GreatHorn

Dynamic Email Monitoring:

Achieving Balance to Optimize Both Security and Productivity

Email is central to your business processes, but security threats are on the rise. Emphasize convenience, and attacks get through. Lock things down, and productivity suffers. Here's how to strike the right balance.

WHITEPAPER

September, 2020

In our new, uncharted business era, a significant number of your employees are working from home. They're connected to your operations through technologies new and old: videoconferencing, chat and, as always, email.

But this new way of working raises the stakes. Employee productivity has never been more crucial, as teams pivot to sustain processes and serve customers. Cybersecurity risk has never been greater, as IT and security functions struggle to control the technologies employees use and the way they work to minimize risk to the organization.

In the face of these challenges, how are you managing email security? Lock it down too tightly, and productivity, user satisfaction and customer service suffer. Make it too lax, and phishing schemes, malware and advanced threats get through, often resulting in a data breach.

The solution is dynamic email monitoring. This automated, machine-learning-enabled approach empowers you to take back control of your email protections. But you need the right technology to achieve the level of email security that matches your unique business needs – quickly, cost effectively and reliably, this time and every time.

An automated, machine-learning-enabled approach empowers you to take back control of your email protections.

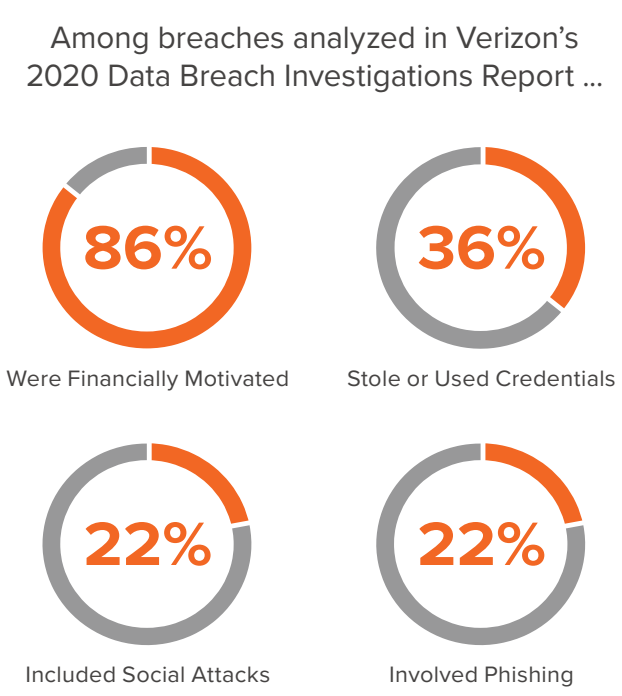
Email Attacks on the Rise

IT and security pros know that when it comes to email security, the hits keep on coming. Phishing, credential theft, malware, ransomware, zero-day attacks, advanced threats – the numbers are always rising.

Phishing and credential theft stand out as particular problems. "As time goes on, it appears that attackers become increasingly efficient and lean more toward attacks such as phishing and credential theft," says Verizon in its "2020 Data Breach Investigations Report."[1]

The comprehensive analysis, now in its 13th year, examined 3,950 data breaches. It found that significant percentages of breaches included social attacks, involved phishing, stole or used credentials, and were financially motivated. (See Figure 1.)

Figure 1: 2020 Security Breach Profile[2]



[1, 2] *"2020 Data Breach Investigations Report," Verizon, 2020*

A broad, gray area of emails exists between the known good and the known bad.

Reevaluating Email Action Severity

Gone are the days when organizations only have to worry about the inundation of spam to their employees. This was a nuisance to IT professionals, but today's cybercriminals are financially motivated. They perpetrate their crime through:

- Spearphishing
- Domain spoofing
- Malicious links
- Malicious attachments
- Keystroke logging
- Impersonation of legitimate, trusted senders

Their goals include:

- Stealing credentials to gain access to corporate and systems and data
- Gaining trust to move laterally through your organization to steal even more credentials and data
- Deceiving users into taking actions such as misdirecting payments or transferring funds

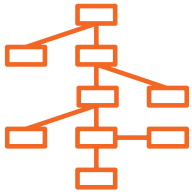
That's why many organizations completely lock down email security. They take the approach that if any email isn't "known good" it is assumed to be "known bad."

