Publication date:
18 Nov 2020
Author:
Rik Turner
Principal Analyst

Omdia Market Radar: Outbound Email Security

Brought to you by Informa Tech

Table of Contents:

Table of Figures:

Summary

Catalyst

Email is a powerful instrument for sending messages anywhere, to anyone, so much so that it has become a universal tool of communication, both within and beyond the business environment. Its status also makes it a prime target for threat actors, and the risks from malware, phishing, and ransomware regularly make the news headlines while keeping an entire industry of technology in business providing security for inbound email flows.

However, another area of email security is now ready for a little more attention than it is currently given. Outbound email security focuses on building in controls to offset identified risks from the so-called insider threat, which spans various scenarios in which sensitive, confidential, or simply the wrong information is accidentally or deliberately sent to the wrong recipients. This outbound email data protection applies at all stages of the process:

- Composition and transmission of email
- Understanding the context and sensitivity of content and recipient
- Encrypting sensitive data while it is being sent (in transit) and while it is stored (at rest)
- Applying controls such as revocation or retraction to prevent or mitigate data leakage

Omdia view

In some sectors, whether because of regulation, the presence of highly confidential data, or specific privacy needs (including personally identifiable information, or PII), there may be a higher risk of deliberate or sloppy intent or action that must be detected and blocked. Organizations operating in these areas (e.g., financial services, legal, healthcare, and the public sector) will find that it is not only in their best interests to do more to protect against data leakage through misdirected emails but that it is something with which they must comply and demonstrate compliance. For this reason, outbound email security and data protection has been important to these sectors and has had most of its deployments in them.

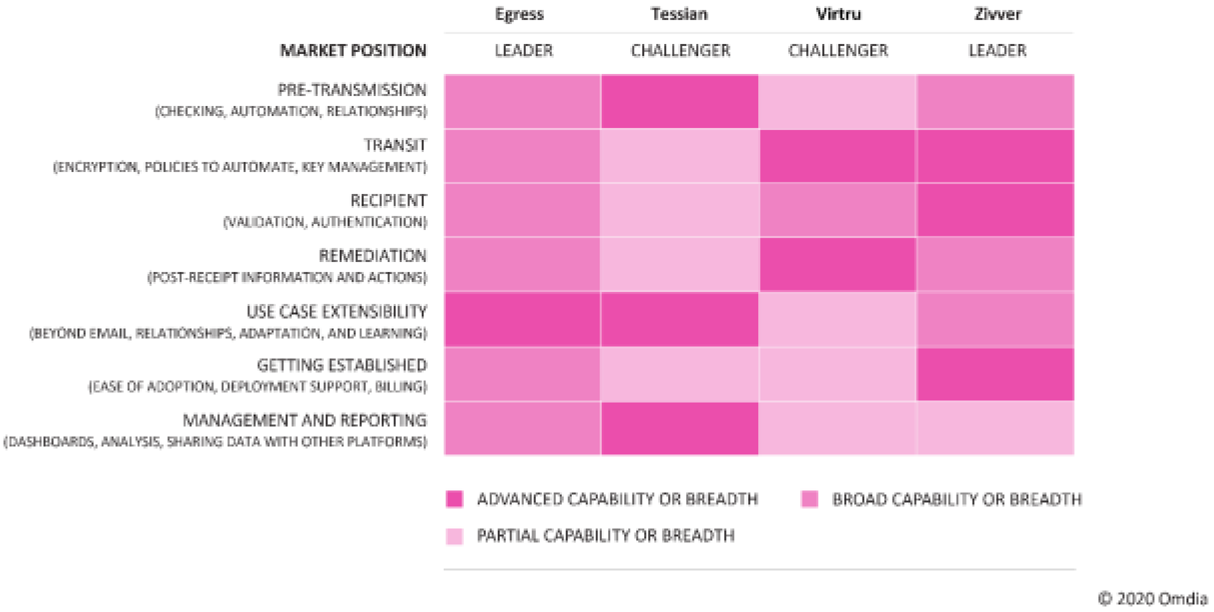
However, organizations in all sectors use email for some form of important business communications and for the transmission of sensitive data that should only be seen by certain recipients. They are also all affected by data privacy and protection regulations. Attacks continue to increase in number and severity and can result in accounts and privileges being taken over by malicious actors that may, for example, use email to exfiltrate data. Nor are legitimate users infallible, and mistakes from inadvertent or accidental data sharing can have significant consequences. All these scenarios can be mitigated with the right controls in place.

Applying the necessary controls and greater rigor, without making the process so difficult or time-consuming that it gets circumvented anyway by frustrated users, is a challenge that organizations will increasingly need and want to address. Encryption could be seen as the way to apply the strongest control, especially for data in transit, and shared public keys can be used to authenticate access by recipients. However, machine learning now opens up ways to intelligently assess the complex relationships between email senders, recipients, and the content they share.

Taking steps to ensure greater data protection and avoid data leakage is something that all companies must deal with, and outbound email security must be addressed. This report sets out the fundamentals of such technology and explores and compares the approaches taken by a number of vendors with a specific focus on this area.

Omdia's research for this report profiled four vendors of outbound email security in depth and rated each of them against a set of key capabilities defined in the **Key capabilities** section. A summary is show in **Figure 1**.

1. Figure 1: Omdia Market Radar 2020: Outbound Email Security



	Egress	Tessian	Virtru	Zivver
MARKET POSITION	LEADER	CHALLENGER	CHALLENGER	LEADER
PRE-TRANSMISSION (CHECKING, AUTOMATION, RELATIONSHIPS)	▨	■	□	▨
TRANSIT (ENCRYPTION, POLICIES TO AUTOMATE, KEY MANAGEMENT)	▨	□	■	■
RECIPIENT (VALIDATION, AUTHENTICATION)	▨	□	▨	■
REMEDIATION (POST-RECEIPT INFORMATION AND ACTIONS)	▨	□	■	▨
USE CASE EXTENSIBILITY (BEYOND EMAIL, RELATIONSHIPS, ADAPTATION, AND LEARNING)	■	■	□	▨
GETTING ESTABLISHED (EASE OF ADOPTION, DEPLOYMENT SUPPORT, BILLING)	▨	□	□	■
MANAGEMENT AND REPORTING (DASHBOARDS, ANALYSIS, SHARING DATA WITH OTHER PLATFORMS)	▨	■	□	□

■ ADVANCED CAPABILITY OR BREADTH ▨ BROAD CAPABILITY OR BREADTH

□ PARTIAL CAPABILITY OR BREADTH

© 2020 Omdia

Source: Omdia

This is a very close market, but Egress and Zivver are identified as *leaders*, having advanced or broad capabilities across the majority of areas. Tessian and Virtru are identified as *challengers*, with partial capability in more than one area.

Key messages

- **Email does serious work.** Widespread acceptance and adoption of email for consumer and work activities has resulted in casual and informal approaches to composing and sending emails, which can often verge on "sloppy." But email is regularly a major component of workflows critical to business operations, where sensitive data should only be seen by specific recipients.
- **Phishing is not the only email security threat.** The rise of spam and various types of phishing attacks has generated organizational (if not always user) awareness of the inbound threats introduced via email. Vendors have vigorously risen to the challenge with defensive tools, training,

and awareness campaigns, but the insider threat risks of outbound email tend to have been somewhat overlooked.

- **Accidents happen and have consequences.** Malicious actors and malware are real and have serious consequences, so there is a need to protect against breach events, but day-to-day activities have risks as well. Mistyping, mis-clicking or slips of autocorrect can lead to inadvertent data leakage, and the resulting breaches can be just as serious as malicious action.
- **Retraction needs teeth.** Messages imploring recipients to ignore emails delivered to unintended recipients, or follow-up emails requesting a “recall,” have cosmetic value only. Retraction needs to actively revoke access to affected content and, at the very least, have an audit trail of any activity between the send and retract actions.
- **Business processes need more than just email.** As much as email is an important element of so many business processes, it is not the only element that needs increased attention for data protection and compliance. Outbound email security is one step on a path toward more rigorous digital business workflows.

Recommendations

Recommendations for enterprises

Despite many protestations about email overload and alternative collaboration and messaging platforms, email is not going away anytime soon, and it will continue to be used to (sometimes quite casually) share sensitive information both within and beyond the organization. This introduces risks that can and should be addressed: data protection involves much more than stopping bad things from coming in and causing problems.

Organizations as well as users may not realize how much sensitive information is already being shared, and it would be prudent to find out. They may then also want to look closely at how users behave and how anomalies, whether accidental or deliberate, might be detected and changes made automatically to ensure that users do the right thing and to support organizational compliance with relevant data protection policies and legislation.

Those who think they can fix this in-house are likely to be in for a shock, because forcing users to change their behavior or to remember to encrypt important data is not going to work. However, the intelligent application of machine learning can automatically apply additional controls and simultaneously educate users about the information they are sharing and the risks that involves.

Similarly, waiting for this to become a problem that is fixed by default by the major email platform companies carries significant risk. First, there is the challenge of interoperability between different email clients and platforms when encryption is used, not only with the likes of Microsoft and Google but also with mobile access to email. Then, more importantly perhaps, there is the fact that email is only one of several digital activities conducted in the workplace where behavior and process affect data security. This may evolve into a bigger consideration than just email.

Recommendations for vendors

Outbound email security could easily be seen as simply "selling security" and targeted at the CISO. In reality, however, it is more about managing risks in business processes and helping people to avoid bad behaviors. It affects lines of business and human resources just as much as those responsible for security. This means that while products and services can be compared on their capabilities, it will be just as important to understand how they fit in.

This is not so much a technical integration matter as a business process and social one. This might be particularly important where a vendor's product is building a picture of relationships and vulnerability information based on past email activities and records as part of a machine learning process. Vendors need to address all aspects of deployment and initial use to ensure that not only are inappropriate actions being prevented but users understand why and how it is beneficial to them as well as to the organization.

Defining and exploring outbound email security

Definition and characteristics

People may complain about being swamped by it, but email is the most widely accepted method of regular digital communication within and between organizations and businesses of all sizes. This overwhelming acceptance brings challenges, especially from a security perspective. Part of the problem is the open ethos of email: connect everyone, share messages including attached content, for universal access, by anyone, on any device, anywhere.

Alternative forms of communication and collaboration are readily available; some have even been touted as "email killers," and many can apply more stringent controls. But the need and ease of access on the move or from home and of communication between different organizations (and systems) means that email survives and thrives as the lowest common denominator for digital information sharing.

This also makes it an effective mechanism for importing malware and spam messages or initiating attacks that "phish" for information and trigger unchecked responses. For this reason, there is a vast array of tools, services, and awareness training directed at trying to protect individuals and organizations from the security risks of inbound messages and the effects they might provoke.

Outbound email

Outbound email is a different matter. The trust placed on emails created inside the organization and then sent beyond brings data leakage and authentication challenges. How can it be ensured that a message has gone to the right person? Could someone else have received or read it by mistake or with malicious intent? Was its content too sensitive or inappropriate to be delivered to certain recipients? Can it be retracted? Was it too much content to send via email?

