Sun Systems
System Integrators

COMPANY PROFILE

Providing state-of-the-art technology solutions in association with Global IT leaders.

www.sunsystemonline.com

Navi Mumbai, Maharashtra

COMPANY OVERVIEW

Sun Systems was established in 2006 with a focus on providing state-of-the-art technology solutions in association with Global IT leaders. In over a decade of its operations, Sun Systems has been consistently providing world class IT solutions to a large number of SME, Corporates and Governments in India. Headquartered in Navi Mumbai, Sun Systems is providing is catering to clients across Maharashtra and neighboring states.

We constantly study the IT industry trends and keep an eye on solutions that fit market niches. We review the products strengths and market standing before introducing them to the market, carry out extensive product assessment and testing, prior to adding them to our portfolio. Our product selection is based on technical excellence, robustness and reliability and its ability to provide tangible business benefits and significant added value for our customers.

Sun Systems broad portfolio provides wide range of comprehensive information management solutions including Information Security, EDR, XDR, SIEM, SOC, SOAR, VAPT Analysis, Video Conferencing, Digital Learning along with IT Infrastructure and holistic technology consulting.

Mission

Improve the security of our customers' IT Setup, provide decision makers with expert advice in cyber compliance & deliver quality and unparalleled service with every engagement.

Vision

Sun Systems will be an acknowledged leader in information assurance and cyber security by delivering outstanding service and superior outcomes for our customers.

NEXT-GENERATION FIREWALL

A Next-Generation Firewall (NGFW) is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS). Next-generation firewalls integrate three key assets: Enterprise firewall capabilities, an intrusion prevention system (IPS) and application control.

Like the introduction of stateful inspection in first-generation firewalls, NGFWs bring additional context to the firewall's decision-making process by providing it with the ability to understand the details of the Web application traffic passing through it and taking action to block traffic that might exploit vulnerabilities.

SDWAN

SD-WAN (software-defined wide area network) is a type of networking technology that uses software-defined networking (SDN) principles to manage and optimize the performance of wide area networks (WANs). It enables organizations to securely connect users, applications and data across multiple locations while providing improved performance, reliability and scalability. SD-WAN is designed to solve the multiple challenges associated with traditional WAN, allowing networking professionals a simpler way to optimize and secure WAN connectivity.

ENDPOINT DETECTION AND RESPONSE

Endpoint detection and response, or EDR, is software designed to automatically protect an organization's end users, endpoint devices and IT assets against cyberthreats that get past antivirus software and other traditional endpoint security tools.

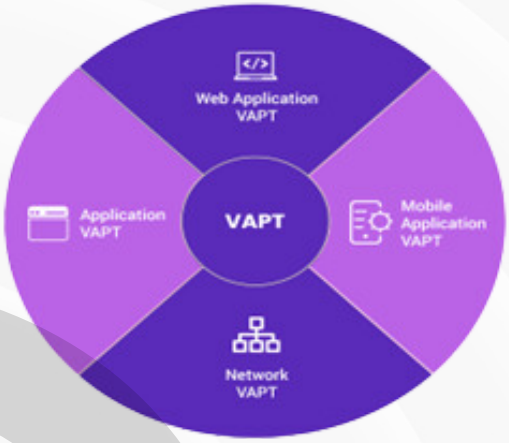
EDR collects data continuously from all endpoints on the network - desktop and laptop computers, servers, mobile devices, IoT (Internet of Things) devices and more. It analyzes this data in real time for evidence of known or suspected cyberthreats, and can respond automatically to prevent or minimize damage from threats it identifies.

EXTENDED DETECTION AND RESPONSE (XDR)

eXtended Detection and Response (XDR) collects threat data from previously siloed security tools across an organization's technology stack for easier and faster investigation, threat hunting, and response. An XDR platform can collect security telemetry from endpoints, cloud workloads, network email, and more.XDR connects data from siloed security solutions so they can work together to improve threat visibility and reduce the length of time required to identify and respond to an attack. XDR enables advanced forensic investigation and threat hunting capabilities across multiple domains from a single console.