But if you make email security too tight, your users have to spend more time and effort to handle core processes, their job satisfaction is eroded and they can't serve customers as effectively. Your IT and security analysts, for their part, spend too much time evaluating suspicious email traffic, handling false positives and responding to user requests to release quarantined emails. Meanwhile, your partners and customers face roadblocks in doing business with you.

On the other hand, if you set your email controls too loose, you allow malicious emails to get through, and you place the responsibility for judgment calls about suspicious emails on your (sometimes inattentive) users. As a consequence, you can potentially expose sensitive personal and corporate data, suffer high costs for stolen credentials and remediation, and degrade the value of your brand.

In response, a growing number of organizations are reevaluating "action severity" – the appropriate level of response to email threats. They recognize that a broad middle zone of emails exists between the known good and the known bad. These are emails that include an email address, domain, link, attachment or other content that for one reason or another makes the email suspicious.

But the threats reside along a continuum from small to large. And that calls for a new approach to email security.



Dynamic email monitoring attenuates and automates your response to threats based on machine-learning algorithms.

Dynamic Monitoring for the Right Response

The solution is dynamic email monitoring. Dynamic email monitoring balances the convenient but high-risk approach of letting every email through with the secure but business-constraining mindset of locking everything down. (See Figure 2.)

Dynamic email monitoring attenuates and automates your response to threats based on machine-learning algorithms. The business rules that form the basis of these algorithms can be tailored to meet unique needs. And the algorithms themselves leverage vast data streams to continually fine-tune themselves for increasingly accurate, effective control of email.

Such email control occurs in real time to strike the right balance between user productivity and ironclad security – at the moment you need it. In the case of known bad links or attachments, for example, it automatically removes the email from the user's inbox. For suspicious email content, the user is prompted in a risk-appropriate manner.

Dynamic email monitoring engages users in the moment of risk, so they're empowered to do their jobs productively and engage with customers and partners effectively – while still complying with the level of security that's right for your organization.

Figure 2: Balancing Email Convenience and Security

User Security Awareness in the Moment of Risk

Employee training and awareness are important to every aspect of your organization's security, including email protections. But security training is typically built around learning videos presented during onboarding and then on a yearly basis. By the time an employee encounters a threat, that training might be a distant memory.

Dynamic email monitoring can help. Security awareness is much more effective when it occurs during the moment of risk, when a user is engaged with the email or threat. In tandem with traditional security awareness training, dynamic email monitoring that warns employees of suspicious emails, with context-specific messages, heightens their awareness and encourages the right behaviors.

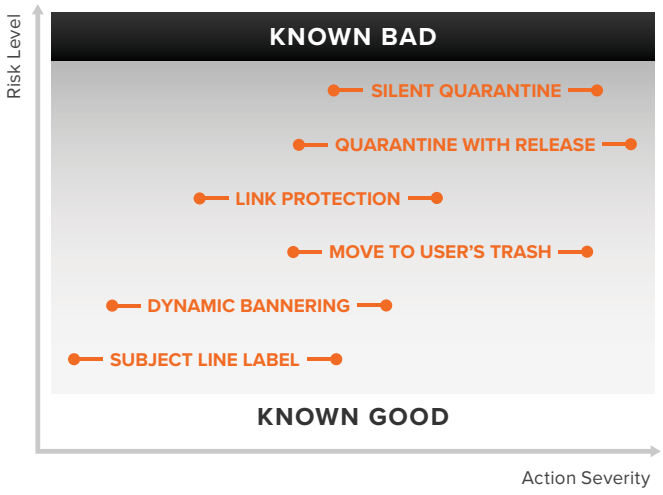
Dynamic email monitoring should integrate with and build on your onboarding and e-learning solutions. That way, every employee can contribute to the effectiveness of your security policies – and become a partner in protecting your organization.

The Six Layers of Dynamic Email Monitoring

Dynamic email monitoring involves six layers of protection in the middle zone of email security. (See Figure 3.) Each layer provides an additional level of security and takes an appropriate action attuned to the severity of the threat.

So, you can select which actions are appropriate for each variable identified as suspicious, in a continuum akin to pumping the brakes or bringing things to a screeching halt. You can customize under which circumstances each layer of protection kicks in for various business roles and situations. Business rules enable you to specify that one set of users can engage with a particular domain name or file type, say, while employees in a different function receive a warning.