The reasons for a misdirected message may be accidental, since user overfamiliarity is high, and a mistake might be caused by "helpful" autocompletion in email software, or it might be sloppy user activity. It could also be malicious intent by the sender or, indeed, by someone else if an account has been compromised and the credentials exploited or there are attempts at deliberate interception en route.

In any case, the results can range from simple embarrassment to significant compromise of sensitive information. Both organizations and individuals need to be better protected.

Key capabilities

Controlling the flow

It is not only the continued growth of email use that elevates the risk of data leakage but also the fact that workforces are becoming more distributed, working in nonofficial settings, and often using tools that were designed with consumers in mind. There is nothing wrong with this last point—it can improve usability—but it makes it harder for even seasoned professionals to keep up their guard, and of course, anyone can make a mistake.

Securing email effectively means addressing the whole process from message creation through delivery to receipt and beyond. It is about protection from not only rogue actions but also the mistakes of users who might otherwise accidentally, or somewhat sloppily, send sensitive information to the wrong person. Outbound email security tools address these issues by adopting one or other (and sometimes a mixture) of two approaches for protecting against data leakage:

- Ensuring data is not going to the *wrong* place
- Ensuring data only goes to the *right* place

Each approach is different and exploits different technologies, but both aim to achieve the same outcome in controlling the flow of data through email messages and attachments. The first works by looking at behavior and checks for anomalies; the latter applies protections, typically encryption and authentication. Whichever combination of approaches is used, at each stage of the email process several factors need to be considered:

- **Pre-transmission.** Who is the email being sent to? How sensitive is the data in the message and attachments? What is the relationship between sender and recipient in the context of the data being shared?
- **Transit.** How is the data transmission being kept private and secured, both while on the move and while being stored at a mail server?
- **Recipient.** Is the recipient valid, authentic, and permitted to see the data?
- **Remediation.** What can be done if the information was sent to the wrong person or if circumstances have changed and they should no longer have access to it?

While outbound email security is about protecting against data leakage for the benefit of the organization, users need to be fully engaged at each stage of the process. It is important that these tools do not negatively affect the user experience or significantly alter their workflow. Users might need additional controls, but they also need to be alerted to good practices and receive feedback as soon as issues are detected. All security relies to some extent on user involvement, and so guidance, education, and awareness form part of what is expected of any security tool.

Getting established

With email being such a well-adopted and familiar communication mechanism, additional outbound security must be incorporated without users changing the way they work or the email clients with which they are already familiar. Without this continuity, users will simply find ways around controls, which could result in bigger problems. IT and security functions are hard pressed as it is, so deployment, integration, and adoption of an outbound email security product will need to be as seamless, automated, and supported as possible across aspects including the following:

- **Workflow integration.** How much historical email information is required? How does it fit into existing email applications? How does it work with mobile devices used to send or receive emails? Can controls be centrally defined and applied by the user?
- **Identity integration.** How does it fit with existing identity systems? Does it require additional configuration? Does it understand personal as well as work email addresses and apply controls to suit?
- **Other integration.** Can it be extended to meet other email integration needs such as automatically generated emails in applications or cloud-based services? Are there open APIs or software development toolkits?
- **Deployment support.** What support is available to assist with setup? How much configuration is automated? How quickly can protection be in place? Is there help for rollout and deployment at a user as well as technology level?
- **Unlicensed users.** What happens when emails are sent to external users who do not have the software or a license to use the service? How do these external recipients access the messages and content sent to them? Do they become guest users, and how is this guest use controlled? Can it be branded by the sending organization?
- **Billing.** Is there a range of commercial options? How does cost scale with usage?

Management and reporting

Applying controls to the process will have an impact on the user, but IT and security managers will need to have control over configuration and the setting up and management of policies. Most organizations will not only want to have flexible alerts and reporting for day-to-day management purposes but will also need assurances for their own governance and procedures and to demonstrate compliance with regulations.

People have high expectations of email responsiveness, so any threats of data leakage posed by outbound email need to be flagged immediately to senders, with real-time feedback and alerts to those managing email or security in general so that prompt action can be taken.

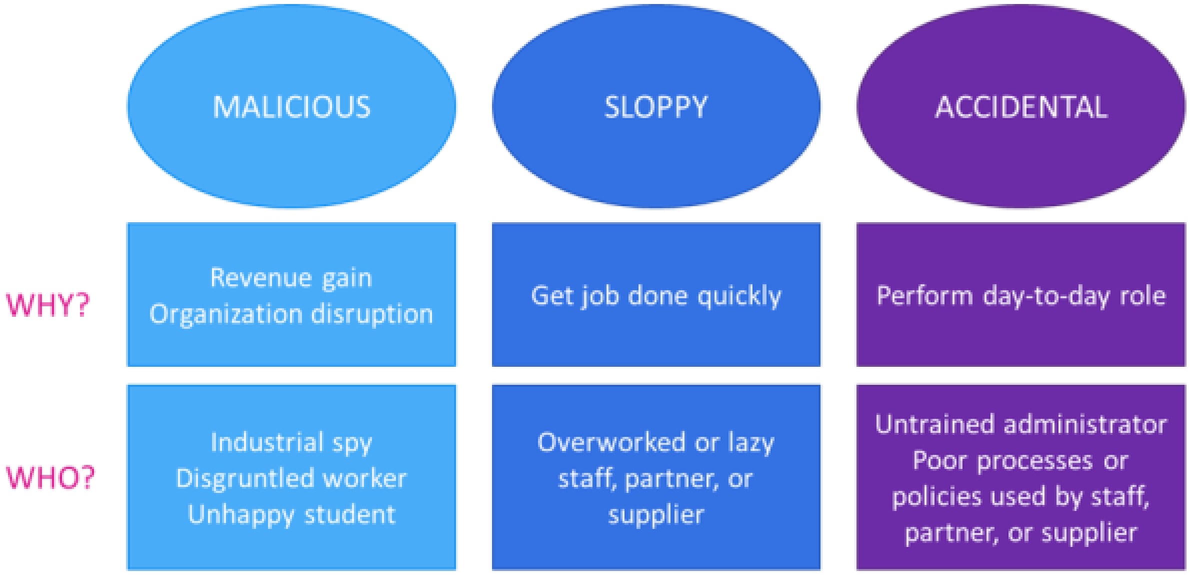
How this information is presented is important, not simply for its ease of use as a graphical tool or dashboard but also to allow for deeper analysis. It might be important to build comparisons internally to find where more user education could be beneficial or to identify vulnerable accounts. External comparable information, if available in suitably anonymized form, might also be hugely beneficial for benchmarking organizations against each other, looking for industry- or sector-wide trends, or adding evidence to the justification of security-spend investment.

As part of integration into wider security operations, information may need to be extracted after the event for further analysis in security information and event management (SIEM), security orchestration, automation, and response (SOAR), or threat intelligence platforms (TIP). Increasingly, the use of behavioral analysis means that the information will be forwarded to other platforms, for example, to assist with training and human resources management.

Business value and applications

The value of outbound email security is in protecting against insider threats, whether they are malicious, sloppy, or accidental. In all cases, insiders have privileges that those outside an organization lack: they have access to internal information and systems, and they have access to tools to help distribute information. Easy-to-use tools such as email are employed every day to distribute huge amounts of information, mostly to the right people. There is nothing at all exceptional about email use, so it is necessary to understand the context and behavior involved (see **Figure 2**).

2. Figure 2: Describing the insider threat



	MALICIOUS	SLOPPY	ACCIDENTAL
WHY?	Revenue gain Organization disruption	Get job done quickly	Perform day-to-day role
WHO?	Industrial spy Disgruntled worker Unhappy student	Overworked or lazy staff, partner, or supplier	Untrained administrator Poor processes or policies used by staff, partner, or supplier

© 2020 Omdia

Source: Omdia

The context and behavior could be any of the following:

- **Malicious.** It could be someone being disruptive, an aggrieved employee, or someone deliberately trying to exfiltrate confidential or sensitive information. Their actions may involve sending to a private email address, could be outside normal working hours, or could be someone sending information that they do not regularly access.
- **Sloppy.** This may not involve deliberate intent to harm the organization, but the individual knowingly tries to bypass systems and ignore training and good practices. They may be sending information so they can use it while working from home or be shortcutting a process by sending messages to someone inappropriate.
- **Accidental.** There may be no motive or intention to do anything wrong, but mistakes are easy to make. Individuals may be acting in good faith and their actions could be accidental, but the result is the same as if a security incident or breach had occurred.

Use-case extensibility

Beyond protecting outbound email, any system that builds a picture based on behavior (in the context of who is sending what to whom) could also be applied to other applications. This may include use cases to do with securing inbound email against spam or targeted spear phishing attacks, or it might be applied to other legitimate forms of communication that would benefit from additional protection. Many business interactions involve the sharing of sensitive or legally significant information between two parties and would therefore benefit from authentication of the participants, protection of sensitive content, and oversight to detect anomalous or inappropriate behaviors. These may include filling out forms, confirmatory signatures important to business processes, or more complex workflows and custom applications that are specific to a vertical market or sector. In all such cases, applying security policies automatically to ensure compliance, without inconveniencing the users or prompting them to consider alternative routes, would be beneficial. For many, securing outbound email will only be a first step, and vendors that go beyond email and offer more will undoubtedly be of interest.

Market landscape

Market origin and dynamics

The challenge of securing inbound email is well known and well understood, with a number of vendors addressing the market with protective products and services, antimalware, and spam filtering. It is a market that has been in existence in one way or another for more than two decades and that has adjusted to changes in how email services are delivered, with the cloud playing an ever-greater role in the services themselves and, consequently, in the way they are secured.

Much of the protection for inbound email is done through automated barrier protection coupled with end-user education and awareness training. Some of these vendors are very well established in the security sector, and there has been consolidation, especially with peripheral services such as specialist email user security training providers having been acquired by security software and service providers.

The outbound email security sector, on the other hand, has its roots in highly regulated industries and communications where the risk and consequences of data being leaked over email are very serious. It is only recently, with the emergence of regulatory changes affecting all organizations, such as the EU’s GDPR (General Data Protection Regulation), that the sector is generating interest in a wider audience.

Whereas inbound email security can be readily addressed at the entry point into the organization, outbound email directly affects the user and needs to be addressed in their email client, on the email server, and even after delivery. The openness of the internet email system, combined with a diverse array of client devices and forms of access, makes the application of outbound email security a more complex challenge that no single email client provider can readily address. Microsoft’s Outlook may have once been the primary email client in the enterprise market (and indeed remains the dominant player), but the rise of mobile and web-based access and competition to Microsoft Office from the likes of Google’s G Suite have created a market opportunity for outbound email security vendors at a time when organizations are becoming increasingly aware of the risks from outbound email data leakage.

