GIGAOM

MARKET RADAR

GigaOm Radar for Phishing Prevention and Detection v1.0

SIMON GIBSON | AUG 14, 2020 - 1:20 PM CDT

TOPICS: PHISHING SECURITY & RISK

GIGAOM

GigaOm Radar for Phishing Prevention and Detection

TABLE OF CONTENTS

1. Summary

In 2020, global email usage will top 300 billion messages sent, according to technology market research firm The Radicati Group. And that can be a problem, because email remains a leading conduit for malware delivery and phishing exploits. The message: an effective anti-phishing solution must be a critical component of your enterprise security strategy.

The ability to effectively analyze and understand email traffic gives us the opportunity to derive great insight into different vectors of threat. These threats include malicious activity, crime, extortion, BEC (business email compromise), as well as insider threats. That insight can then be used to respond and effectively secure and protect both employees and organizations alike.

Vendors in the market today tackle this challenge in a variety of ways. Some focus purely on inbound email communications, others on internal communications within the same (or otherwise trusted) domains. As in many other areas of information security however, there is no silver bullet. The best approach will ultimately be some hybrid of these, building a layered approach often called defense in depth.

In this Radar report, we have considered a broad cross-section of the many solutions and approaches in the market today.

When evaluating these vendors and their solutions, it is important to consider your own business and workflow. Different solutions, or combinations of solutions, will be more or less appropriate depending on the nature of your email traffic and business workflow. It is also important to consider your internal ability to handle the potential complexity of the solutions. For some it may be preferable to settle on one comprehensive solution, while for others building a best-of-breed architecture from multiple vendors may be preferable.

2. About the GigaOm Radar

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics–such as scalability, performance, and TCO–that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Vendor Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

3. Market Categories and Deployment Types

For a better understanding of the market and vendor positioning (**Table 1**), we categorized solutions for Phishing Prevention and Detection by their target market segment and the method (or methods) by which they can be deployed. The target market segments are:

- **Small/Medium Enterprise:** In this category we assess solutions on their ability to meet the needs of organizations ranging from small businesses to medium-sized companies. Also assessed are departmental use cases in large enterprises, where ease of use and deployment are more important than extensive management functionality, data mobility, and feature set.
- **Large Enterprise:** Here offerings are assessed on their ability to support large and business-critical projects. Optimal solutions in this category will have a strong focus on flexibility, performance, data services, and features to improve security and data protection. Scalability is another big differentiator, as is the ability to deploy the same service in different environments..
- **Specialized:** Optimal solutions will be designed for specific workloads, end users, and use cases. In some instances the product is designed to "learn and adapt." In others they may allow customization of the code.

Phishing detection and prevention tools support a variety of deployment models. We recognize the following approaches in this report:

- **In-Line**: The vendor becomes your mail server and processes your email before forwarding it on. This stops an email immediately, before it has the chance to land at the client's inbox.
- **Out of Band:** Your company is still the mail exchanger (MX), but journaling is used to "BCC" every email to the phishing service. The service then processes the message before reporting back if a suspicious email was discovered. Out-of-band services have the advantage of defending against phishes that occur from within the same domain (such as in the case of an account takeover), which an inline service will not detect. However, this approach can produce a time delay in spotting an attack.
- **Cloud:** The solution is available in the cloud. Often designed, deployed, and managed by the cloud service provider, the solution is not available beyond that specific cloud service. The advantage of this type of solution is the integration with other services offered by that cloud service provider (functions, for example) and its simplicity.
- **On-Premises:** The solution can be implemented in the enterprise data center.
- **Endpoint:** The solution can be deployed on the endpoints (personal computers, mobile devices, and the like).

