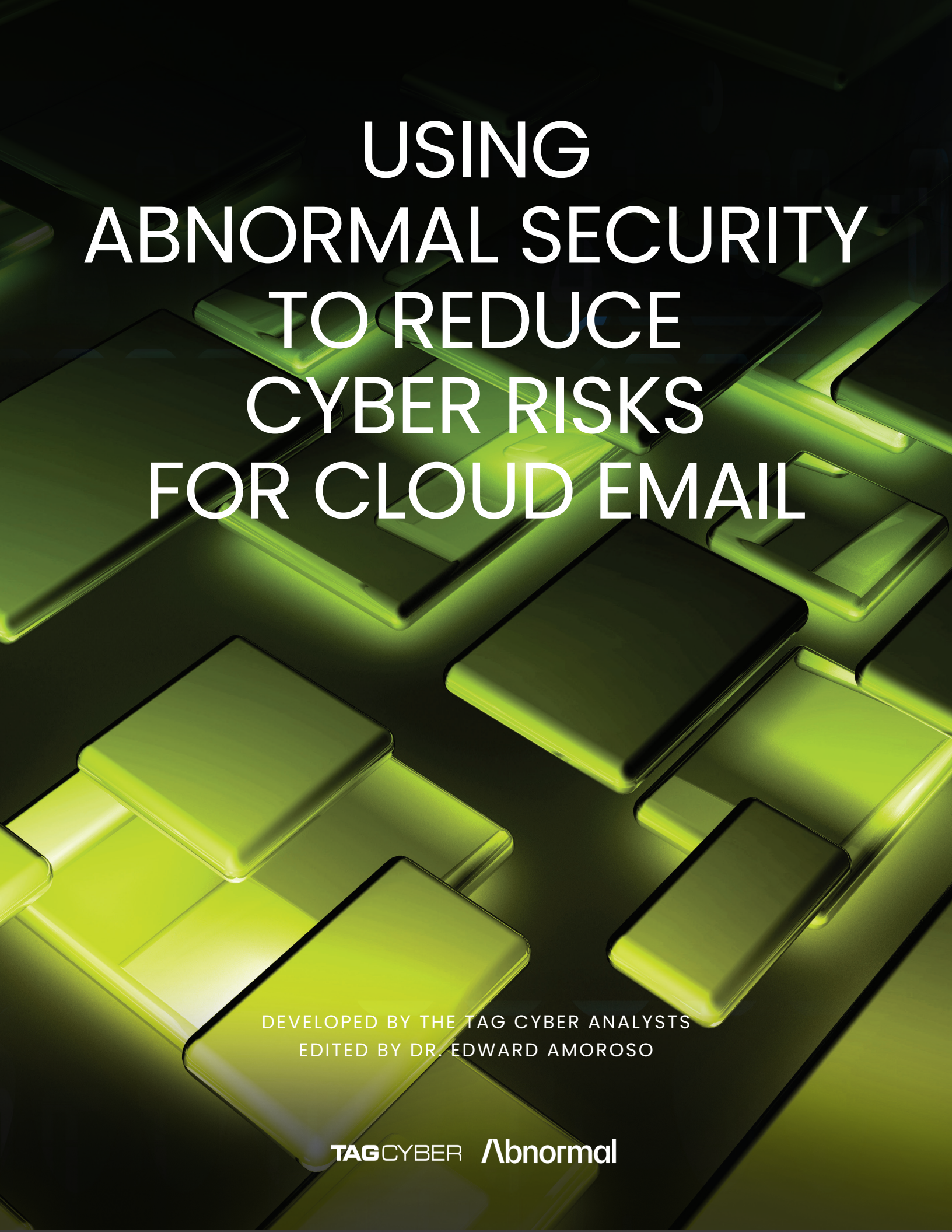

USING ABNORMAL SECURITY TO REDUCE CYBER RISKS FOR CLOUD EMAIL

DEVELOPED BY THE TAG CYBER ANALYSTS
EDITED BY DR. EDWARD AMOROSO

TAG CYBER Abnormal

USING ABNORMAL SECURITY TO REDUCE CYBER RISKS FOR CLOUD EMAIL

DEVELOPED BY THE TAG CYBER ANALYSTS
EDITED BY DR. EDWARD AMOROSO

Anyone working in business or government will agree that modern workplaces barely resemble those of earlier generations. The obvious shifts toward virtual work were underway long before the global pandemic, and the case can be made that COVID-19 just accelerated those trends.

The primary theme associated with the modern workplace is flexibility: employees, partners, and customers are now free to work from flexible locations, at flexible times, and with flexible schedules. While this might create discomfort for more traditional organizations, it creates a welcoming workplace for a new generation of people. And as one might have predicted, it also changes the cyberthreats that security teams must address.

In this series of articles from the TAG Cyber analysts, we explain and analyze the cyber risks associated with a major aspect of the new modern workplace—cloud email. We introduce the Abnormal Security platform to illustrate new controls for cloud email, as well as how practitioners can take advantage of modern technological innovations to stop socially engineered attacks and new emerging threats before they reach end-user inboxes.