Figure 3: Managing the Middle Zone of Email Security



Dynamic Layers of Protection

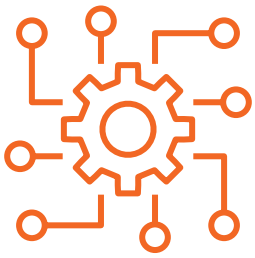
Most common options for gray area, include:

- **Subject line label** – The application injects an alert in the email subject line warning the user that the message contains suspicious content, such as financial details.
- **Dynamic bannering** – The software applies a more prominent, context-based notice. For instance, that the email originates from an external source and appears, to be spoofing your CFO or requesting payment on an invoice.
- **Link protection** – Because the software continuously observes embedded links, it can take risk-appropriate action. For an uncommon link, it can redirect to a safe page that warns the user before proceeding. For a known malicious link, it can disable the link altogether.

Most common options for highly suspicious and malicious, include:

- **Move to user's trash** – For an email that's more likely to contain a threat, the application can move the message to the user's trash or other designated folder.
- **Quarantine with release** – For an even more suspicious email, the software can remove the email from the recipient's inbox and provide a notification that the email was quarantined. The user is offered a workflow to request the email's release from quarantine. The email would then enter a process for further analysis – either automated or manual – before its released to the user.
- **Silent quarantine** – Finally, if the email contains a known malicious link or attachment, it's simply removed from the recipient's mailbox.

You can customize under which circumstances each layer of protection kicks in for various business roles and situations.



Transforming Payloads Into Payoffs

The advantages of dynamic email monitoring are tangible – and can show up on your bottom line. You gain the capabilities you need to block malicious payloads, credential theft and other attacks – while allowing your users to maintain their productivity and serve customers. With dynamic email monitoring, you can:

- Set your security to the level that meets your unique needs
- Address your most pressing threats, including spearphishing, domain spoofing, malicious links, malicious attachments and credential theft
- Match action severity to threat level
- Continually fine-tune your security to changing requirements
- Layer enhanced email security on top of your existing security environment
- Relieve IT and security staff from manual analysis of suspicious emails
- Allow users to engage with email the way they expect toEnable employees to remain productive, satisfied and engaged
- Deliver excellent email experiences to employees, partners and customers
- Support the smooth operation of your business

A global pharmaceutical company with more than 20,000 employees recently implemented dynamic email monitoring to achieve tighter email security. The enterprise was barraged by more than 16,000 credential-theft attacks and more than 21,000 email-compromise attacks in a single year that had bypassed both the gateway and the native cloud platform's detection.

The constant onslaught placed an enormous burden on the security function and exposed the organization to unacceptable risk. The company believed it was using robust email security tools, but those controls clearly weren't up to the job.

Without removing and replacing its existing security solutions, the company was able to quickly and effectively layer on dynamic email monitoring. As a result, it achieved the level of email security it required. It gained the ability to detect attacks luring users to click on malicious links or log into malicious websites. All while making sure employees have access to the email they need to do their jobs effectively.

The advantages of dynamic email monitoring are tangible – and can show up on your bottom line.

Your Partner in Dynamic Email Monitoring

GreatHorn offers a robust solution that enables dynamic email monitoring and ensures the highest levels of security for your email traffic. Our threat intelligence engine integrates with your existing security infrastructure – as well as e-learning platforms to promote effective security training.

Our email security expertise is based on our deep experience meeting the most demanding security needs of market-leading enterprises around the world. What's more, our collective intelligence – built on the management of billions of emails every month across our client base – drives the continual enhancement of our machine-learning algorithms.

In a new era of remote, contactless business – sustained in large part through email connections – more enterprises are recognizing the need for a better approach to email security. Dynamic email monitoring gives you the tools you need to protect your organization's most valuable information assets – while ensuring the employee productivity and customer service that power your business.

About GreatHorn

GreatHorn protects organizations from more advanced threats than any other email security platform. By combining its highly sophisticated threat detection engine with accessible user context tools and integrated incident response capabilities, GreatHorn Email Security shields businesses from both sophisticated phishing attacks and fastmoving zero-day threats, freeing security teams from the tedium of email security management while enabling them to respond to genuine threats faster than ever before.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other social engineering-based phishing attacks.