Table 1: Vendor Positioning

	MARKET SEGMENT			DEPLOYMENT MODEL				
	Small/Medium Enterprise	Large Enterprise	Specialized	In-Line	Out of Band	Cloud	On-Premises	Endpoint
Agari	+++	++	++	++	++	++	++	-
Area 1	++	+++	++	+++	++	+++	-	-
Broadcom	++	++	+	++	++	++	++	++
Bromium	+	+++	++	-	-	-	++	+++
Cisco	++	+++	+	++	++	++	++	++
Cofense	++	++	+++	-	-	-	-	-
G Suite	++	++	+	++	-	++	-	+
Microsoft 365	++	++	+	++	++	++	++	++
Mimecast	+++	++	+	++	++	++	-	+
Proofpoint	+++	++	+	++	++	++	++	-
Raytheon Forcepoint	+	+++	++	++	++	++	++	++
Virtru	+	-	+	++	-	-	-	+++
Webroot	++	+	+++	++	+	+	+	+
Zimperium	+++	+++	+++	++	+	++	++	+++

+++: strong focus and perfect fit of the solution
++: The solution is good in this area, but there is still room for improvement
+: The solution has limitations and a narrow set of use cases
- : Not applicable or absent.

Source: GigaOm 2020

4. Key Criteria Comparison

Following the general indications introduced in the report, "Key Criteria for Evaluating Phishing Prevention and Detection," **Table 2** summarizes how each vendor included in this research performs on the features and criteria we consider differentiating and critical for an enterprise phishing protection solution. The definitions of these criteria are:

- **Analytics:** The completeness and scope of a vendor's analytical tools
- **Standards Support:** Does the vendor help its customers to enforce DMARC and SPF policies, and does it offer customers a platform to manage standards?
- **Deployment**: How flexibly can the solution be deployed and how well is it integrated with existing infrastructure?
- **Sequestration**: When a phish is detected, will the product remove it from all of the targets that received it, and how well does the vendor do at preventing false positives?
- **Orchestration**: Does the tool play well with others, and are the standard frameworks for integrations with existing security information and event Management systems present?
- **End to End:** To what extent has the vendor provided an end-to-end solution that detects inbound phishes, both through the infrastructure and on the endpoint?
- **Addresses Insider Threat:** Is the product positioned to take advantage of enterprise insider threat detection programs that address intent to leave, harassment, and theft?

Table 2: Key Criteria

	KEY CRITERIA						
	Analytics	Standards Support	Deployment	Sequestration	Orchestration	End to End	Addresses Insider Threat
Agari	++	+++	++	-	+	-	-
Area 1	+++	++	++	++	++	-	+
Broadcom	-	++	+	-	-	+++	-
Bromium	+	-	+	+++	++	+	-
Cisco	+++	+++	++	++	+	-	+
Cofense	++	-	+	-	+	-	-
G Suite	++	++	++	+	+	+	-
Microsoft 365	++	++	++	+	+	+	-
Mimecast	++	+++	++	+	+	++	++
Proofpoint	+++	++	++	++	++	-	-
Raytheon Forcepoint	+++	++	++	++	++	++	+
Virtru	+	++	++	++	++	+++	+
Webroot	++	-	+	-	+	-	-
Zimperium	++	+	+++	++	++	+	-

+++: strong focus and perfect fit of the solution
++: The solution is good in this area, but there is still room forimprovement
+: The solution has limitations and a narrow set of use cases
- : Not applicable or absent.

Source: GigaOm 2020

In addition, this report considers the higher-level evaluation metrics that play a key role in a decision to choose one solution over another. The evaluation metrics considered in this report, graded in **Table 3**, are the following:

- **Architecture:** Does the solution have a compelling architecture to grow and adapt?
- **Scalability:** Will the solution scale effectively for large-scale deployments?
- **Flexibility:** Is there a degree of flexibility and customization possible to adapt the solution for specific use cases?

- **Efficiency:** How much impact does the solution have on email traffic flow and response times?
- **Performance:** How robust is the solution's performance under heavy load?
- **Manageability and Ease of Use:** How easy is the solution to configure, manage, and use?