Currently the major email players—Microsoft, Google, and to a lesser degree, Apple—apply minimal controls (e.g., email recall in Outlook). For now, for outbound security, there is a requirement and an opportunity that increasingly need to be addressed, which are agnostic to the email client being used.

The security vulnerability with outbound email is mostly human, is frequently caused by error or sloppiness, but can occasionally be malicious. It must be tackled in a way that is not overly laborious, so that users do not attempt to avoid or subvert it, and equally does not require too much manual administrative intervention to ensure compliance. Applying outbound security involves a combination of

- Building a picture of relationships between content and recipients, based on risk
- Applying tight controls to detect, protect, and remediate

Vendors have emerged using a range of tools including machine learning and encryption, mostly enjoying market success and growth in their home markets (in the US or in Europe), and are now looking to grow their international presence further. This is potentially the time when the market will come to wider attention, and security vendors that have been successful elsewhere, particularly with inbound email, may look to grow their capabilities by acquisition. Otherwise, industry giants may also wake up to and address the need directly. Either way, it is important that outbound email security vendors clearly demonstrate the value they provide to their customers over as broad a variety of use cases as possible.

Key trends in the outbound email security market

Some of the vendors that tackle inbound email security have some sort of outbound protection, but in the main the outbound email market is populated by specialist vendors that have typically initially addressed highly regulated vertical sectors in their own geography. The market might be said to be in the early adopter stage, where products and services meet specific needs but are not quite achieving mass adoption. As the specific needs grow in number and coalesce, or the impact of deployment falls so that it requires less planning and thought, then adoption widens.

This can be a slow process that is suddenly accelerated by a powerful player stepping into the market or when external circumstances force a change. Thus far, none of the major players that might make a difference, in particular Microsoft or Google, appears to show any intentions of doing so, but this may change. If that were to be the case, there might be a sudden rationalization of the number of smaller vendors and acquisitions.

External circumstances may be having a more immediate impact, in that the coronavirus pandemic has accelerated many digital transformation programs. As business processes become digital, the importance of data integrity rises. Legislative changes for accepting remote authorization using suitable technologies may progress more rapidly given the pandemic incentive. This means that technologies for protecting data communications, including outbound email protection, will crop up on the radar for many more organizations than the current, highly regulated sectors.

Future market development

Email security has rightly focused primarily on the inbound threat as technology continues to drive the automation and complexity of attacks, and global connectivity exposes all organizations to greater risk. The strong protective perimeter around organizations would at one time lead many to assume a much-increased level of trust inside the organization compared with outside it. However, even if this was at one time justified, it is no longer the case, and organizations need to take a much less trusting approach to the data traveling over their network and the actions of employees or others operating inside the organization. Issues arise because people might lack training or awareness and make mistakes, some are sloppy, and others cause problems through deliberate actions. All must be addressed.

Outbound email security tackles the thorny issue of insider threat, where data is being compromised or leaked by someone who is already in a position of some privilege, such as an employee or a trusted third party. While this may make its implementation different from that of some security tools, it can also share common capabilities with others, especially with regard to behavioral analysis.

Should outbound email security remain a standalone product or service, or will it merge with other capabilities? There is pressure on the market to consolidate, with vendors increasingly aware of the security tool sprawl problem that CISOs face, and many ideas and technologies that apply to outbound email have benefits elsewhere in other security applications. With that in mind, and the risk that slumbering giants may awaken, it is likely that outbound email security vendors will need to either broaden their impact (for example, to address data leakage from other aspects of collaborative working) or, perhaps, become part of a portfolio of wider capabilities offered by larger players looking to consolidate multiple security capabilities into a single platform.

Vendor landscape

Profiled players

The criteria for a vendor's inclusion in this report are twofold. First, they should be primarily, if not exclusively, focused on outbound email security. Several of the heavy hitters in inbound security also have some degree of capabilities for outbound, but none of them have anything approaching the focus on this problem space that the vendors profiled in depth in this report bring to it.

Second, they should have a major presence in the European market. Omdia wanted to focus particularly on Europe because it has certain peculiarities not found in North America, where many technology vendors originate and are active:

- The overwhelming majority of the companies in this geography fall into the small-to-medium-sized business (SMB) category, which typically does not have extensive security teams, a factor that often conditions the type of technology it deploys.
- The EU has in place the GDPR, a world-leading requirement that countries and regions elsewhere are in the process of emulating, adapting it to their own situations (e.g., the California Consumer Privacy Act, or CCPA). GDPR imposes serious fines for data breaches and can be said to have raised the profile of privacy and protection legislation globally, driving demand for the kind of technology under discussion in this report. As a result, for the last few years, Europe has been the crucible for such legislation, and to paraphrase Frank Sinatra, if an outbound email security vendor can make it there, it can make it anywhere.

Returning to the Omdia view, this report profiles four specialist vendors of outbound email security in depth and rates each of these vendors against the key capabilities identified earlier.

Broadly speaking, any form of protection adopts one of two approaches:

- Applying restraints and prevention measures (think shackles and padlocks)

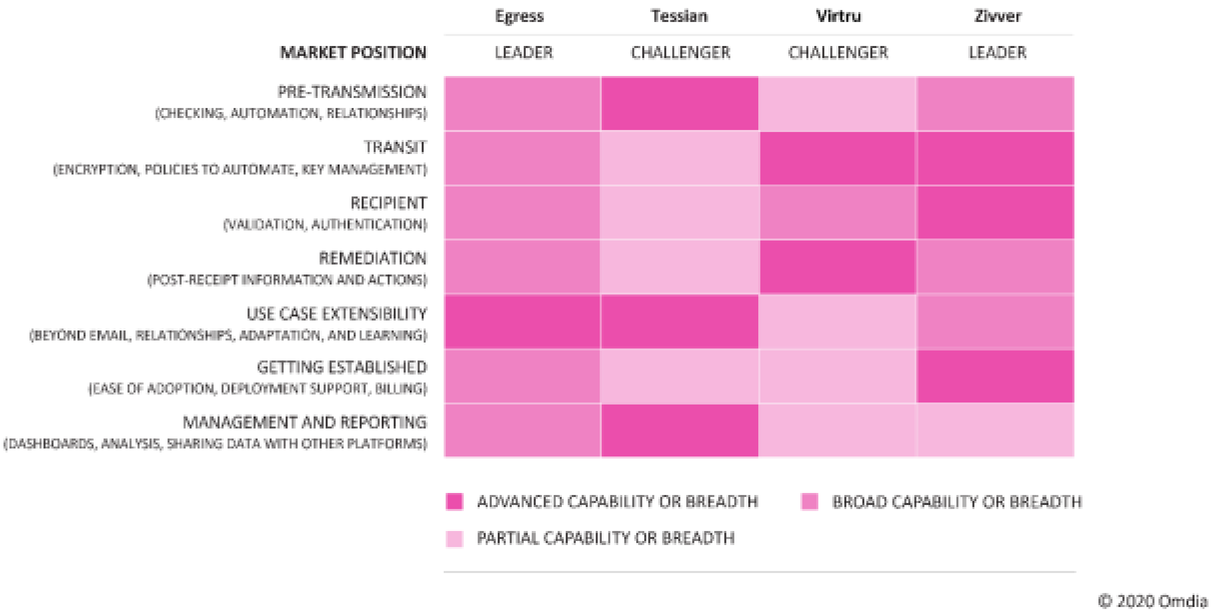
- Keeping a close eye on activities and reacting to anomalies (think CCTV, burglar alarms, etc.)

Both are individually valid and may well be combined in some way.

The vendors profiled in this report fall into these two categories, namely those that approach the problem of outbound email security from a perspective of encryption (e.g., Virtru) and those that come at it by applying machine learning to understand the activity of users and their recipients with a view to taking appropriate action to address all the various forms of insider threat (e.g., Tessian). Egress is something of a hybrid in that it applies machine learning to spot anomalous or risky behavior and then uses encryption as it deems appropriate. Zivver, meanwhile, analyzes communication patterns and based on these, visibly (rather than transparently) corrects possible errors, thereby seeking to educate and inform users in the process about how to minimize future occurrences.

These different ways of achieving outbound email security make it challenging to come up with criteria against which to judge all four of the vendors. There are also slight or nuanced differences in capabilities, so scoring should not be judged as an absolute but as a way to distinguish or show differentiation between approaches. Nonetheless, the report seeks to define requirements that any of the vendors needs to address, ones against which they can and will be assessed by customers (**Figure 3**).

3. Figure 3: Omdia Market Radar 2020: Outbound Email Security



	Egress	Tessian	Virtru	Zivver
MARKET POSITION	LEADER	CHALLENGER	CHALLENGER	LEADER
PRE-TRANSMISSION (CHECKING, AUTOMATION, RELATIONSHIPS)	▨	■	□	▨
TRANSIT (ENCRYPTION, POLICIES TO AUTOMATE, KEY MANAGEMENT)	▨	□	■	■
RECIPIENT (VALIDATION, AUTHENTICATION)	▨	□	▨	■
REMEDIATION (POST-RECEIPT INFORMATION AND ACTIONS)	▨	□	■	▨
USE CASE EXTENSIBILITY (BEYOND EMAIL, RELATIONSHIPS, ADAPTATION, AND LEARNING)	■	■	□	▨
GETTING ESTABLISHED (EASE OF ADOPTION, DEPLOYMENT SUPPORT, BILLING)	▨	□	□	■
MANAGEMENT AND REPORTING (DASHBOARDS, ANALYSIS, SHARING DATA WITH OTHER PLATFORMS)	▨	■	□	□

■ ADVANCED CAPABILITY OR BREADTH ▨ BROAD CAPABILITY OR BREADTH

□ PARTIAL CAPABILITY OR BREADTH

© 2020 Omdia

Source: Omdia

This is a very close market, but Egress and Zivver are identified as *leaders*, having advanced or broad capabilities across the majority of areas. Tessian and Virtru are identified as *challengers*, with partial capability in more than one area.

Each of these vendors is profiled in detail later in this report.

Other players

In addition to the vendors reviewed in depth, there are a number of other vendors offering some degree of outbound security for email systems, and it is useful to list some of these.

Agari

In addition to its antiphishing products Phishing Defense and Phishing Response, Agari also offers an intelligence service around business email compromise called Active Defense and has a product called Agari Brand Protection, which addresses one specific type of outbound exploit, namely domain spoofing/brand hijacking.

This is a form of attack in which someone sends emails as if they came from your organization, which can obviously have serious financial, legal, and reputational implications. Agari addresses this issue with its implementation of Domain-based Message Authentication, Reporting, and Conformance (DMARC), an IETF standard ratified in 2015 for email authentication, which Agari's CEO Patrick Peterson helped to develop.

