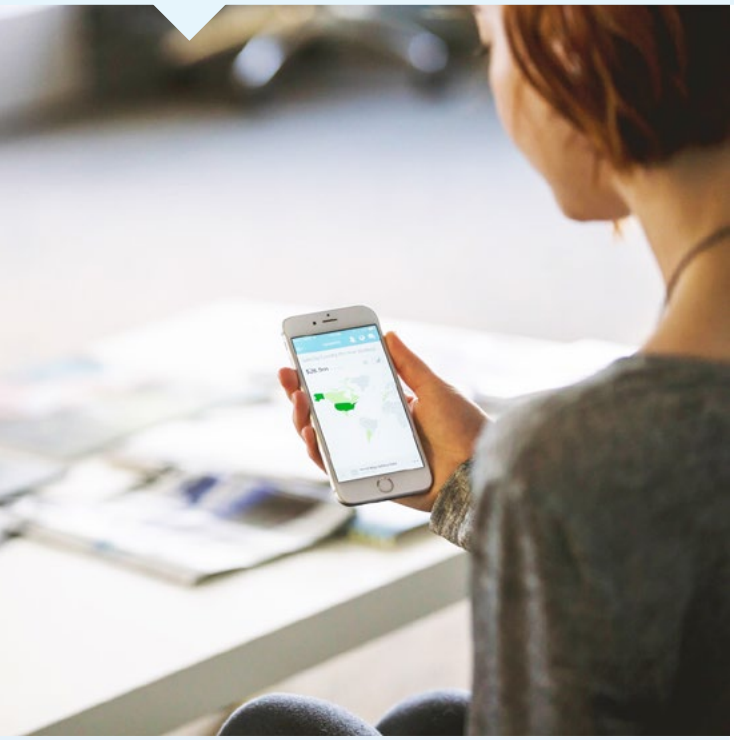
MAX by LOGICnow | Mail

Email Security

The need for comprehensive email security is greater than ever

Email continues to be the most common attack vector by which networks are compromised and malware spread. Spam still comprises the majority of messages sent, while blended threats and phishing attacks continue to grow in both volume and sophistication. Too often, existing antivirus and anti-spam solutions are vulnerable to emerging threats.



Robust email security encompasses not only protection against the obvious threats to security, but also the less obvious threats to productivity. Given the critical nature of email as a communication tool for businesses, any downtime can have a substantial impact on an organization's productivity.

The MAX MailProtection service from LogicNow provides built-in, automatic email continuity to ensure that users can easily continue to access and respond to email at all times, in addition to robust defense against spam, viruses, and other email-borne threats.

1 Adaptive Spam Defense

A core component of any email security solution is highly accurate spam detection. MAX MailProtection blocks spam in the cloud through a robust combination of methodologies for message analysis, including:

- Authenticity Checks encompassing detailed header analysis, SMTP conversation details, message encoding and formatting, and other characteristics
- Message Fingerprinting to compare email signatures to known spam messages
- An extensive, continually updated Heuristic Rule Set
- Real-Time Message Source Analysis to assess whether an increased volume of mail flow is a legitimate high-volume mailing, or the result of a spammer hijacking vulnerable systems
- Pattern Detection that can detect emerging spam based on recurring patterns
- Customizable whitelists and blacklists that can be applied on an account-wide, organization-wide, domain-wide, or user-specific basis

The result of this comprehensive approach is an extremely accurate system for detecting spam, backed by an industry-leading service level agreement that guarantees 99% spam detection and no more than one false positive for every 100,000 messages.

2 Sophisticated Threat Detection

Viruses are growing in sophistication. Social engineering or web-based threats are increasingly combined with email-based attacks. Viruses and variants can be disseminated across the globe in just minutes, while the periodic emergence of new types of attacks such as the Cryptolocker virus seem to change the threat landscape overnight.

The need to protect networks and devices against malware is clear. What is less well understood is the vulnerability that many organizations still face, even with an antivirus solution already in place.

Most antivirus solutions are signature-based systems. This means that when a new virus emerges, antivirus software may only detect the threat if that virus matches an existing signature, or only after the anti-virus vendor has had time to develop and distribute an updated signature that recognizes the new virus. This creates a window of vulnerability that can endure for hours or even days, during which time the organization is at risk. Robust security is essential to ward off these threats, including the use of multiple scanning engines with the appropriate technology to fight zero-day and even zero-hour attacks.

MAX MailProtection offers a unique, powerful combination of defenses including traditional signature-based virus engines, virtualization-based malware detection technology, and zero-hour pattern-based antivirus defense. These technologies block email-borne malware – including fast-moving, emerging threats – faster than traditional signature-based systems, dramatically reducing risks for customers. MAX MailProtection's robust malware defense is backed by an industry-leading service level agreement that guarantees customers 100% detection of all email-borne malware.

3 Email Continuity

Email is the lifeblood of today's organizations, so it is critical that this communication channel is online at all times. Regardless of whether the customer is hosting its own email or using a third-party service such as Google Apps or Microsoft Office 365, the impact on productivity of even a short outage can be significant.

MailProtection's built-in email continuity requires no prior preparation or training, and automatically begins working in the event of any temporary issues with the customer's primary infrastructure – DNS issues, network or routing problems, hardware or software errors, or maintenance windows. More than simple queuing of messages, the continuity within MAX MailProtection allows end users to easily continue to access and respond to messages, while their primary infrastructure is off-line. Given the importance of ongoing email communications, a continuity solution should be a requirement for every organization's email security plan. Email is a critical communication tool for almost all businesses. MAX MailProtection customers can rest assured that they are protected by continuously improving, comprehensive email security encompassing highly accurate spam detection, robust virus defense, and built-in email continuity, to maximize their productive use of email.

LOGICnow delivers the only 100% SaaS, fully cloud-based IT service management (ITSM) platform, backed by collective intelligence and the highest levels of layered security. LOGICnow's MAX products including Risk Intelligence, Remote Management, Backup & Disaster Recovery, Mail and Service Desk – provide actionable insights, helping IT professionals rewrite the rules of IT. For more information, visit www.logicnow.com.

Connect with us!

Please get in touch if you have any questions about any of our services.


UK: +44 0 1313 414899
US: +1 855 801 5461
APAC: +61 8 7123 4068


info@LOGICnow.com


@LOGICnow

LOGICnow
CHOOSE INTELLIGENCE