Table 3: Evaluation Metrics

	EVALUATION METRICS					
	Architecture	Scalability	Flexibility	Efficiency	Performance	Manageability Ease of Use
Agari	+	+++	++	++	++	++
Area 1	++	++	++	++	+++	+++
Broadcom	+	+++	++	++	+	+
Bromium	++	+	+	+	++	+
Cisco	++	+++	++	-	++	++
Cofense	+	+++	++	+	+	++
G Suite	++	+++	++	+	++	++
Microsoft 365	+	+++	+	+	++	++
Mimecraft	++	++	++	+	++	++
Proofpoint	++	+++	++	+	++	+
Raytheon Forcepoint	+++	+++	++	+	++	+
Virtru	+	+	++	++	+	+
Webroot	+	++	+	-	+++	++
Zimperium	+++	+++	+	++	+++	++

+++: strong focus and perfect fit of the solution
++: The solution is good in this area, but there is still room forimprovement
+: The solution has limitations and a narrow set of use cases
- : Not applicable or absent.

Source: GigaOm 2020

5. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 1**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

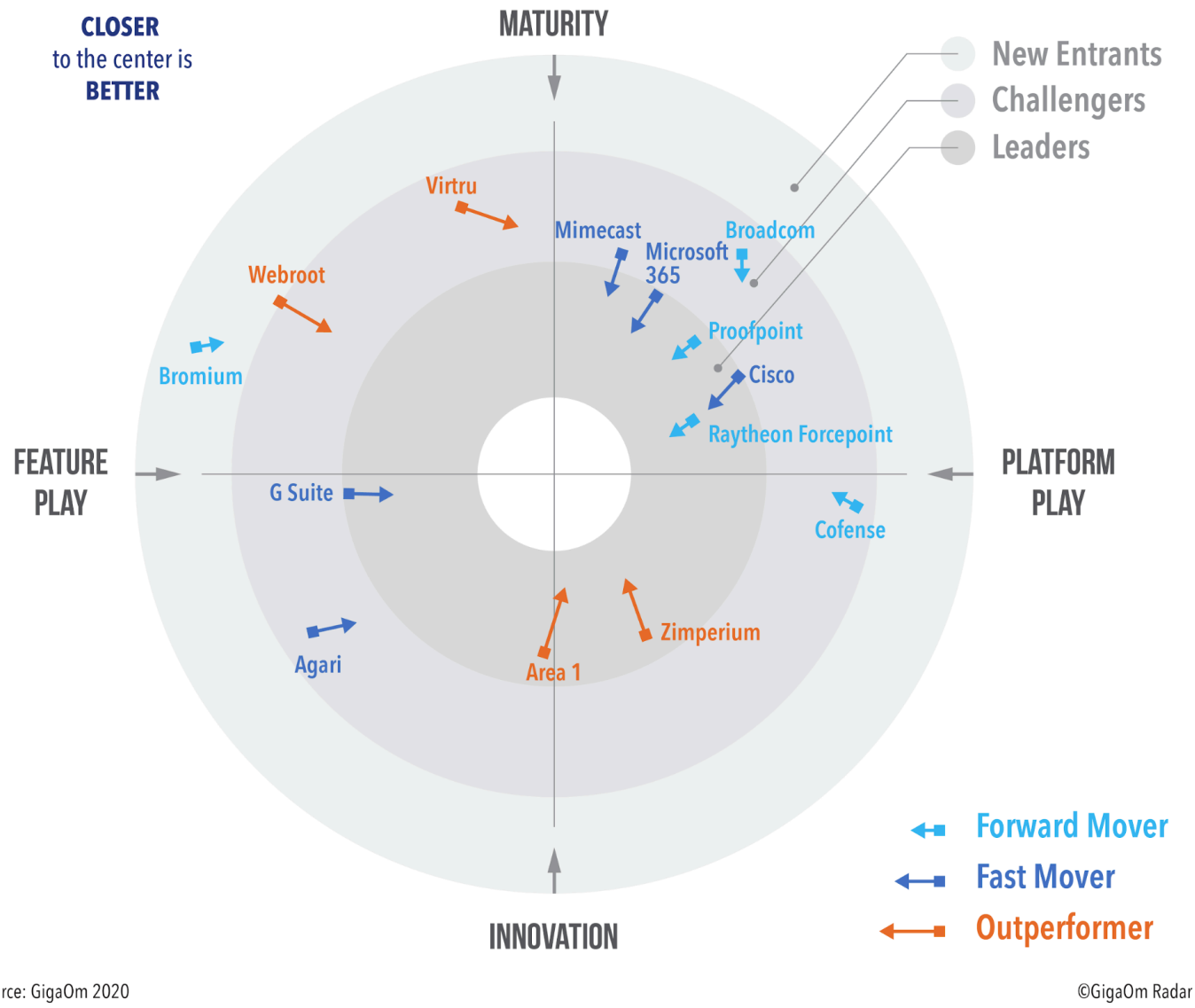

Figure 1: GigaOm Radar for Phishing Prevention and Detection

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.

The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

6. Vendor Overview

Agari

Agari focuses heavily on understanding trust relationships to inform what is normal communication versus what might be suspicious. Agari is installed at Google and Microsoft and uses that very large swath of visibility to build communication relationship models. Agari offers solutions for enterprises to deploy DMARC easily and report on how their domains are being used across the internet. Agari's founder, Pat Peterson, has roots that go way back to email standards, which is reflected in the company's product.

The Agari Secure Email Cloud includes four products: Agari Brand Protection and Agari Business Fraud Protection, which focus on DMARC email authentication, Agari Advanced Threat Protection to prevent phishing email from reaching employee inboxes, and Agari Incident Response to accelerate phishing incident triage, remediation, and breach containment for the SOC.

Strengths: Agari's strengths are rooted in the amount of email it processes per day, and that insight allows it to pick up on phishing attack trends before some of the competition. Agari focuses on brand protection that ensures valid domains are not spoofed with look-alikes. It is able to understand what relationships should look like by analyzing conversations.