DMARC leverages two existing email authentication mechanisms, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). It works by enabling the administrative owner of a domain to

- Publish a policy in their DNS records to specify which mechanism (DKIM, SPF or both) is employed when sending email from that domain
- Check the "From:" field presented to end users
- Determine how the receiver should deal with failures

It also provides a reporting mechanism for actions performed under those policies. Agari maintains an Email Threat Center, where it aggregates real-time DMARC statistics from the domains of top banks, social networks, healthcare providers, major government agencies, and other organizations. Agari Brand Protection, meanwhile, provides an automated approach to implementing and managing DMARC email authentication, autogenerating and hosting the relevant DNS records. Its automated workflow is designed to ensures DMARC records are robust, error free, and up to date.

Microsoft

Microsoft is, of course, the 800lb gorilla of enterprise email systems, ever since the on-premises days of Exchange servers. Over the last decade, it has expertly migrated customers across to the cloud-based version of its software delivered as a service, Office 365, which launched in 2011, enabling the company to remain the dominant player in this key market segment.

The vendor has done a lot of work on inbound email security within Microsoft 365 Business, which includes Office 365 Advanced Threat Protection (ATP), a cloud-based filtering service against malware, ransomware, and harmful links, embodied in features such as ATP Safe Links and ATP Safe Attachments. On the outbound side of things, meanwhile, it offers the following capabilities:

- Various message encryption options make sure that a sensitive email to be sent by an employee is encrypted before sending.
- Read Receipts offers the ability to see whether an email has been read by the recipient, an email feature that can be requested by senders but that is not something that recipients are obliged to allow.
- Email systems generally have no default recipient authentication mechanism to determine whether the right person has received an email. However, S/MIME encryption can be used to make sure people other than the recipient cannot read the email (i.e., senders encrypt a message with a public key before sending, and the recipient needs to have the specific private key in place to decrypt the message).

- While automatic revocation of an email is not possible within Office 365, there is a message recall feature, which Microsoft is currently working on improving.
- There are security reports on logins, TLS usage, data leakage, and other features.

Mimecast

Mimecast is best known as a provider of inbound email security, but its Email Security with Targeted Threat Protection service also has outbound features such as data loss prevention (DLP).

There are also extended capabilities that are part of an Internal Email Protect add-on, which applies the same protection for URLs and attachments as per inbound email, but for internal and outbound mail. Its features include

- The ability to detect lateral movement of internal threats via email, that is, from one internal user to another
- Identification and blocking of internal threats or sensitive data attempting to leave an organization's boundaries
- Automated removal of internal emails that are determined to contain insider threats or sensitive data
- Continuous rechecking of previously delivered files to identify and remediate any malware that was not identified before
- Integration into the Mimecast admin console for reporting, configuration, and management

Sophos

Founded in the UK and listed on the London Stock Exchange, Sophos is now led by US executives and is focused on growing its international presence. Unlike many of its competitors with a background in antivirus software, the vendor focuses almost entirely on the business security market.

While best known for its inbound email scanning capabilities, the Sophos Email product also scans outbound traffic, its DLP searching for financial data, confidential contents, health information, and PII in all emails and attachments. It enables security teams to create custom CCLs using Sophos Content Control Lists or to customize out-of-the-box templates for specific CCLs.

The outbound scanning capability also comes with push-based encryption for any sensitive data it encounters. The push approach to encryption has the advantage over pull encryption (where a recipient is sent to a web portal to view the encrypted data) that it is more difficult for hackers to obtain login credentials. On the other hand, once an email has been sent using pull encryption, its contents are mostly out of the hands of the sender, because it is pushed directly into the recipient's inbox, whereas with the pull variant the data remains on a portal controlled by the sender's company.

Sophos Email also has an add-in for Office 365 that lets end users encrypt emails themselves rather than leaving it to their IT department.

Vendors on the Market Radar: Outbound Email Security

On the radar: Egress

Omdia view

While the security risks of inbound email are well understood and could be broadly characterized as malicious actors trying to phish for information or break in, often in an automated fashion, outbound email is more problematic, partly because it directly involves the people inside the organization.

They might have malicious intent too, or be sloppy, or more often, just simply make a mistake. The consequences are similar: data leaks out or is delivered to people for whom it was not intended. Egress provides tools to prevent, protect against, and investigate these outbound email issues.

Email messages can carry very sensitive information or even just moderately sensitive information that would be problematic if it was delivered to the wrong recipients. Even relatively innocuous messages can cause embarrassment (or worse) if sent to the wrong place.

While protecting the organization from malicious incoming messages is a well-established market, with a host of technology vendors offering many products and services, and carriers and service providers automatically filtering out rogue traffic, the market for dealing with outbound messages is less mature. When messages carry less important or nonprivate information, the risks are low, but increasingly, email is a tool for transmitting information that is critical to the organization or would cause data privacy issues if messages ended up in the wrong hands. The volumes of email are huge, while dependency on using email in key business processes is high and shows no signs of diminishing, so inevitably, lapses will occur.

While the stakes have always been high for those in heavily regulated industries, no organization is immune to the consequences of an accidentally misdirected email causing a privacy breach. The standard tools used for email offer little to prevent accidents and even less to stop deliberate malicious acts of, say, a disgruntled employee, so there is an opportunity to avoid such events and protect the organization from negative impact.

Why put Egress on your radar?

People make mistakes and are generally willing to learn from them but can be unreceptive to being forced into new ways of working that they do not understand or appreciate. Egress's Intelligent Email Security Software is focused on the human layer of security. It uses machine learning to identify anomalous behaviors to prevent data leakage, applies encryption to protect sensitive data, and has tools to investigate, analyze, and report on the risks of data sharing.

Highlights

The Egress approach to outbound email security is called Intelligent Email Security and consists of three components:

- **Egress Prevent** to stop data breaches before they happen

- **Egress Protect** to send and receive encrypted email
- **Egress Investigate** to understand, monitor, and report on network security

Egress Prevent identifies anomalous user behavior and applies corrective action. It uses machine learning to build a picture from historical email records and ongoing inspection to continuously monitor behavior. A risk assessment is built by analyzing the recipient's domain for authenticity and historical communications, the sender's history, specific geographic and system information about the recipient, and the content of subject, message, and attachments. From this, Egress Prevent provides a quantifiable risk assessment as a numeric score within the email client, using this to dynamically apply appropriate protection and guide against misdirected emails.

It uses an add-on in the Outlook client, in combination with an email gateway, to support Outlook Web Access and mobile email from iOS and Android. The Outlook add-on provides immediate user feedback and guidance on anomalous behavior, for example, if inappropriate recipient email addresses are typed or autocompleted.

Activities are logged, and administrators can track sensitive data; risks to regulatory compliance; and users that may be at risk, may require too-frequent assistance with misdirected emails, or may be attempting to intentionally leak sensitive data.

Egress Protect uses AES-256bit encryption to secure email message content and attachments. This also includes the ability to share files larger than the size limitations normally imposed by Microsoft Exchange. Encryption can be selected by a single click or applied by policy and performed at the Egress email gateway, or in Outlook, at the desktop. Encrypted messages can be sent and received via Egress's mobile apps and its online web reader as well as from Outlook.

Egress's Smart Authentication functionality assesses the recipient's domain, geographic location, and system information to determine a level of trust. This is then used for either

- Seamless authentication of the recipient, granting them automatic access to the Egress-encrypted message if the risk is deemed low
- Requiring that the recipient log in to an account they have created on the Egress system or else provide some form of multifactor authentication if the risk assessment is high

Egress supports a number of authentication methods to authenticate recipients. These include single sign-on, Active Directory, and SAML and OAuth providers.

Email recipients can reply to and initiate secure emails and file transfers to Egress subscribers at no cost to themselves.

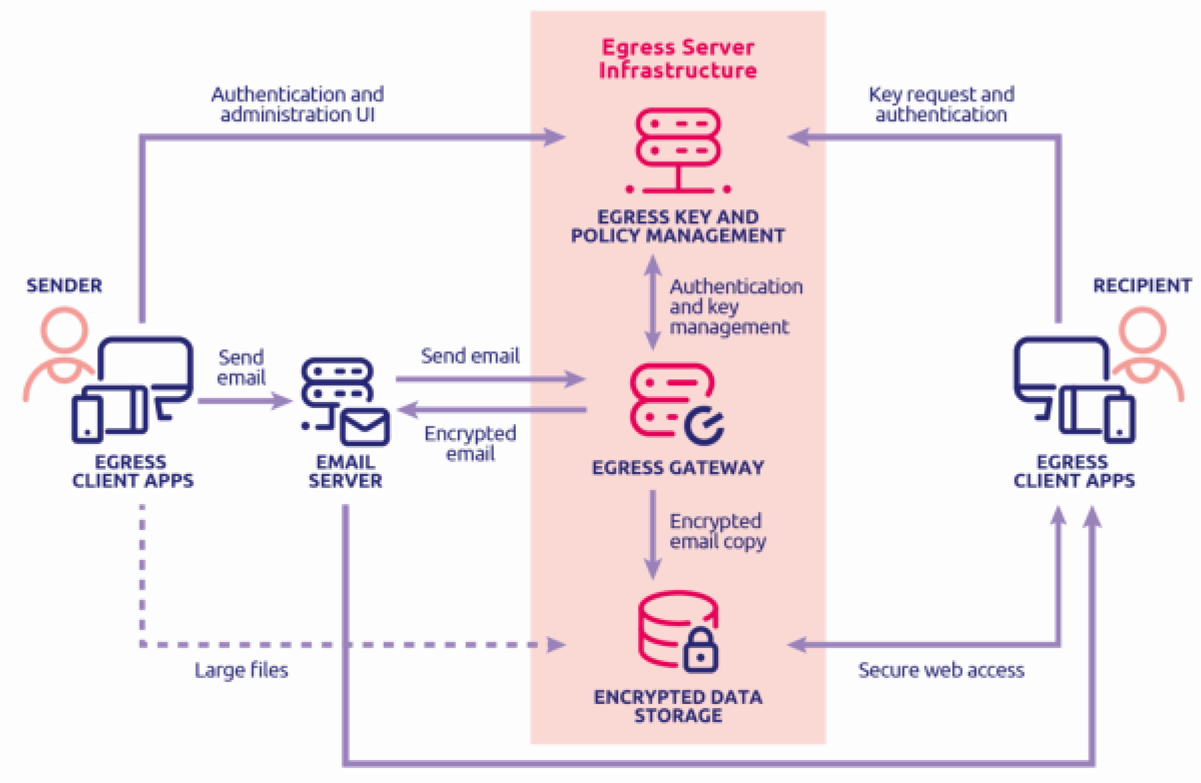
Egress provides a range of APIs within the Protect platform, covering the following functions:

- Encryption and decryption of email messages
- Custom authentication methods and providers
- Managing policies within the Egress solution
- Providing access to logs and system events

The platform can be provided in white-label mode, enabling the enterprise customer to brand it as its own and give it a look and feel in keeping with other internal applications, and Egress provides a full audit trail with all actions taken on email messages, including encrypt, decrypt, revoke, replies, and expiry, logged in detail and made available to both users and administrators in the form of reports.

