Brought to you by Informa Tech

OMDIA

Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: Retarus offers security, compliance, and infrastructure for corporate email

Summary

Catalyst

Retarus is a provider of cloud-based enterprise services in non-voice communications (email, fax, and SMS). This report focuses on its email security services, collectively referred to as Retarus Secure Email Platform.

Omdia view

Email is central to multiple business processes around the globe, from collaboration to procurement and interactions with channel partners and customers. This status also makes it a favorite target for threat actors, with estimates suggesting that some 90–95% of all cyberattacks involve email somewhere in the process. The explosion in ransomware, already a problem before coronavirus and only amplified by the pandemic's impact on work practices, has raised the profile of email-borne attacks in the minds of regulators, cyber insurers, and enterprises themselves, such that security on both inbound and outbound email traffic has become a requirement of any defensive strategy.

In this scenario, the ability to deliver comprehensive email security services with capabilities including threat detection and mitigation, backup/archiving, and encryption positions Retarus to address the growing need to secure both the inbound and outbound email communications of enterprises.

Why put Retarus on your radar?

Retarus's Secure Email Platform is a comprehensive set of capabilities enabling the security and compliance of corporate email systems on both inbound and outbound traffic. Its modularity enables it to be acquired piecemeal, which can be advantageous for companies already invested in Microsoft's email security: they can get modules that complement what is provided by Microsoft without the need to invest in the cloud gateway that is the core of the Platform.

The Transactional Email service, which carries emails from its customers' web apps (see details below), is also an interesting differentiator for the overall portfolio.

Market context

The world of inbound email security has been going through a number of major changes over the last decade, due to a variety of factors. The two largest are as follows:

- The first concerns the migration of how the email function itself is delivered, from on-premises deployments of licensed software to cloud-based services. The main actor here is of course Microsoft, which dominated the on-premises world with its Exchange technology and unveiled its cloud-based alternative, Office 365 (O365), in 2011. Since then, ever more enterprise customers have moved to this delivery model for their emails, enabling their employees to continue to use the Outlook clients on their laptops to receive their messages, thus dramatically easing the migration process.
- As a result of becoming a cloud-based email services provider, Microsoft also began to invest in email security through both acquisition and internal development, with its security capabilities being included in the different the SKUs of Office 365 (now renamed Microsoft 365 and extending beyond email).

These two developments have been crucial in the sector. An email security industry grew up in the on-premises world and was based on secure email gateway (SEG) technology, which introduces a software server before emails reach the corporate mail server to perform inspection of the messages and remove suspect ones. Vendors in that segment were obliged to develop cloud-based versions of their technology as O365 adoption took off.

However, with Microsoft itself offering SEG-like functionality – that is, protection from malware, spam, and spyware – with its Exchange Online Protection (EOP) technology, which is bundled into all O365 SKUs from E3 upwards, the SEGs are also obliged to justify customers' investments in their technology rather than just going with Microsoft. This is normally done by noting that EOP is really "SEG-lite" – that is, not as comprehensive as a full SEG.

Beyond that, however, a new wave of email security companies has grown up in the O365 era, offering technology that interacts with a user's inbox via API rather than sitting in front of the mail server. These non-SEGs offer the ability to detect the more advanced forms of email-borne attacks, such as phishing and business email compromise (BEC). They work on the assumption that a customer is using either a SEG or Microsoft EOP to catch the more basic forms of attack, while their claim for their technology is that it detects and blocks the more advanced attacks that both SEG and EOP miss.

In parallel with all these developments, a smaller market segment has grown up of vendors offering security on outbound email traffic, generally based on either data encryption or behavioral analysis to detect problematic behavior. The requirement for security on outbound email traffic started life in highly regulated sectors, where the awareness of insider risk is more acute but is gradually spreading to the broader enterprise market. Omdia believes it will become more widespread over time.