Challenges: Agari's focus is more broadly distributed among DMARC, brand protection, and analysis, so it is less focused than some on detecting subtle tactics used in pretexting attacks. The long tail in the way that its solutions operate can mean that learning can be slow. In effect, the Agari solution protects the organization from phishing by protecting the brand from being used in phish. While this feature may be appropriate in some use cases, it may not be in others.

Area 1

Area 1 deploys small pattern analytics technology to monitor the attack infrastructure used by criminals and spiders on the Internet to detect phishing campaigns. This proactive monitoring then informs its model to block them. Area 1 relies on a mixture of trust relationship heuristics and embedded attachment and URL detection.

Apart from its unique technology, Area 1 also employs a novel approach with its cost structure. It is the only company we spoke with that has implemented a "pay-per-phish-model." In this model, the company charges only for the phishes it has caught. This should make deploying Area 1 ahead of any other vendor's SEG (Secure Email Gateway) a no brainer. Services are offered via the cloud. Area 1 focuses on prevention and believes that training and awareness are no match for good technology.

Area 1 deploys inline as a mail exchanger (MX) or out of band, using APIs or journaling. This approach enables deployment at the edge to monitor inbound email. It can also monitor internal east-west phishing attacks. Area 1 also gets a boost from the recent launch of a joint solution that incorporates

Virtru's innovative encryption-based email protection scheme.

Strengths: Area 1's sole focus is on the detection and prevention of phishing campaigns, with a pay-per-phish model that charges only for phishes that are caught. Area 1 uses Google Big Query to enable customer security teams to access lightning-fast searches when responding to incidents. The Virtru partnership adds value.

Challenges: Area 1 is in a hyper-growth phase, which means it may endure some growing pains as it develops new capabilities. Area 1 until recently was limited to anti-phishing and email security, though the partnership with Virtru changes that.

