DATASHEET

SorbSecurity

AI-powered Behavior Analysis

Cloud Security Solution Partner

SORBSECURITY

Sorb Cloud

- 99.999% service availability
- 99% blocked SPAM
- 100% known virus protection
- 100% Phishing protection
- 100% APT protection via Document payload

SorbSecurity Cloud Email Security Features

- Dynamic classification and control of emails
- Multi-layer threat protection
- Flexible policy and content filter
- Detailed reporting
- Scalable to support even the largest organizations
- Mail Archive

SorbSecurity Cloud Email Security Benefits

- Protection against not only SPAM and Virus and more Advanced attacks including Phishing, Malware and Advanced Persistent Threat
- Reduced administration overhead
- Quick and easy reports, searches, and investigations

Protect Organization from All Email Threats

SorbSecurity Cloud Email Security (the "**SCES**") helps you on securing and controlling both inbound and outbound email through an easy-to-use and easy-to-deploy cloud-based solution. With SCES, you can protect your staff, data and brand reputation from the modern threats includes but not limited to:

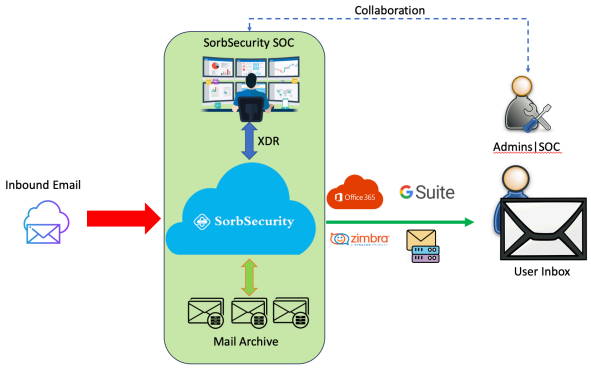
- SPAM
- Phishing
- Malware
- Ransomware

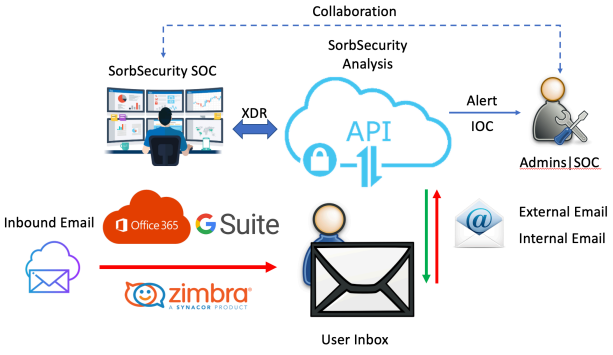
Next Generation Email Solution

SCES keeps your staff safe from all email threats. We are flexible to meet all complex environments to help our customers and partners. We support cloud, hybrid, and on-premises with all virtual infrastructure (Azure, Google Cloud, VMWare, KVM, AliCloud etc.) or physical appliance.

Threat Protection and Prevention

Effective threat protection starts with the efficient and accurate detection. SCES uses multiple layers of leading dynamic behavior driven analysis technology to detect challenging threats, including phishing and malware.





Email Firewall

Denial of Service (DoS) Protection

Protect your communication infrastructure. With DDoS Mail Protection, you protect your email exchanges with co-workers, customers, service providers, and suppliers.

SMTP Rate Limit

Message throttling refers to a group of limits that are set on the number of messages and connections that can be processed by an Exchange server. These limits include message processing rates, SMTP connection rates, and SMTP session timeout values. These limits work together to protect the mail server(s) from being overwhelmed by accepting and delivering messages.

Sender IP Reputation Analysis

Our Sender IP database is like a credit score to gauge your credit worthiness but for email: It measures the health of your email program.

SMTP Transaction Check

Once the SMTP dialogue is underway, you can perform various checks on the commands and arguments presented by the remote host.

Sender authentication

You can use SMTP sender authentication to ensure that the sender of a message is a legitimate user of an SMTP server.