Product/service overview

Retarus started in email with a SEG, and over the years it has expanded its offering, adding non-SEG functionality which it describes as "postdelivery protection," to protect against phishing and BEC. Retarus thinks of the overall offering of this platform in three pillars, namely security, compliance enablement, and infrastructure, particularly on the outbound email side of things. Beyond actual email security, the portfolio, which goes to market under the Secure Email Platform banner, now includes the following:

- **Email Compliance services**
  - **Email Archive**. This enables customers to archive large email volumes on a long-term basis, with retrieval and audit functions.
  - **Email Encryption**. Encryption makes it possible for companies to comply with applicable data protection regulations, safeguard valuable know-how, and protect confidential information.
- **Email Infrastructure services**
  - **Email Continuity.** These failover services provide customers with a backup system so that they can be reached by email, even when their main mail system is down, and prevent commercial losses or damage to their reputation. This service can run in the background, even for customers who are not signed up for the rest of the Secure Email Platform. Such customers can still use it as a fallback for when their corporate email system is down. Some customers have used this service during ransomware attacks, enabling them to rebuild the servers of their corporate email system and running Retarus Email Continuity as an offline alternative in the meantime.
  - **Predelivery Logic**. This service is essentially a policy engine on the gateway that enables email workflow automation, analyzing and processing emails according to content, origin, and other criteria before they reach the corporate infrastructure. This offers user-dependent email routing to specific servers or locations within the company network. Emails can be analyzed and processed based on their content or language, including automated pre-sorting into role-based inboxes.
  - **Transactional Email**. Retarus provides this service to carry emails from its corporate customers' applications, covering a range of requirements such as order confirmations, password resets, status notifications, and even newsletters.
  - **Bounce & Response Manager**. This handles emails that keep getting a bounceback, which first involves checking whether they are coming back with malware embedded in them, and second improves the workflow for how such emails are handled. That is, it determines whether the return is triggered by an out-of-office scenario or is in fact a legitimate customer request.

- **Trace & Recover**. Trace & Recover is a short-term archiving capability designed to address a couple of common use cases: one is for e-commerce companies that cannot send an invoice to a customer without going back to the original system on which the order was generated, and another is in contact centers, where the agent doesn't have access to the full backend application and cannot send an email without restarting an entire process. In both scenarios, having some documentation in short-term archive that can be viewed via a browser-based consultation is clearly advantageous.

As for how it takes its email security portfolio to market, the offering has certainly been centered around the SEG until now, but there two modules (Transactional Email and Email Continuity) that are already available as standalones (i.e., without the need for the cloud gateway) and there are plans for two more – Sandboxing and Archive & Backup – to follow suit.

This reveals an awareness on Retarus's part that email security is moving away from the gateway model, even in its cloud-based version, and that a number of the modules can conveniently be acquired to complement what a customer is already taking from Microsoft or another email security provider.

Company information

Background

Retarus was founded in 1992 by CEO Martin Hager. The company's VP of Technology is Michael Grauvogl, who has been developing software for Retarus since 1994 and holds multiple patents together with Hager.

Retarus launched its first offering, a corporate fax service, in 1993, adding its email security service the following year. By 1996 it was making its first foray into electronic data interchange (EDI), the inter-business communications technology that had taken off as supply chains grew more complex and international. In 1997 it added encryption to its services for outbound corporate email. In 2003 it launched WebExpress, a web-based service that enables enterprises to send personalized content to large distribution lists by email, fax, or SMS.

International expansion began in the 2000s. The company currently operates out of offices in its home country of Germany as well as in eight other European countries, the US, Singapore, Thailand, and Australia.

Retarus remains privately held, without VC funding.

Current position

The business services offered by Retarus fall into three broad categories, each of them called a platform:

- **Communications Platform**. The Communications Platform covers an organization's communications needs in the areas of fax, SMS, and transactional email (i.e., outbound communications for purposes such as newsletters, order confirmations, password resets, and status notifications).
- **Business Integration Platform**. This comprises managed EDI services, a service called WebConnect for contacting non-EDI suppliers via mail, Intelligent Capture (another means of connecting with suppliers without EDI), electronic invoicing, and e-procurement.