Broadcom

Purchased as part of the acquisition of Symantec in Fall 2019, Broadcom's Symantec Email Security Cloud products offer a range of SEG, including DLP and e-discovery, email archiving, and continuity solutions. Broadcom couples its SEG with training and cloud-based threat protection, while its footprint means that its signatures and threat intelligence are coupled, making for a robust offering. In addition to offering services in the cloud, SEG is available on-premises.

Strengths: Broadcom has a large portfolio of security products that customers can leverage and orchestrate to provide visibility. Things like GDPR compliance and CASB dovetail nicely with its SEG.

Challenges: Not a pure phishing prevention play. Product suites are large and present complexity.

Bromium

Bromium offers phishing protection and process isolation or machine impermanence. In cases where phishing prevention is additive, installing an agent-based defense might make sense. Bromium isolates running processes from one another; uses heuristics to determine malicious execution or injection; and, in tandem with an SEG that does pretext filtering, presents a robust solution set. Bromium's approach is focused on stopping the effect of phishing attacks rather than the cause.

Strengths: Client-side sandboxing and process isolation means that one infected file or executable will not harm other digital assets.

Challenges: Management of isolation to enable Bromium's full functionality requires sandboxing applications and documents. This can disable standard workflow or add overhead in management. Bromium does not leverage DNS or DMARC or other traditional analytics.

Cisco

A dominant player in the space, Cisco offers a broad range of services that can be deployed on-

premises or in the cloud. Its solutions prevent phishing emails from landing in the inbox, detect outbreaks on networks and endpoints, and secure access with two-factor authentication, among other capabilities.

The Cisco Advanced Phishing Protection and Email Security Appliance is built on the Ironport appliance and incorporates some of the domain protection and threat intelligence technology from niche player Agari. The Cisco suite includes threat intelligence, malware protection, and forged email detection, as well as data loss prevention and message archiving. Cisco also offers Advanced Malware Protection for Endpoints (AMP), Cisco Visibility for Endpoints, and Threat Response.

Strengths: Cisco over the years has acquired point-specific capabilities that, in their totality, give the company a tremendous range of security capabilities. Its security products target broad swaths of industry, and because of its market saturation, finding people to operate Cisco solutions is generally straightforward.

Challenges: Cisco products are designed to operate together, and orchestration in heterogeneous environments can be demanding.

Cofense

Cofense (formerly Phishme) offers products targeted at awareness, reporting, and training. Cofense works to spot phishing campaigns and isolate them, relying on its threat intelligence and employee training. The service offers plug-ins for Outlook that enable employees to report phishing easily and allow the SOC to orchestrate a response. Cofense is a strong believer in automation and orchestration. It integrates with FireEye and Splunk, and provides its own dashboards as well.

Strengths: Cofense is the market leader in phishing training and awareness, with a broad array of modules and scenarios that improve base security awareness among employees. The service offers a “triage” button that allows employees to report a suspected phish.

Challenges: Cofense is not focused on email processing or detecting BEC, DMARC, or standards.

G Suite

Google understands better than anyone that email is the skeleton key to our digital life. With access to email, we are able to change passwords, receive magic login links, and create new accounts. Its approach is to control unauthorized access to email, full stop. As commercial off-the-shelf-products go, Google G Suite is arguably the best in the world.

Google G Suite offers multiple levels of protection. All customers get advanced URL, external image, and malicious attachment filtering, powered by Google AI-enabled deep learning. Very good spam protection is included.

While the basic level includes protection from attacks, enterprise-level customers are provided attachment scanning with the Security Standbox, as well as enhanced security via G Suite Advanced Phishing & Malware, which allows policy enforcement for sending and receiving email. Finally, G Suite customers can add Advanced Protection, which sets up an extra layer of security designed to thwart targeted online attacks against a user's account. For companies operating in hostile environments, this is some of the best off-the-shelf protection available.