Egress Investigate provides secure search capability, analytics, and insights into email communications, both plain text and encrypted, through a graphical dashboard interface for compliance and reporting. Email data is indexed so it can be rapidly searched, with graphical controls to initiate automated redaction of sensitive data before exporting results and the obscuring of nonpertinent sensitive data in Subject Access Requests.

4. Figure 4: Egress approach to outbound email security



Source: Egress

Background

Egress was founded in October 2007 by CEO Tony Pepper, COO Neil Larkins, and chief science officer John Goodyear. The three founders previously worked together in senior roles at Reflex Magnetics, a data security company that was later acquired by Checkpoint Software Technologies. Reflex Magnetics offered products that secured against data exfiltration via removable media as well as email encryption.

Egress has raised $47.4 million in three funding rounds, the latest being a Series C round for $40 million in December 2018, led by FTV Capital.

Current position

Egress Intelligent Email Security comprises three modules, Prevent, Protect, and Investigate, which are available separately with subscription on a per user mailbox per year basis. They are also bundled together, with all three elements being the main bundle, and some customers opt for a bundle of Egress Prevent and Egress Protect. There is an Outlook client add-on that can be downloaded and mobile clients for iOS and Android, and the gateway platform is provided as a service. Egress partners with four service providers:

Microsoft Azure, Amazon Web Services (AWS), UKCloud, and UKFast. Egress can be trialed free or used free by recipients after they have registered for a free Egress ID. This comes with 25 free credits; each one allows an encrypted message to be sent or shared to another non-Egress customer's email address.

Egress's first security solution for email encryption, now known as Egress Protect, was launched in March 2010 and was adopted initially by local authorities in London before spreading to other public and private sector customers. The product now known as Egress Prevent was launched in March 2016, and the reporting and analysis model, Egress Investigate, was launched in June 2017.

In August 2020, Egress launched Investigate 365 in the Microsoft marketplace. This tool is free to run for 14 days, and it analyzes 12 months of data to investigate misdirected emails, unverified TLS, and DLP policy violations in up to 100 mailboxes and can thus serve to stimulate demand for the licensed products.

The company also offers secure file sharing and collaboration products, namely Egress Secure Workspace for controlled and audited data sharing workflows and Egress Secure Web Form for secure content upload.

Analyst comment

Egress has most of its existing customers in the markets, such as financial services and healthcare, that have been driven by regulatory pressures for better outbound email security protection. However, it has also had success in other use cases for guarding against email sensitivity such as "ethical" walls that need maintaining between different parts of an organization (e.g., in law firms) and profanity protection. While these may not appear to be typical security issues, they are becoming increasingly important in a globally connected world. Tackling these diverse use cases, which spread beyond regulated sectors into other areas, will be important for growing the market. Egress appears to recognize this and has embarked on research and marketing campaigns to highlight and raise awareness of, for example, the high levels of GDPR breaches caused by accidentally sent emails.

Understanding and reacting to user behavior, historical as well as current activities, will become increasingly prevalent as the use of machine learning continues to grow. Egress has a good foundation on which to grow its capabilities or find a partner with greater market presence to feed those capabilities to a wider market.

There is a risk in being a smaller or specialist company next to the industry email giants such as Microsoft or Google, which in theory could at any moment awaken to the challenges of email security. However, despite some internet protocol standardization and the market dominance of certain email clients, there is still variety, and it is hard for a single player, even an industry giant, to take on all the necessary third-party integration. Egress is a Microsoft Gold Partner, and there is space in the Microsoft ecosystem for expertise that addresses specific needs.

Table 1: Data sheet: Egress

Product/service name	Egress Intelligent Email Security	**Product classification**	Outbound email security (DLP, encryption)
Version number	5.50	**Release date**	August 2020 (latest version)
Industries covered	Finance, legal, healthcare,	**Geographies**	EMEA, North America

	government, emergency services	**covered**	
Relevant company sizes	All	**Licensing options**	Per user subscription
URL	www.egress.com	**Routes to market**	25+ users: channel model Under 25 users: direct
Company headquarters	London, UK	**Number of employees**	250

Source: Omdia

On the radar: Tessian

Omdia view

The ease with which email can be used by anyone to share information, widely and to anyone else, is hugely powerful but also a source of significant risk. This risk comes not from the technology but from the people who use it for the relationships they have with others through their communication flows. Unlike inbound threats, where deliberate attacks are made, outbound email security lapses are caused by a range of internal human actions (deliberate or, more often, inadvertent) during normal working activities. Tessian uses machine learning to better understand email communication and relationships to bolster an organization's outbound email security against risks caused by human errors, sloppiness, or malicious intent. It also understands inbound email behaviors to apply protection against spear phishing, business email compromise (BEC) fraud, and targeted impersonation attacks.

Rigid organizational structures, processes, and procedures are being challenged by the ease with which anyone can readily communicate with anyone else inside or beyond their organization. Email is the default mechanism and medium for many workflows. While more structure and better controls might be preferred by the organization, individuals are very comfortable with the flexibility of email. Increasingly, perhaps, too comfortable in fact, which is why inbound email is such an important line of defense against malicious intent.

However, while there are no external adversaries to identify, the insider threat to confidentiality, privacy, and sensitive data should not be underestimated. Despite there being little default protection in the major email platforms, such as from Microsoft or Google, organizations could and should do much more to protect themselves from outbound email data leakage.

The question is: How? Technology can authenticate recipients and protect data in transit, but it has to be used in a way that does not undermine or impinge on the easy and flexible information sharing that email users expect. Ultimately, email is about the flow of information between people, so another way to defend against errors or malicious use is to better understand the flow of user behavior and look for anomalies.

Why put Tessian on your radar?

The power of email comes from its ability to connect people and to share information between all types of organizations. Most people will try hard to do the right thing, but accidental mistakes happen; sometimes people are sloppy, and sometimes they are deliberately malicious, and emails with sensitive information can be sent to the wrong place. Tessian's approach, using machine learning to understand normal behaviors, the context of specific recipients, and message contents themselves, means anomalies can be detected and data leakage, accidental or otherwise, prevented.

Highlights

The Tessian Human Layer Security platform is based on its "human layer security engine," which uses content and relationship analysis and machine learning to identify behaviors. Rather than start with prebuilt rules, it turns existing historical and real-time email data and continuous monitoring into the intelligence required to apply security, using content inspection of messages, and builds a stateful map of the relationships between senders and recipients. It continues to learn over time as the network of internal and external employee contacts evolves and grows with new projects and changing business needs.

Every email carries a wealth of metadata to define the context of the relationship and communication. In addition to the basic delivery information (email header, sender and recipient email addresses, IP address, subject line, time stamp), there is derived information such as domain reputations and recurring identifiers in content such as salutation, project names, sign-offs, and signatures. If there are attachments present, additional intelligence can be gleaned from them, including names, content type, project names or identities, and encryption status. All of this together builds a contextual map of normal behaviors, which can be used for real-time analysis and detection of anomalous behavior to prevent threats, whether inbound or outbound, to email security, which Tessian offers as a series of modules, all of which are deployed on a common underlying platform:

- **Tessian Guardian** addresses the accidental data loss that is usually caused inadvertently, or perhaps sloppily, by employees going about their normal day-to-day activities. This is the most common type of data security incident reported to data protection regulators: people get tired, or autocompletion in software can lead to incorrect recipients or content attachment. Tessian Guardian (and all of its modules) deploys into the email stack on top of existing secure email gateways and all enterprise email environments (Office 365, G Suite, MS Exchange) and provides automatic protection within 24 hours of ingesting historical email data and building employee relationship graphs from it. These graphs evolve and adapt as the machine learning continuously monitors ongoing email activity, and real-time anomaly detection alerts users with contextual warning messages, with precise reasons for the alert and guidance (e.g., predicting correct recipient) before emails are sent so that errors can be rectified. Tessian Guardian's alerts are invisible to the end user until a misdirected email is detected, resulting in a nonintrusive user experience and data loss prevention without alert fatigue.
- **Tessian Enforcer** protects against the deliberate exfiltration of data, perhaps by sloppy or malicious action, over email. It is powered by the same human layer security engine as all Tessian modules and so analyzes millions of data points for every outbound email, detecting anomalies that indicate data exfiltration might be taking place before any data leaves the organization. It includes employees' business and nonbusiness (e.g., personal) email accounts, which it can automatically detect from historical email data. Responses to block emails, warn users, or silently track the event can be set depending on the organization's policies. It is invisible to the end user until potential data exfiltration is detected.
- **Tessian Constructor** allows organizations to implement custom filters to prevent breaches of regulatory compliance or specific internal policies such as ethical walls, restrictions on the use of abusive language, or attempts to send particular types of sensitive information outside the organization. Filters can be narrow or broad in scope for individuals, teams, or the entire organization and can be triggered by content, attachment sizes, recipients, and so on. When

noncompliant activity is detected, based on the organization's policies, the message can be blocked and the sender warned with a message to alert them as to why it was not compliant or silently tracked with metrics reported back to security teams through the HLSIvisual dashboard.

- **Human Layer Security Intelligence** (HLSI) provides visibility into the threats being detected in specific categories (misdirected emails, data exfiltration, and inbound BEC and other targeted impersonation attacks) and actions undertaken by the Tessian platform. It identifies and displays threat insights, including benchmarking against peers; supports threat investigation with prioritized lists, detailed threat breakdowns, logs, and APIs for integration with SIEM and SOAR platforms; and has tools for threat remediation including automated domain blacklisting, quarantine, and postdelivery protection.
- **Tessian Defender** is the vendor's inbound email security module, using the same human layer security engine as the rest of the portfolio to prevent spear phishing, BEC fraud, and targeted impersonation attacks. In addition to turning organizations' email data into intelligence to detect inbound attacks, it uses Tessian's global threat network, an anonymized database of all forms of targeted impersonation attacks detected by Tessian, to prevent threats never seen before within an organization. When unsafe emails are detected, it alerts users with contextual warning messages, with precise reasons why the email is unsafe, thereby educating users.

With regard to additional security for emails while they are in transit between the sender and recipient, companies using any of the vendor's outbound modules with its agents and, potentially, the Outlook add-in, rely on the security provided by the Office 365 or Gmail service itself. If, however, they use the Tessian Gateway in order to protect emails sent from mobile devices, the emails are scanned in transit and are relayed from Gateway to client server using SMTP. All SMTP connections between servers use opportunistic TLS by default. There is also an option to force TLS-only connections if desired; that is, the user can set the system up always to send TLS-encrypted messages and can then change it manually, in an ad hoc manner, to go over to opportunistic TLS if they prefer.

As for authentication after transmission, it is performed on the Tessian Gateway when SMTP connections are received; this uses both IP white-listing and sender/recipient domain checks before allowing the connection to proceed. IP white-listing is also performed by the client's server when the SMTP relay connection is received back from the Tessian Gateway.