Mail Routing

Inbound control

To prevent your mail system from accepting unwanted mail, SCES provides a set of controls that let you restrict incoming SMTP connections. The Inbound Connection controls let you specify whether SCES checks the names of connecting hosts in DNS or, if by host name or IP address, the remote hosts from which the server allows and denies connections.

Destination control and load balance

Flexible policy to control the mail flow to route or reroute to the destination servers, balancing the traffic to the different destination. Or, even BCC, change recipient and etc.

Outbound source and rate control

Outbound rate controls are applied to protect against spam and mass-mailing malware from compromised accounts. It helps prevent spammers and hackers from compromising your email server by relaying mass mailings. It also helps protect our systems and keep our customers safe.

Content Security

Heuristic spam detection

The heuristics detection method differs from the signaturing system because it uses predictive technology instead of reactive technology. The predictive nature of targets unknown spam threats and suspicious emails. It scores each email against a set of rules. If an email achieves more than a specified score, it is identified as spam. The heuristics detection method helps to identify those spam emails that change most frequently, such as unsuitable or fraudulent mailings. The heuristics detection method also enables you to block newsletters.

AI spam signatures

The use of machine learning means that there's a transition from pattern recognition in spam emails to self-learning and optimizing systems. Here are ways that AI-based tools will detect and filter spam:

Keyword and content-based filtering: Machine learning approaches such as Neural Networks, Bayesian classification, k-nearest neighbor(kNN), and others are used. Here, keywords, phrases, and their distribution and frequency are assessed, and rules are made to filter spam email.

Similarity-based filtering: kNN is used to classify emails based on whether they are similar to stored emails. Email attributes form a foundation and based on these, new instances are plotted as points for future emails.

Sample-based filtering: Machine learning algorithms are trained to detect new emails as spam or not based on training data extracted from sample mails. These sample emails are from legitimate and spam emails.

Adaptive email spam filtering: Spam emails are made into groups. Each group is represented by a token or emblematic text. These groups of representative texts are made up of words, phrases, and even meaningless strings. Incoming email is compared to these tokens or representative text and classified into spam or not-spam.

Reputation based spam analysis

RBL reputation analysis votes on the probability that the message is spam based on comprehensive information about the source of the message, rating the reputation of the sender based on the percentage of spam messages sent from that IP address in the past. SCES assigns a level of trust to key real-time blackhole lists (RBL) that rates the reputation of the RBL based on its accuracy at blocking spam. While most service providers use RBLs, SCES also provides a customer-configurable process for limiting false positives to help ensure that our customers receive a high level of spam protection with minimum impact on their businesses.

Category based spam analysis

Non-malicious emails will have a category of None and will have a low spam score. Certain policies such as Permitted Sender& intentionally bypass Spam Scanning and so no information for these will be displayed.

Sender pattern-based analysis

SCES will learn the sender and receiver communication and build the pattern model. Based on its pattern model, the engine will decide

Content analysis and intention recognition

The presence of spam content in social media is tremendously increasing, and therefore the detection of spam has become vital. The spam contents increase as people extensively use social media. The time spent by people using social media is overgrowing, especially in the time of the pandemic. Users get a lot of text messages through social media, and they cannot recognize the spam content in these messages. Spam messages contain malicious links, apps, fake accounts, fake news, reviews, rumors, etc. To improve social media security, the detection and control of spam text are essential. The various techniques involved in spam detection and classification involving Machine Learning, Deep Learning, and text-based approaches.

Attachment Protection

Anti-Virus

Anti-Virus engine offers an extensive real time scanning and virus definition updates. Catch a variety of known virus, outbreak, spyware, trojans, worms and malware threats.

