

MANAGED CLOUD EMAIL SECURITY (MCES)

WHY YOU NEED

MANAGED CLOUD EMAIL SECURITY (MCES)

Email is a mission critical form of communication for businesses of all sizes. Unfortunately, it is also one of the simpler attack vectors to exploit. When users get an email, their natural response is to open it, making your business one click away from a potential data breach and business disaster. Cybercriminals know this.

No wonder email is a highly popular method used to distribute many forms of malware. A recent study revealed that 96% of all phishing attacks occurred via email using employee credentials and 91% of successful attacks start with an email. Furthermore, it is estimated a successful ransomware attack costs a business on average \$1.85 million

As bad actors continue to discover new ways to exploit email systems, vulnerabilities and attacks will keep growing. This requires businesses to adopt a vigilant approach to monitor, protect and secure email platforms minimizing user impact.

WHY CHOSE NETWORK BOX USA

MANAGED CLOUD EMAIL SECURITY (MCES)

The Network Box USA MCES is a cloud-based solution specifically designed to secure a business's email platform and block the flow of malicious emails to users. If a malicious email never makes it to a user's inbox, it cannot do any damage.

MCES's multiple mail scanning engines verify every email on your platform and block all malicious emails containing bad links, malware, spam, and scams from being received by a user.

MCES leverages intel from 25 anti-spam engines, 18 anti-malware engines, and is backed by a database of over 55.6 million signatures. MCES's patented push technology ensures businesses are protected with the latest security updates, in just under 45 seconds from availability, and its email scanning engine catches spam with a success rate of 99.78% making it the best choice for email security.

MCES IS POWERED BY NETWORK BOX USA:



**BEST-IN-CLASS THREAT
INTELLIGENCE**

**ZERO-DAY THREAT
PROTECTION**



**SELF-OPERATED
SECURITY RESPONSE CENTER**

3 ISO Certifications
PCI DSS 3.2 attestation
70+ threat intelligence partners



**FULLY STAFFED
SECURITY OPERATIONS CENTER**

UNIFIED MANAGEMENT GUI

Network Box USA Managed Cloud Email Service secures a business's email platform and protects users while minimizing risk

MCES scanning engine catches spam with a success rate of 99.78%

MCES FEATURES

✓ Protects Against Threats the Same Day They Appear

The rate at which new threats are generated makes it difficult to keep your protection up to date. MCES includes Z-Scan, a fully automated real-time zero-day anti-malware/anti-spam engine which creates and releases fingerprints, effectively reducing the time between discovery and protection to mere seconds.

✓ Securing Email in the Cloud Saves on Bandwidth and Frees Up Resources

In today's threat landscape, email security needs to be an ongoing focus. MCES includes anti-malware scanning, SPF checks, sender IP reputation, challenge response, and the list goes on. All of this puts greater processor demands on a server and its network, but MCES removes this burden by moving email scanning and filtering to the cloud, looking at an email before it enters your network.

✓ Cleans email flow before it gets to your network

Emails containing malicious messages can bottleneck your mail server, possibly preventing time-sensitive messages from reaching recipients. With MCES, emails are filtered and scanned prior to even reaching your mail server.

✓ Shields you from possible DDoS attacks

Email DDoS attacks inundate mail servers with large volumes of messages. These attacks can easily compromise bandwidth and disrupt business operations. MCES stops these attacks in the cloud before the messages even reach your mail server. For some clients, email may be the only port open to the Internet. As such, scanning in the cloud allows you to completely lock down your firewall and set it in stealth mode so hackers can't even find it.

✓ Hides your IP Addresses from hackers

With your private IP addresses, a hacker can track your Internet activity and see the inner workings of your network (*for instance, how many computers you're connected to*). MCES provides another line of defense to deviate hackers away from your network.

✓ Provides a queue for your emails

What happens to emails when your Internet or server go down? MCES has multiple redundancies for Internet connectivity, power, and hardware, ensuring an uptime and availability of 99.999%. Should your Internet, firewall, or email server go down, emails will still be scanned and queued on their systems, ready to be delivered to you as soon as yours are back online.



POWERED BY NETWORK BOX USA.
THAT'S CYBERSECURITY DONE RIGHT.

NETWORK BOX USA MCES DATASHEET (managed cloud email security)

MCES SERVICE INCLUDES:

- ✓ Protection for SMTP
- ✓ Protection for encrypted protocols (SMTPS, STARTTLS)
- ✓ Email Policy Enforcement to block active content within emails
- ✓ Web Policy enforcement to block unsavory content within emails
- ✓ Challenge Response
- ✓ Proprietary Relationship Database
- ✓ Network Box Anti-Spam Module
- ✓ Envelope Verification
- ✓ Blocking of spamming IP addresses
- ✓ OCR (Identifies spam images)
- ✓ Directory Harvest Attack Protection
- ✓ DoS/DDoS Protection
- ✓ Anti-phishing and spear-phishing
- ✓ Protection against "CEO fraud attacks"
- ✓ Anti-malware
- ✓ Network Box Proprietary Antivirus
- ✓ Kaspersky Labs or Bitdefender Antivirus
- ✓ Z-Scan true real-time zero-day anti-malware protection
- ✓ Anti-Spyware
- ✓ Email Spooling and Queuing
- ✓ DLP (Data Leakage Prevention)
- ✓ Support for IPv6
- ✓ LDAP Link (support for Radius as well)
- ✓ Mail Portal email report
- ✓ Option for real-time personalized user interface
- ✓ 24x7x365 Monitoring and PUSH Updates
- ✓ 8 AM to 8 PM Business day support for email issues



POWERED BY NETWORK BOX USA.
THAT'S CYBERSECURITY DONE RIGHT.