Reporting, analytics, remediation, and audit trails

Tessian offers management and reporting via HLSI online portal, exportable PDF reports, API integration for SIEM/SOAR, and regular email alerts. Tessian argues that a key differentiator is that it does not require any configuration: it operates automatically, using machine learning and historical data. If desired, configuration options are available, and these can be operated via the portal.

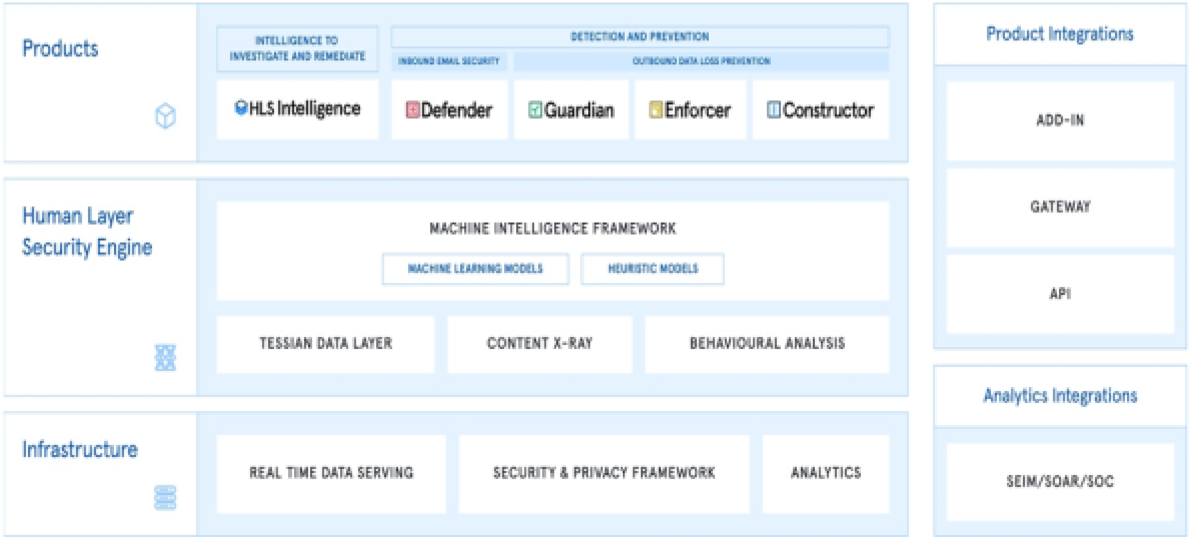
Analytics pages in Tessian's HLSI portal display aggregate statistics, showing how threats are being mitigated and how risks are changing over time, and display benchmarks against peers. Users can also carry out investigations within HLSI portal by drilling down into specific security events detected by Tessian's products. Events include both high-risk users and individual emails.

Various remediation and reporting options are available for events, including quarantine, mailbox claw back, and single-click deny lists. Users can export data from the HLSI portal in PDF format for reporting purposes, and security events can be exported by API to SIEM or SOAR platforms.

The Tessian HLSI portal offers monitoring for Tessian integrations to flag any potential issues. There is also auditing functionality that allows customers to track key configuration changes made by administrators.

As for audit trails, every email that is deemed a potential threat by Tessian is logged and made available in the Tessian HLSI portal, in xlsx reports, and via API for SIEM/SOAR. The reports show a number of details including the sender, recipients, action taken after seeing the initial warning, and the eventual outcome of the sending of the email.

5. Figure 5: Tessian approach to outbound email security



Source: Tessian

Background

Tessian, originally called CheckRecipient, was founded in 2013 by Edward Bishop, now CTO; Thomas Adams, now head of client-side engineering; and Tim Sadler, now CEO. The three founders were engineering graduates of Imperial College in London who, while working in the financial sector, realized how often and easy it was for sensitive information to be accidentally emailed incorrectly or to the wrong recipients.

It has raised a total of $58.7 million in seven rounds of funding, the latest a Series B round for $42 million in January 2019, led by Sequoia Capital.

Current position

The Tessian Guardian, Enforcer, and Defender modules are available separately on a per user per year subscription basis. Deployment uses agents and a lightweight Outlook add-in. There is also a Tessian Email Gateway, which protects mobile email users. Tessian Guardian was launched in 2016, with the Gateway added in 2017.

Whichever protection modules are chosen, all come with Tessian HLSI built in. This provides insights and detailed reports on misdirected emails and data breaches detected and prevented.

Sales focus is in EMEA and the US and all through direct sales. The information gathered by Tessian is email metadata and is stored in Dublin (for the European market) and in the US.

The machine learning is not limited to, but is most performant in, the English language. However, Tessian finds that for its target customers, business language is mostly English anyway.

Analyst comment

Tessian's underlying approach differs slightly from those of other players in the market. Its behavioral analysis using machine learning has been applied to both inbound and outbound email security, meaning that it can gather all information related to email relationships with a common platform. As a platform based on machine learning, context, and relationships, it might also be considered complementary to other email security products and services, such as those focused more on encryption.

It also has a strong marketing message about relationships and networks of individuals, recognizing that the intelligence from email metadata is a significant asset. This might make it a more attractive proposition for a large market player looking to add preventive user-behavior analytics capabilities to its portfolio.

However, there are challenges in a number of aspects. The assumption that the language of business is mostly English is understandable, especially for a US-headquartered company, but it may limit future market opportunities, as may the strategy for the storage of data in Dublin for Europe. While this is only email metadata and not the content itself, some sensitive organizations and territories may require a more local and cautious approach to their metadata, even if EU regulations do not mandate such an approach.

While the company sells only direct at the moment, it has been looking into channel options. This may be useful not only to grow sales but also to broaden the strategy and help address other markets beyond the US and EMEA.

Table 2: Data sheet: Tessian

Product/service name	Tessian Human Layer Security Platform Products include: Outbound Email Security: Tessian Guardian, Tessian Enforcer, Tessian Constructor Inbound Email Security: Tessian Defender Human Layer Security Intelligence	**Product classification**	Email security Inbound and outbound email security Data loss prevention Human layer security
Version number	n/a	**Release date**	2015
Industries covered	Technology, legal, financial services, healthcare, manufacturing	**Geographies covered**	UK, US, Nordics, South Africa, Asia Pacific, Middle East
Relevant company sizes	All	**Licensing options**	Subscription
URL	www.tessian.com	**Routes to market**	Direct
Company headquarters	San Francisco, CA, US; London, UK	**Number of employees**	150+

Source: Omdia

On the radar: Virtru

Omdia view

Email has become ubiquitous, with access growing from a client application on a desktop computer to encompass all sorts of mobile devices and email access delivered as a cloud-based service. This brings many security challenges and privacy concerns. While inbound email and the risk of introducing malware is a widely known threat, the risks around data loss and leakage when emails are sent (i.e., outbound email security issues) are less widely discussed.

Virtru tackles these outbound risks through encryption and authentication to ensure that those sending emails have sufficient and effective control over who can receive, access, and view them.

Much corporate email traffic will typically be oriented around the use of Microsoft Office365, Outlook, and Exchange, but other cloud-based services, such as Google's G Suite, are being adopted, initially in the technology sector but also elsewhere, as the scalability and flexibility of cloud-based services outweigh security concerns. While inbound email security is widely addressed by organizations and enhanced by carriers, service providers, and networks employing, for example, automated spam filtering, outbound protection is something an organization needs to put in place itself. This is no simple matter, because if it is seen as too intrusive or difficult to apply, users will simply find another way of getting their job done, even if it compromises security.

Outbound email confidentiality and the risks of data leakage may be well understood in tightly regulated and security-conscious sectors such as government, financial services, and healthcare. However, all organizations need to be aware of the implications and impact of data privacy, especially with the growing number of consumer protection regulations and the risks to intellectual property in globally connected supply chains. The challenge increases as more people work from home or in comfortable environments where their guard may drop. Having put protection in place for inbound email threats, more organizations need to consider how they address outbound email confidentiality and control.

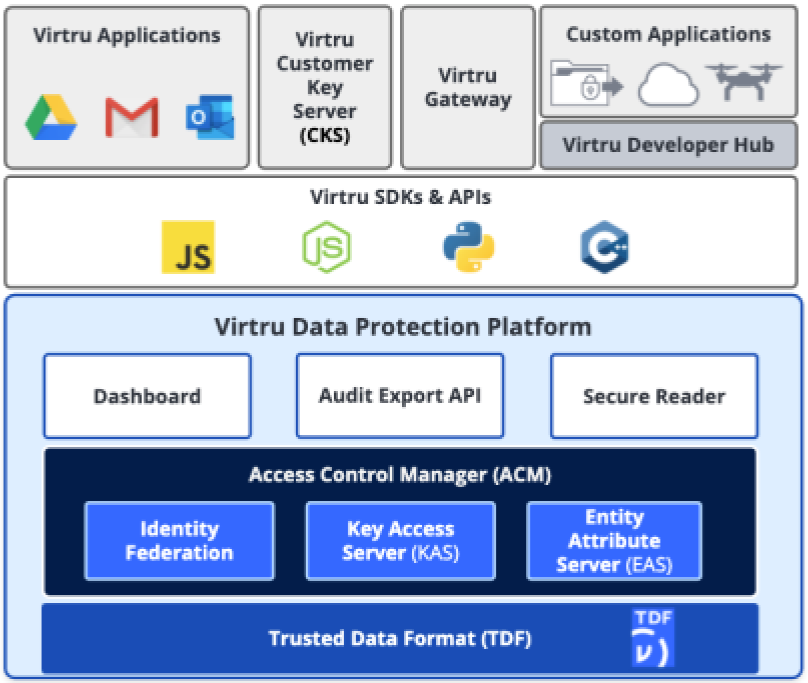
Why put Virtru on your radar?

Virtru applies end-to-end encryption and confidentiality controls to outbound email. The protection of Google accounts only applies to a smaller market of email users at the present, but in combination with controls for Outlook, it extends Virtru's appeal to organizations of all sizes including traditional markets such as federal government and healthcare and newer ones such as cloud-native and highly distributed organizations.

Highlights

The approach adopted by Virtru focuses on data protection through object-level encryption to provide end-to-end security. It is based on the Virtru Trusted Data Platform (TDP), which supports the applications for encrypting email and custom applications. At its heart is an Access Control Manager (ACM), which allows organizations to set, manage, and enforce policies. The ACM hosts encryption keys, manages policies, and brokers the authentication and authorization workflows. Encrypted data is stored separately from the encryption keys protecting it, and the TDP supports a zero-trust model where all system components are continuously authenticated, verified, and authorized (see **Figure 6**).

6. Figure 6: Virtru approach to outbound email security



Source: Virtru

Information access and management is via a dashboard providing visibility of all protected data, access, users, and groups along with content rules and configuration. There is an API for exporting logs of all protection, access, control, and administrative activity for integration with SIEM tools and security operations center (SOC) operations for monitoring, analysis, or compliance.