Strengths: Google does a very good job of detecting phishing campaigns at mass scale and can, to some extent, detect targeted ones. It focuses on preventing phishing and malware from being delivered, and blocking takeover of customer accounts and applications. Advanced Protection adds an extra layer of security.

Challenges: While Google has a full suite of phishing, malware and account protections, some organizations will want additional layers that G Suite does not address, such as policy enforcement between organizational units for analyzing human-to-human behavior used in social engineering and pretexting type attacks. The security around application protection, Google Smart Lock, and security keys requires some overhead, administration, and user training.

Microsoft 365

Microsoft 365 boasts several levels of protection against phishing attacks. For enterprises that want more protection, Microsoft offers ATP (Advanced Threat Protection) in three flavors. There is basic Level 1 coverage that comes out of the box and includes attachment and link filtering. Level 2 adds threat tracking, while Level 3 (E5) further adds collaboration and workflow tools. Companies often augment security and establish defense in depth by deploying anti-phishing solutions from pure-play vendors alongside the protections built into Microsoft 365.

Strengths: Microsoft phishing prevention tools are easy to deploy and create policy around. E5 customers can write workflow policy and ensure that employees and vendors use only the enterprise approved tools, which helps security teams manage threats.

Challenges: Because Microsoft is so large and serves many types of customers, its ability to understand the inner workings and unique requirements of individual enterprise customers is limited.

Mimecast

Mimecast is a large player that recently acquired Solebit to enhance its malware detection and forensics. Mimecast offers an SEG and couples it with an email continuity service to mitigate downtime and provide 100% email availability. It deploys exclusively via the cloud and offers broad email management services as well as phishing prevention. Mimecast provides bottomless archiving and a sub 7-second SLA on search. The Ataata acquisition enables Mimecast to offer security awareness and phishing training for an organization's users.

Strengths: A very complete, mature solution, Mimecast performs NLP, analytics, SOAR, and follows SPF/DMARC standards.

Challenges: Because the solution is very robust, there is a learning curve and need for experienced personnel to deploy and tune the solution.

Proofpoint

Proofpoint began as a pure, secure email gateway (SEG) and has evolved its offerings to include threat intelligence and incident response, as well as data management and protection. Solely devoted to phishing protection, it has leveraged its phishing DNA to provide advanced threat protection on mobile devices. It also provides a stand-alone threat intelligence product that its customers can leverage with security information and event management (SIEM) or user behavior analytics (UBA).

Proofpoint processes on the order of 5 billion messages per day and offers a full suite of phishing prevention and domain protection products. Proofpoint SEG is available both in the cloud and on-premises.

Strengths: Proofpoint processes huge volumes of email and was early to understand the value of threat intelligence and isolation of attachments.

Challenges: Proofpoint's UX and workflow process can be disruptive to end-users, and the administration of it can be cumbersome.

Raytheon Forcepoint

Raytheon Forcepoint offers an advanced classification engine that puts a lot of emphasis on the trust relationships between the sender and receiver. Its Advanced Classification Engine (ACE) layers in data classification, security about embedded scripts, and web site references and reputations. Forcepoint offers both on-premises and cloud-based data warehousing for searching and e-discovery.

Strengths: Forcepoint is a powerful secure web gateway and set of tools focused on broad corporate security that includes DLP, insider threat detection, and email. It offers a comprehensive suite of security tools.

Challenges: With its broad focus and flexibility, Forcepoint imposes both complexity and cost.

Virtru

Virtru's approach to securing email is to take it private. It employs end-to-end email encryption and access controls to ensure that only intended recipients can access email content and attachments. For detection and remediation of phishing emails, Virtru has partnered with Area 1 to provide a bundled

solution that integrates Area 1's advanced anti-phishing capabilities.

The Virtru scheme encrypts all messages and attachments with AES 256-bit Access Control Keys on the content creator's client via a browser extension, Microsoft Outlook plug-in, mobile app, or another Virtru-enabled client. Access control policies may be applied at this time, either manually, via the user, or automatically via data loss prevention (DLP) rules preconfigured by administrators.