IT SECURITY AUDIT

An IT security audit is a comprehensive assessment of an organization's security posture and IT infrastructure. Conducting an IT security audit helps organizations find and assess the vulnerabilities existing within their IT networks, connected devices, and applications. It gives you the opportunity to fix security loopholes and achieve compliance.
This includes things like vulnerability scans or conducting penetration tests to gain unauthorized access to the systems, applications, and networks. Finally, the penetration testing reports generated after performing all the necessary procedures are then submitted to the organization for further analysis and action.



SECURITY OPERATION CENTRE (SOC)

A security operations center (SOC) is an in-house or outsourced team of IT security professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible. An SOC also selects, operates, and maintains the organization's cybersecurity technologies, and continually analyzes threat data to find ways to improve the organization's security posture.The chief benefit of operating or outsourcing an SOC is that it unifies and coordinates an organization's security tools, practices, and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective and more cost-effective response to security threats

SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)

Security orchestration, automation and response, or SOAR, is a stack of compatible software programs that enables an organization to collect data about security threats and respond to security events with little or no human assistance. The goal of using a SOAR platform is to improve the efficiency of physical and digital security operations.
SOAR platforms have three main components: security orchestration, security automation and security response.

- SECURITY ORCHESTRATION connects and integrates disparate internal and external tools via built-in or custom integrations and application programming interfaces.
- SECURITY RESPONSE offers a single view for analysts into the planning, managing, monitoring and reporting of actions carried out after a threat is detected.
- SECURITY AUTOMATION, fed by the data and alerts collected from security orchestration, ingests and analyzes data and creates repeated, automated processes to replace manual processes.

EMAIL SECURITY

Electronic mail has become completely ingrained into the way our communities and companies communicate in the 21st century. Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise. Email is a popular medium for the spread of malware, spam, and phishing recipients to divulge sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. Email is also a common entry vector for attackers looking to gain a foothold in an enterprise network and breach valuable company data.

VIDEO CONFERENCE

Video conferencing is a technology that allows users in different locations to hold real-time face-to-face meetings, often at little to no cost. There are many ways to utilize video conferencing technology, such as company meetings, job training sessions, or addressing board members.Video conferencing saw a huge boost amid the global COVID-19 pandemic. The stability and quality of the video conference may fluctuate with the speed and reliability of the data connection

DIGITAL CLASSROOMS

A digital classroom refers to a classroom that is fully immersed in technology. These classrooms rely on educational apps and websites to enhance student learning. Feedback loops and technology are also important parts of a digital classroom. Feedback loops in a digital class ensure that students receive input from their professors in a timely manner. Professors can also customize their feedback based on student, lesson, group and more. Technology is the most visible part of this type of classroom and encompass hardware, software, operating systems and social media channels.

OUR TECHNOLOGY PARTNERS

Canon · Lenovo · Quick Heal Security Simplified · cisco · Hewlett Packard Enterprise

TREND MICRO · DELL · Microsoft · hp · paloalto NETWORKS

FORTINET · EPSON · SONICWALL · Synology

OUR CLIENTS

> Our growth has been based on maintaining relationships with our clients across a broad range of industries.

CISF · CIDCO · Income Tax Department · FDA Maharashtra · Indian Railways · University of Pune

Bombay High Court · MMRDA · Indian Navy · BARC · Indian Air Force

State Bank of India · GP Parsik Bank · CFS Camlin Fine Sciences · SHRIRAM Group

HAL · Air India · India Post · AIR · Symbiosis International University

16 +

Year’s Experience

25+

Industries Served

300+

Happy clients

Sun Systems
System Integrators

Sun Systems

#202, Building-3, Sector-3, Millennium Business Park, Mahape, Navi Mumbai Maharashtra, India.

022 4127 9731 / 90046 07067

sales@sunsystemonline.com

www.sunsystemonline.com

Follow us on :