. H.R. Rasuna Said Kav.
B 10-11 Kuningan, Setia Budi, Kecamatan Setiabudi, Kota Jakarta
Selatan, Daerah Khusus Ibukota Jakarta 12910, Indonesia
Tel: (+62) 21-2168-4132

SANGFOR MALAYSIA

Suite 11.01 & 11.02 , Level 11 of Centrepoint North, Mid Valley City,
Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3645

SANGFOR THAILAND

141 Major Tower Thonglor (Thonglor10) Floor 11 Sukhumvit Road,
Kholngtan Nuea Wattana BKK, Thailand 10110
Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES

Unit 14B 14th Floor, Rufino Pacific Tower, 6784 Ayala Avenue,
Makati City, Philippines
Tel: (+63) 9688998920

SANGFOR VIETNAM

Unit 11.01 MB Sunny Tower, 259 Tran Hung Dao Street,
Co Giang Ward, District 1, Ho Chi Minh City, Vietnam
Tel: (+84) 903-631-488

SANGFOR SOUTH KOREA

305, 76, Yeonmujang-gil, Seongdong-gu,
Seoul, Republic of Korea.

SANGFOR UAE

Office #718, Publishing Pavilion, Production City, Dubai, UAE
Tel: (+971) 52855-2520

SANGFOR PAKISTAN

Office No.210, 2nd Floor, "The Forum",
Plot No. G-20, Block 9, Khayaban-e-Jami, Clifton, Karachi, Pakistan
South Region: (+92) 321 2373991
North Region: (+92) 304 5170714
Central Region: (+92) 314 519 8386

SANGFOR ITALY

Sede Principale: Via Marsala 36B, 21013, Gallarate (VA)
Sede a Roma: Via del Serafico, 89-91, 00142 Roma RM
Tel: (+39) 0331-6487-73

SANGFOR TÜRKIYE

A Blok. Kat 51. D 643, Atatürk Mh, Ertuğrul Gazi Sk,
Metropol İstanbul Sitesi. 34758 Ataşehir/İstanbul
Tel: (+90) 216-5156969

SANGFOR LATAM OFFICE

Torre Onyx Segundo Piso, Av. Río San Joaquin 406, Amp Granada,
Miguel Hidalgo, C.P. 11529, Ciudad de México, CDMX.

SANGFOR SAUDI ARABIA OFFICE

Office 505, Al Dhabab Complex 5th Floor, 6347 Anas Ibn Aous,
Al Murabba, Riyadh.

AVAILABLE SOLUTIONS

Cybersecurity

Athena NGFW - Next Generation Firewall
Smarter AI-Powered Perimeter Defense

Athena EPP - Endpoint Protection Platform
The Future of Endpoint Security

Athena SWG - Secure Web Gateway
Secure User Internet Access Behaviour

Athena NDR - Network Detection and Response
Intelligent Detection and Response Platform

Athena XDR - Extended Detection and Response
The Best Fusion of SecOps and GenAI

Athena MDR - Managed Threat Detection & Response Service
The Cyber Guardian of Your Business

IR - Incident Response
Sangfor Incident Response – One Call Away

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

Athena SASE - Secure Access Service Edge
The Smarter, Simpler, and More Secure Way to Connect

SD-WAN
Boost Your Branch with Sangfor

Cloud Computing

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

VMware Alternative
The Ideal Platform to Streamline Your off-VMware Journey

aDesk - Virtual Desktop & Virtual App Solutions
Seamless Experience, Secure and Efficient

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com