Attachment Pre-Detector Check

Attachment pre-detector crack and analyze abnormal attachment traffic, and attachment file type to predict and block potential attachment threats

Cloud Sandbox

To protect against the unknown, new advanced malware emails and attachment files will be submitted to Cloud Sandbox. Suspicious email attachments will be sent as encrypted packages to the powerful Cloud sandbox to run dynamic sandbox scanning. The Cloud Sandbox provides the extra layer of analysis which Antivirus engine is not able to cover up. The Cloud Sandbox provides the professional and comprehensive analysis report for the SOC or IT to better understand the attacks. The Cloud Sandbox would cross-check with the Cloud URLProtect module for any suspicious URLs in the samples for getting the full coverage to defeat the downloader attacks. The Cloud Sandbox supports lots of file types, including but not limited to office document, executable files, archives etc.

Phishing Protection

Scam

The robust phishing detection engine can protect the users from these attacks,

- Company Impersonation
- Spear phishing
- Email Account Takeover
- Phishing Emails

Dynamic Phishing Detection

A phishing detection scheme based on evolving neural network & reinforcement learning is proposed. It can detect zero-day phishing attacks by exploiting learning of new behaviours. Evaluation was performed using well-known data sets.

BEC

SCES can identify the red flags of BEC emails (like reply-to addresses that don’t match sender addresses) and use machine learning to analyze email language for indications of an attack.

Zero Trust Protection

The zero-trust model means not allowing delivery of messages unless they originate from a email which is completed trusted and clean and sender who has been granted explicit permission to deliver messages to that inbox. SCES can be effective when it comes to identifying trends in social engineering and malicious content, but they don’t provide much usable information when it comes to sender identity, due to the rapidity with which email attackers mutate their identities.

Mail Archive (SCEA)

Say goodbye to email clutter and hello to seamless organization with SCEA – the ultimate solution for modern email management. Packed with cutting-edge features designed to enhance productivity

and streamline your communication, SCEA is here to transform the way you interact with your inbox.

Unlimited Storage

Never worry about running out of space again. With SCEA, enjoy unlimited storage capacity for all your emails, attachments, and important documents. Say farewell to storage restrictions and hello to endless possibilities.

AI Assistant

Experience the power of artificial intelligence right in your inbox. SCEA 's advanced GPT boost learns from your behavior to provide personalized suggestions, prioritize emails, and even draft responses on your behalf. Effortlessly stay on top of your correspondence without lifting a finger.

Cloud Access

Access your emails anytime, anywhere with seamless cloud integration. Whether you're in the office, on the go, or working remotely, SCEA ensures that your emails are securely stored in the cloud, ready to be accessed whenever and wherever you need them.

Mail Encryption & Secure Message Delivery (SCEE)

Centralized Encryption Architecture

SCEE supports centralized, policy-driven encryption for inbound and outbound emails.
Key capabilities include:

- Policy-based automatic encryption triggered by content, sender, recipient, domain, or DLP rules
- Gateway-level encryption enforcement without requiring end-user intervention
- Centralized key management and encryption control
- Seamless integration with existing mail servers and hybrid/cloud environments
- Administrative visibility and audit logging of encrypted communications

The centralized approach ensures uniform encryption enforcement across the organization and prevents accidental transmission of unencrypted sensitive data.

This model is suitable for:

- Government and PSU deployments
- BFSI and regulated industries
- Organizations requiring centralized compliance control

Password-Protected Secure Delivery (Body & Attachment Protection)

SCEE supports secure message delivery using password-protected email body and/or attachment encryption.

Capabilities include:

- Password-protected email body encryption
- Password-protected attachment encryption (e.g., encrypted PDF/ZIP formats)
- Secure notification email with protected content access
- Configurable password policies (complexity, expiry, retry limits)

This approach enables secure communication with external recipients without requiring specialized encryption software.

Use cases include:

- Secure document sharing with third parties
- Confidential financial or HR communications
- Ad-hoc secure message delivery
- Protection of personally identifiable information (PII)

Outbound Accuracy Delivery

Deliver & Track the outbound emails for the business

SCES helps your business by tracking your emails to the peers and prospects. SCES could track the advertisement and marketing emails individually and provide the report for the business understanding of your investment in email communication.

GPT Business Optimization

AI Responder

SCES helps more than security, and business, productivity by

- Translate the email from all known languages to English
- Summarize the email
- Draft the response, accept or decline the request