Tracking reads and revoking

Once an email has been sent, the sender can see who has read it and seen any attachment from their sent folder, where open green message icons are shown for those recipients who have opened it and closed gray message icons for those who have not. They can also get this information from their personal Virtru dashboard, while admins get the same level of information, but across all a company's users.

Message revocation is also enabled from within both the user's sent folder and their dashboard, with the user pressing a red hand ("stop") icon to revoke the message for a particular recipient.

Virtru currently has no mechanism for a sender to authenticate a recipient, because authentication is required on the individual user level before access to secure content is granted, which is how the system validates that the person accessing is the intended recipient (i.e., validation rather than authentication per se). That said, the recipient will be asked to authenticate through Virtru's Secure Reader, either with their Gmail/Outlook credentials or via a verification link/code sent to their inbox.

Auditing

The aforementioned ability to track who has read an email and any attachments is, of course, one dimension of auditing the system. In addition, all user and administrator activity around data protection, sharing, access, and control policies is logged continuously. Administrators can export these logs for analysis using the analytics tool of their choice or configure an API integration to feed these logs into their SIEM solution, combining Virtru activity data with other security event data for correlation, predictive analysis, and forensics.

Trusted Data Format

The Virtru TDP is underpinned by Trusted Data Format (TDF), which is an open standard providing attribute-centric, object-level encryption that connects encrypted data to policies and metadata to ensure that protected data can only be accessed by authorized users. This provides fine-grained access control and protection that travels with the data and can be shared across any device or platform. Virtru has a software developers kit enabling third parties to build applications to embed discrete policies and rules for their data into their own custom workflows. This could be particularly useful in applications requiring persistent, secure, multiparty control of large amounts of data in applications such as managing Internet of Things devices, secure analytics across multiple separate datasets, and contact tracing.

Virtru uses the TDP as the base to provide its own applications for encryption in Outlook, Gmail, and Google Drive. These applications allow for secure sharing of email messages, attachments, and files with end-to-end encryption and persistent access controls. They also allow for access to be revoked, messages to expire, forwarding to be disabled, and the attachments of watermarks so that it is clear where content has been sent in the event of data leakage. Policies can be set to use automated admin-defined rules for organizationwide controls or by individuals taking control of individual messages.

Securing the data through separation of keys and content

Virtru uses a split-knowledge approach to data protection, where content and encryption keys are stored separately so that only authorized parties can access unencrypted content. This architecture ensures that Virtru can never access unencrypted content or decrypt user content outside of customer-controlled Virtru clients. Only recipients authorized by the content creator can access and decrypt protected content.

Virtru's zero-trust approach ensures the separation of keys and content at all times. In instances when Virtru has the keys, it cannot access the content; when Virtru services have the content, Virtru does not have access to the keys.

Furthermore, with the Virtru Customer Key Server, an added layer of public-private key pairs hosted on the customer's premises are used to rewrap (or double encrypt) the first layer of keys to give customers even more control and protection against unauthorized third-party access.

User interfaces

The system is designed for ease of administration through the dashboard interface, so users have access to all the features without needing new email accounts or passwords. For Gmail there is a browser extension for the Google Chrome browser (which can be user installed) and an add-on for Outlook users. There are separate mobile apps for iOS and Android to allow users to send or read protected messages. For nonusers, such as those outside an organization, there is a secure web-based reader for receiving and reading protected messages and attachments. This can be branded by the sending organization, and all nonusers have to authenticate and reauthenticate each time they want to access the content. Copying and forwarding is restricted, and documents have a persistent watermark based on the recipient's email address.

Background

Virtru was founded in 2012 by CEO John Ackerly and his brother, CTO Will Ackerly. Before founding Virtru, John Ackerly was an investor at private equity firm Lindsay Goldberg LLC and had previously been responsible for technology policy at the White House and policy and strategic planning director at the US

Department of Commerce. Will Ackerly was a specialist in cloud analytics and security architecture at the National Security Agency (NSA), where he invented the TDF, the open standard for the secure transfer of data that forms the basis of Virtru's technology.

The company has raised $76.8 million in funding over five rounds, the most recent being a Series B round led by ICONIQ Capital for $37.5 million in May 2018. Further investors include Bessemer Venture, NEA, Samsung, Soros Capital, and Blue Delta.

Current position

Virtru announced its encrypted email and privacy service in January 2014 for popular email services and clients including Gmail, Yahoo, Outlook, and Mac Mail. The concept at this point was to give private individuals the power to secure their email messages, rather than encryption being perceived as the preserve of highly trained engineers and security experts. It extended the service to Microsoft 365 in March that year, launched its encrypted email app for Android in June, and extended the services with Virtru for Business to include organizations using Google Apps in July 2014.

In December 2016, Virtru was recognized by Google as recommended encryption for G Suite applications, and in July 2018 it teamed again with Google to bring end-to-end encryption to Google Drive.

While the company had an initial focus on the individual, it has since enjoyed success across regulated industry sectors and midsize to large enterprises, with currently over 20,000 organizations as customers from SMBs to federal government and Fortune 50 companies.

Virtru has a large customer footprint in the US with a growing presence in EMEA, where the focus is initially on the UK and France.

It sells direct but has also had some success with resellers and consultants, in particular around Google's G Suite. Virtru is Google's recommended supplier for encryption.

There is a flat fee for the platform itself, which is offered in three tiers (basic, intermediate or enterprise) and then a subscription per user per year, for the email or file encryption application.

Virtru has active technology partnerships and integrations, mostly built on TDF, with Atos TrustWay Hardware Security Module, WireWheel's portal, Titus, FireEye's Helix Security Platform, Intel Data Guard, Ionic, CloudMigrator, and McAfee.

In August 2020 Virtru formed a partnership with inbound email security vendor Area 1 Security. The companies will supply a joint offering comprising Virtru Email Protection and Area 1 Horizon, through both direct sales and each other's channel partners.

Future plans

Virtru's product developments in the near term include improvements to the visibility of the admin data and the addition of audit and visualization capabilities. The company also plans to offer a new secure file-transfer capability that will build on its Google Drive offering to expand its footprint in the file protection market. This will support secure file-sharing workflows independent of a specific client to allow organizations to enable both inbound and outbound file sharing with all of the persistent protection and granular access controls that are part of the Virtru platform.

Analyst comment

The core encryption platform is flexible and powerful, as would be expected given the vendor's background in US federal government and its initial market focus on regulated industries. Extending the platform's email encryption usage to include Gmail as well as Outlook users may not immediately offer large numbers of extra customers, but Gmail has a lot of noncorporate users, and G Suite overall is growing in popularity, although in the early stages this seems more prevalent in the technology sector.

The challenge for Virtru, as it is for all companies operating in this sector, is staying relevant if the larger email companies become more active in securing outbound email. For Virtru, its relationship with Google in particular would appear to be key.

Table 3: Data sheet: Virtru

Product/service name	Virtru Data Protection for Email (Gmail and Outlook)	**Product classification**	Email encryption; data protection
Version number	Gmail: V7.17.0.0 Outlook: v3.10	**Release date**	Gmail: initial v1 released January 31, 2013 Current version released July 18, 2020 Outlook: initial v1 released July 22, 2014 Current version released November 11, 2020
Industries covered	All, with a focus on regulated industries with consumer and corporate privacy concerns: healthcare; federal, state and local governments; education; and manufacturing	**Geographies covered**	All, but with a focus on North America and EMEA
Relevant company sizes	All, with a focus on 1,000+ employee organizations (midsize to enterprise)	**Licensing options**	Annual per user subscription
URL	www.virtru.com	**Routes to market**	Direct sales (North America and EMEA focused) and cloud solution consultants and resellers (e.g., MavenWave, Damson Cloud)
Company headquarters	Washington, DC, US	**Number of employees**	~100

Source: Omdia

On the radar: Zivver

Omdia view

Email can be a source of accidental or deliberate data leakage, and the communication demands of highly regulated sectors are one of the reasons why legacy technology such as fax is still being used to authenticate senders and recipients and protect the privacy of shared information. Zivver offers comprehensive and email data protection and secure file transfer, which deliver similar benefits, that users should find easy to use and can put them in control of the information flow process.

Sharing of information has never been easier, and despite numerous alternatives, email is still the common, simple, and preferred option for many. Its simplicity brings problems, however, and although additional measures have long been available to add some security to email messaging, they are often cumbersome or do not cover all aspects of the email process.

As well as the risk of a message being snooped on in transit, the lack of guaranteed authenticity of sender and recipient is a problem, as anyone who has ever had their email account hacked or received an email from a hijacked account will understand. This is a particular issue in highly regulated sectors such as legal, healthcare, and insurance, where there is the risk of not only reputational damage but also significant fines. The use of old but secure fax technology is still prevalent, but it lacks the flexibility that is an increasingly common requirement and introduces unnecessary cost and complexity.

It is in these highly regulated markets in particular that the need for outbound email security, to protect against sensitive data leakage, has been most pressing and, therefore, also where dedicated outbound security vendors have enjoyed most uptake to date. However, as regulations protecting data privacy strengthen, and the risks as well as fines increase, it is inevitable that more organizations will need to apply better controls to the messages that are being so simply and frequently sent from within.

Why put Zivver on your radar?

The insider threat of accidental, negligent, or malicious transmission of sensitive data via email to the wrong recipients is something that all organizations will recognize as a problem. For some it will be more critical, especially in terms of regulatory compliance where secure and authenticated communications are required. Zivver secures outbound email, calling what it does email data protection, with an emphasis on educating and enabling users and keeping the user experience simple to help them make better decisions.

Highlights

Zivver protects email data by monitoring email messages, attachment content, and recipient addresses, with a focus on enabling users, educating them with good practices, and supporting them to make better decisions about their use of this particular communication method. It does this through the entire process—before, when the email is being composed; during transmission; and after—ensuring that the content is only read by the right person. Multiple measures are employed at each stage:

- **Before.** Recipients, message content, and attachments are monitored, and the sender is alerted to a potential risk or mistake before the mail is sent. The system checks the sensitivity of the information in the email and whether the particular recipient has received that type of sensitive information before; if not, it warns the sender. This helps prevent accidental delivery to the wrong recipient caused by “helpful” autocompletion functions in email clients. In addition, it helps to make users aware of sensitive content in emails (e.g., social security numbers in attachments), warns users about potential misuse of To and CC, and helps employees protect information of a specific sensitivity type according to company policy.