- **Secure Email Platform**. This platform includes security, archiving, encryption, business continuity for the email service, the transactional email component also included in Communications Platform, and Predelivery Logic, which is a service that lets companies analyze and process emails according to content, origin, and other criteria before they reach their infrastructure. Use cases include organizing, redirecting, monitoring, and editing of emails.

The vendor has made the Secure Email Platform more modular over the last year and is clearly readying it for more indirect sales driven through its partners. It highlights the fact that a number of its modules come with functionality that is not available from Microsoft's email security products. The company sees this modularity as more channel-friendly, enabling its technology to be offered as an overlay on Microsoft's.

Retarus serves a customer base that includes enterprises such as Volkswagen, Porsche, Goldman Sachs, and Citibank. It does not go down as far as the SoHo or SMB segments, focusing instead on a core target market comprised of companies in the 1,000–10,000-employee segment, though it does have customers with as many as 180,000 corporate users. Around 85% of its business is currently direct, but it also sells through some major partners, including IBM, Atos, and T-Systems (the IT services arm of Deutsche Telekom) and is expanding its market reach into smaller companies by developing its channel partner network.

The vendor has three data centers in Europe (Munich, Frankfurt, and Zurich), two in the US, and two in Asia and Oceania, with customers free to choose which data center they use for backup, a feature that is important for compliance purposes, where data residency can be an issue.

Future plans

Aside from the additional standalone modules mentioned above, Retarus is also readying integrations with third-party systems in two areas. In sandboxing, where the vendor uses Palo Alto Networks' products in its data centers to deliver the service, it will shortly add the ability to integrate with other sandboxes already in the customer's environment; similarly, in encryption, the customer will soon be able to bring its own platform, integrated with the Retarus services.

With these plans, Retarus continues to pursue its general open platform approach, which is also reflected in other areas. For example, the company is continually evaluating the integration of market-leading technologies and data sources following a "best of breed" approach. The same applies to deeper integration into third-party ecosystems in the area of business applications, as far as their Transactional Emails offering is concerned.

Another focus remains the channel business which will be further expanded by adding additional local partners to the global network.

Key facts

Table 1: Data sheet: Retarus

Product/service name	Retarus Secure Email Platform	**Product classification**	Modular services for email security, email compliance, and email infrastructure
Version number	N/A – cloud-based services	**Release date**	N/A
Industries covered	Manufacturing, automotive, trade & logistics, utilities, financial services, healthcare, public sector (via partners), telco (via partners)	**Geographies covered**	EU, APAC, US
Relevant company sizes	Midsize, enterprise	**Licensing options**	Pay-per-use/mailbox-based
URL	https://www.retarus.com/secure-email-platform/	**Routes to market**	Direct and indirect sales via partners
Company headquarters	Munich, Germany	**Number of employees**	430+

Source: Omdia

Analyst comment

The competitive landscape in email security is a complex one, in which dedicated specialists such as Proofpoint and Mimecast compete with vendors with a broad security portfolio – for example, Cisco, Barracuda, Trend Micro, and Sophos – as well as with a bevy of non-SEG startups. Furthermore, all this plays out against a backdrop in which an IT industry heavyweight (Microsoft) not only dominated the corporate email services segment, but also offers email security bundled into the various SKUs of O365.

While Microsoft's security offerings are not as complete as those from dedicated vendors, they may be "good enough" for some customers, thus calling into question the need for investment in additional security platforms. And of course, there is always the danger, particularly for the non-SEGs, that while they can claim to complement its email security offerings today, tomorrow it may decide to develop competing technology to theirs, or simply buy one of their brethren, thereby putting them into direct competition with the tech giant.

In this scenario, Retarus brings a couple of interesting features to the conversation. Firstly, there is the fact that its Secure Email Platform is more comprehensive than the offerings of many competitors, particularly ones selling into the midmarket. Secondly, the modularity that they have been introducing into the Platform over the last year, and which looks set to increase in the coming quarters, bodes well for its ability to coexist peacefully (and profitably) with Microsoft in this area.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Omdia Universe: Selecting an Inbound Email Security Platform, 2021–22 (September 2021)

Omdia Market Radar: Outbound Email Security (November 2020)

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com