To allow recipients to read emails without installing Virtru's software, Virtru utilizes an external object store, such as Amazon S3, to surface encrypted emails.

Strengths: The solution provides end-to-end encryption for trusted communication between already-known entities. The recently announced joint solution with Area 1 adds phishing detection and remediation to Virtru's toolbox.

Challenges: The established Virtru solution did not easily protect emails from new senders—leaving use cases that require many "new" email conversations (a B2C helpdesk, for example) exposed. The Area 1 deal may close this gap.

Webroot

Webroot offers email protection from malicious attachments on the endpoint, but does not offer protection from pretexting scams. It offers the ability to manage DNS, training, and reporting. The primary focus is around URL/URI, domain reputation, and threat intelligence. The Webroot solution is designed to report on the validity of a visited URL, but does not remove from the inbox or server the email that may have brought you to that destination. It relies on the recipient clicking on a link before providing protection.

Strengths: Robust Internet reputation scoring capabilities enable customers to analyze URLs and help determine whether they present a risk. This capability can be leveraged to understand the kinds of sites being visited by an enterprise.

Challenges: Webroot's primary focus is categorization: it can be effective at stopping known bad traffic, but if a URL is not reported as malicious, it is not effective. The approach is also not effective in stopping pretexting attacks. We also believe it is relatively easy for persistent attackers to defeat categorization algorithms.

Zimperium

Zimperium offers endpoint protection, specifically on mobile devices. Whereas most solutions seek to eliminate the phish before the inbox, Zimperium's on-device z9 engine takes a different tack. It prevents targeted mobile attacks, the use of unauthorized profiles that could bypass corporate controls on mobile devices, as well as attacks that leverage man-in-the-middle techniques. Zimperium is managed through "zConsole," which can be deployed in any cloud or on-premises. It takes updates

through a process Zimperium assists with as needed by its customers. The process for updates is similar between cloud hosts and on-premises.

Strengths: Focused solely on mobile device protection, Zimperium is the leader in this space. Its holistic approach to detection of phishing attacks targeted at users' mobile devices allows it to block phishing attacks that use text, social media, and personal and corporate email as vectors. It can do this while ensuring user privacy.

Challenges: Because it focuses on the holistic state of the mobile device and users' privacy, Zimperium does not intercept email content. While it can use heuristics to detect BEC, its efficacy in that space is diminished.

7. Analyst's Take

Standing up effective protection against phishing attacks is one of the single most important defensive measures you can take to protect your enterprise. Before considering the solutions in this report, however, companies should first assess their security programs and be able to answer "yes" to the following two questions:

- Do we have a robust phishing prevention program in place?
- Do we enforce multi-factor authentication for email?

Organizations that can't answer a firm yes to both of these questions should focus on building out these capabilities first. Only then will they be in a good position to deploy custom security measures.

As this report shows, there are many approaches available in the market. Regardless of solution, we recommend that enterprises layer at least two different approaches into their strategy, to provide effective defense in depth.

In addition, it's important to consider carefully the nature of your email traffic and its role in sensitive workflows. This will help you decide which approach, or combination of approaches, will afford you the best overall protection.

Finally, do not underestimate the "human factor" in developing your anti-phishing strategy. Effective awareness training to inform and influence the right behaviors can pay big dividends by reducing the overall level of risk produced by phishing attacks.

8. About Simon Gibson

Simon Gibson is a CISO and subject matter expert on security. He has been responsible for driving security capability into products, enterprises and supporting complex engagements.

Simon led the Information Security Group at Bloomberg and served as their CISO. He has managed attack teams, incident response teams and been responsible for the defensive security posture in the financial, government, manufacturing and PCI industries.

Simon is a renowned speaker and panel moderator. He has counseled fortune 100's on building their programs and worked with US Government public private information sharing initiative

9. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

10. Copyright