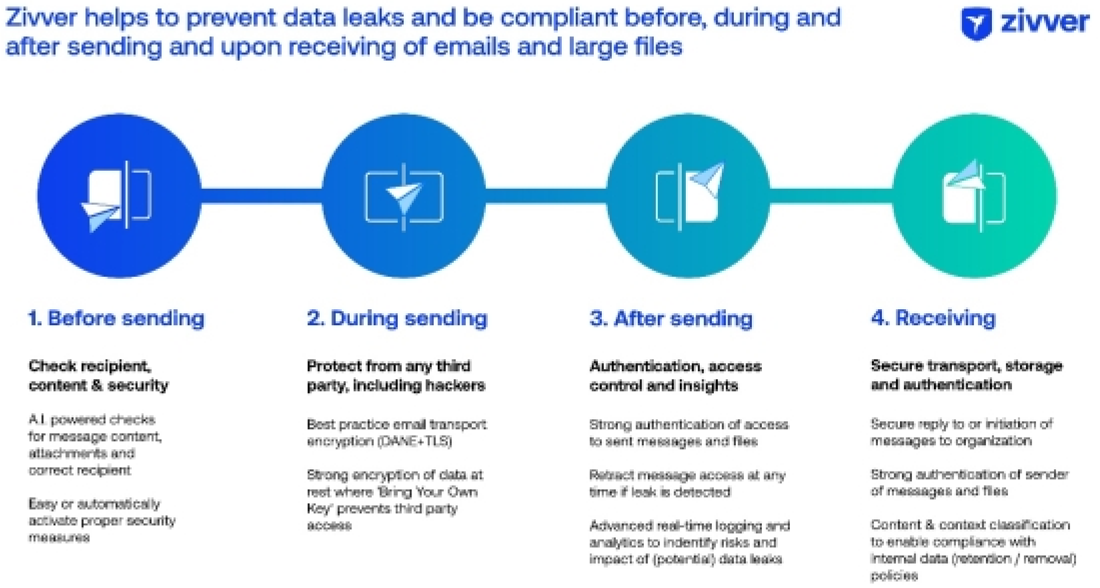
- **During.** Message content and attachments are secured, both in transit and at rest, with a combination of public/private key encryption, where Zivver does not have access to the private (decryption) keys. Recipients are always subject to confirmation, including two-factor authentication (e.g., Zivver sends an SMS code to recipients). If large amounts of data need to be sent, Zivver offers the secure sharing of attachments of up to 5 terabytes of data. This avoids the risk of using cloud-based data repositories to share data without an audit trail of what has been shared.
- **After.** Zivver offers out-of-the-box recipient authentication options, such as sending automatic SMS codes, to prevent unauthorized access. Additionally, emails can be revoked if they are later discovered to have been sent inadvertently, and Zivver gives insight into which recipients have already accessed the message and which have not, thus alerting to the impact of a mistake. Messages can also be given an individual expiration date to comply with the organization’s data retention policy.

These actions can ensure data loss is prevented by minimizing both external and insider threats, whether deliberate or accidental. Zivver also tracks and aids data-breach reporting, which is useful for improving compliance and, ultimately, reducing the consequential costs of breaches.

To extend its use and value to those without a Zivver account, anyone can receive, reply to, copy, and download secure email messages from a Zivver account user. For each such email, the recipient receives a notification to direct them to a secure guest environment. To initiate secure external messaging to those without accounts, there is an add-on to a Zivver subscription for users to be able to link a Conversation Starter to their account by placing a secure email link in their signature. External connections can then also send private information within the secure email environment.

Organizations can personalize their use of Zivver so that external recipients see a corporate-branded guest environment with the name of the sender, their organization’s logo, and an optional personalized message at the foot of the email. After unlocking the secure message, the recipient enters the conversation page, which also reconfirms the source by displaying the sending organization’s visual identity. While this is an opt-in feature, it is useful to help make clear the originating organization of the message.

7. Figure 7: Zivver approach to outbound email security



Zivver helps to prevent data leaks and be compliant before, during and after sending and upon receiving of emails and large files

zivver

1. Before sending

Check recipient, content & security

A.I. powered checks for message content, attachments and correct recipient

Easy or automatically activate proper security measures

2. During sending

Protect from any third party, including hackers

Best practice email transport encryption (DANE+TLS)

Strong encryption of data at rest where 'Bring Your Own Key' prevents third party access

3. After sending

Authentication, access control and insights

Strong authentication of access to sent messages and files

Retract message access at any time if leak is detected

Advanced real-time logging and analytics to indentify risks and impact of (potential) data leaks

4. Receiving

Secure transport, storage and authentication

Secure reply to or initiation of messages to organization

Strong authentication of sender of messages and files

Content & context classification to enable compliance with internal data (retention / removal) policies

Source: Zivver

Background

Zivver was founded in 2015 by current CIO Rick Goud and CEO Wouter Klinkhamer. Goud has a background in medical informatics, holds a PhD in decision support systems in healthcare and worked as a strategy consultant in healthcare for more than six years. Klinkhamer has a background in business administration and law and worked as a management and strategy consultant for more than 10 years.

The experience of the regulatory demands on security and privacy in healthcare may have been an early influence, but the company has grown to more than 100 employees and more than 3,000 customers in a range of highly regulated sectors such as local government, legal, and insurance as well as healthcare.

After seed funding of $3 million in April 2017 led by henQ Capital Partners, Zivver had a Series A funding round in October 2018, raising $12 million and led by Dawn Capital with DN Capital in addition to henQ Capital Partners.

Current position

Zivver is provided in three levels and price points: Start, Professional, and Ultimate. It is licensed as a per user monthly subscription service, billed annually and with discounts at all levels for volume and for longer, multiyear contracts. All versions include email encryption, two-factor authentication, and the ability to revoke messages. Start has only web browser or mobile app access (Android and iOS), while the other versions add Outlook (Desktop and Online) or Gmail integrations, secure file transfer, and adjustable business rules. Ultimate has additional administration elements for Active Directory synchronization, single sign-on, managing authentication recipients, and default message expiration.

Zivver is delivered as a service, with a minimal on-premises footprint. The vast majority of its customers (95%) use Microsoft Outlook or Office 365, but Zivver recently launched a Gmail integration. Zivver capabilities are accessed through an extra toolbar that is integrated in the compose window of the relevant email client. Zivver integration can be deployed as a simple self-install by users or as part of a standard centrally managed installation. Typical deployment involves only a few elements of configuration and can easily be accomplished in a few hours, including integration with on-premises or Azure Active Directory and the configuration of single sign-on using existing identity management systems. There is also an API for further backend systems integration to applications such as CRM or electronic patient records systems, where messaging may be generated automatically and can make use of Zivver's secure communications.

Deployment support, especially for communications tools, can often benefit from more than technical integration. To this end, Zivver has created deployment playbook services for different scenarios and can offer full go-live support including deployment and training to ensure effective use and rapid user adoption. Integration and deployment support are provided by Zivver directly in the Netherlands and through channel partners in the UK. By packaging this go-live service, Zivver has created a proposition for channel partners to add to or wrap around their own capabilities.

In addition to outbound email security, Zivver also has Mailbox Retention Compliance, a product to help organizations control sensitive information residing in inboxes. This scans received emails and uses organization-defined compliance rules to mark sensitive emails as being subject to a specific rule or overdue in violation of a retention requirement. This product provides the organization with insights and logging for compliance and helps to support and educate employees.

Future plans

Zivver implements email data security as a use case on a more generic business communications platform. This means it is also adding further secured business use cases. So far it has launched secure video communications, Zivver Meet, and it is also exploring further business communications that would benefit from an easy-to-use secure platform, such as sending secure forms (like TypeForm) and digital signatures (like DocuSign). To build on this approach, while Zivver's channel partners today tend to offer a cybersecurity angle as part of their value add, it is increasingly looking at those who focus on other critical business communications needs.

Analyst comment

Zivver is designed to be easy to adopt and use. In regulated environments where email is undoubtedly already well established, its use could reduce security and privacy risks. This can be accomplished without alienating users or forcing them to change their approach, while also making them more aware of good communications hygiene.

Zivver applies a combination of public and private key encryption, plus the option of two-factor authentication to encrypt message content and ensure only authentic recipients receive and can view the content sent. Zivver does not have access to the private encryption keys, which means it cannot view or be forced to reveal encrypted messages; however, it also means it cannot perform additional inspection or searching of encrypted content on behalf of the user. The nonholding of private keys is not unique, but very few vendors in this space adopt that approach, possibly only Virtru in addition to Zivver.

In addition to the application of information sensitivity and recipient email checks during email composition, Zivver can also check for sensitive or confidential information residing in an inbox and apply controls such as removal or alerting of noncompliant email data retention. While this is not strictly part of outbound email security, it could be very useful for spotting information that should have been deleted or stored elsewhere and could be a useful element of managing confidential data and compliancy rules.

As the market evolves and the understanding of the need for outbound email grows beyond the tightly regulated sectors, the larger and typically North American technology vendors will likely rise to the fore. Some of these, such as Microsoft, will be centered around email, and there is also the growing use of Gmail in organizations to consider, so it is good that Zivver has Gmail integration. And of course, one of the heavyweights in inbound email security such as Proofpoint or Mimecast might perceive the addition of a more focused outbound security capability as beneficial. Any of these vendors could develop the technology internally or choose to acquire a company with a ready-made platform and customer base.

That being the case, there are risks for specialized, Europe-based organizations. Zivver does well to make itself easy both to use and to fit in to existing working practices, but it will need to do more as it aims to extend into other verticals and territories. Its outbound email security product is built as a use case on a more generic secure communications platform, and this could be its route forward.

Zivver has already launched a secure video service and has plans for securing other day-to-day business communications processes such as filling in forms and digital signatures. For some sectors and to meet regular legal requirements, these types of services will depend on changes in regulations, but new remote working practices, many catalyzed by the coronavirus pandemic, may be the incentive for these regulatory changes to happen faster. Zivver may be a minnow in competitive terms, but securing critical business processes beyond just email could be its way to remain and grow in importance as the pond grows in size and the bigger fish become more active.

Table 4: Data sheet: Zivver

Product/service name	Zivver Secure Email	**Product classification**	Outbound email security
Version number	Outlook Desktop: 4.3.0 Outlook Online (OWA): 3.38.0 Gmail Extension: 1.0.8	**Release date**	Outlook Desktop: Initial release: March 2017 Current version: September 2020 Outlook Online (OWA): Initial release: January 2019 Current version: July 2020 Gmail: Initial release: July 2020 Current version: September 2020
Industries covered	Medical, local government, legal, and insurance	**Geographies covered**	In EMEA focus is on the Netherlands, Germany, Belgium, and the UK
Relevant company sizes		**Licensing options**	Per user monthly subscription
URL	www.zivver.eu	**Routes to market**	Direct and channel partners
Company headquarters	Amsterdam, Netherlands	**Number of employees**	100+

Source: Omdia

Appendix

Market Radar methodology

- Detailed technical briefings were conducted with each vendor in the report.
- Supplemental information was obtained from vendor literature and websites, other Omdia surveys, and Omdia's data products and market forecasts.
- The report was peer reviewed by at least two different analysts or consultants.

Authors

Rik Turner, Principal Analyst, Cybersecurity

Maxine Holt, Senior Research Director, Cybersecurity

Rob Bamforth, Associate Analyst

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

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com