USING ABNORMAL SECURITY TO REDUCE CYBER RISKS TO CLOUD EMAIL

DEVELOPED BY THE TAG CYBER ANALYSTS
EDITED BY DR. EDWARD AMOROSO

This book focuses on how cloud email risk can be effectively managed with a modern technology platform. We outline threats to cloud email and introduce advanced artificial intelligence protections using the Abnormal Security solution to illustrate a cyberdefensive approach.

CHAPTER 1

HOW SHOULD THE MODERN WORKPLACE ADDRESS CLOUD EMAIL SECURITY?

Why the modern and evolving workplace requires focused and ongoing security attention to cloud email threats.

Enterprise security teams must understand the mechanics of the modern workplace to design proper cyberdefensive schemes. Without such insight, the security functions and protection controls could be targeting the wrong types of threats. In fact, without a clear understanding of how employees actually work, security teams might just build security programs consistent with generic compliance frameworks.

To begin, we'll analyze three major trends in the modern workplace that directly impact how cybersecurity must be implemented.

Three Trends in the Modern Workplace

With so many professionals now working remotely, three major trends are changing how work is performed in the typical enterprise. These trends are unmistakable and have been accelerated by recent events such as the COVID-19 pandemic, as well as major advances in cloud infrastructure, SaaS tools, and collaboration systems such as Microsoft Teams and Zoom.

Additionally, they seem to transcend all industrial and government sectors and have been found to apply equally across organizations of varying sizes, scopes, and locations.

- ***Trend 1: Work from Anywhere –*** Work locations have shifted from physical corporate premises to virtually anywhere.
- ***Trend 2: Cloud Application Usage –*** Cloud-connected applications have grown significantly for employees, partners, and customers.
- ***Trend 3: Virtual Work Coordination –*** Work coordination in a typical organization has shifted from face-to-face meetings to virtual collaboration.

Email, in particular, has become the primary means by which remote workers collaborate virtually, and this helps explain why the cyberthreats to email systems and messages have exploded in intensity in recent years.

These workplace trends have led companies such as Zoom to emerge as major players in the enterprise market. It is not uncommon, for instance, for employees to spend their entire workday in online meetings or communicating via SaaS-hosted applications like Outlook and Slack. This contrasts with prior work generations who were more likely to be seated together in physical conference rooms.

Trend	From	To
Work Location	Office/Premise	Office/Premise
Application	Data Center-Hosted	Public Cloud/SaaS
Coordination	Face-to-Face Interactions	Virtual Collaboration

Figure 1. Shifts in the Modern Workplace

As one would expect, the impact of these workplace trends on cybersecurity is significant. Specifically, with targeted resources now virtual and largely dependent on email, adversaries have adjusted their focus accordingly.

Security Impact of Work from Anywhere

The shift toward employee work from anywhere was emerging long before people were staying home to avoid COVID-19. Today's workers typically seek to balance their work, family, life interests, and obligations. The flexibility of working anywhere represents a major benefit—one that can help companies attract and retain the best talent.

Two technologies have become more significant in the context of this shift: virtual conferencing and email. This should not come as a surprise to any observer, and the security implications here are immense. Email, in particular, has become the primary means by which remote workers collaborate virtually, which helps explain why cyberthreats to email systems and messages have exploded in intensity in recent years.

Advice for enterprise teams in this area should be clear: steps to augment existing email security controls should be a priority. In fact, if one were to conceptualize the single place where investments—even modest ones—in security will pay the greatest current dividend, it is hard to argue that email protections would not be the top choice. Security teams are thus wise to ensure they are working with the best email security vendors in the world.

Security Impact of Cloud Application Usage

The shift to cloud and SaaS has caused the focus of IT infrastructure to shift from a premise-based ecosystem to one that is both distributed and virtual. This change increases the flexibility of services, allows workers to share information, and provides ubiquitous access to data, applications, and shared services.

The shift has also transformed how third-party suppliers are handled, including how they are contracted, maintained, and coordinated. By using new capabilities like cloud-based portals for data sharing, teams can reduce the burden of awkward virtual private networks (VPNs) and similar utilities. But cloud and SaaS use also increases the cyber risk of mishandled data and misconfigured systems.

Once again, the need emerges for security teams to engage in partnerships with the best cloud and SaaS security solution providers—generally in areas related to ongoing posture assessment and dynamic threat mitigation. But just as with work from anywhere, we must acknowledge email's vital role in cloud and SaaS coordination. This underscores the urgency of partnering with an excellent email security vendor.

Security Impact of Virtual Work Coordination

Finally, when work is distributed everywhere and when resources are migrated to the cloud, work coordination becomes virtual. This has great benefits on the quality of work-life situations, such as travel and relocation. Many jobs that previously demanded in-person support can now be performed through work-from-anywhere arrangements—so long as the virtual work coordination can be managed.

The security implications are comparable to what is outlined above. And yes, email security emerges once again as a primary threat mitigation driver. The reality is that virtual work coordination, especially across organizations, relies heavily on email. This implies that to effectively mitigate the risks involved in virtual work coordination, it seems that email plays a significant role in determining the required level of security.

CHAPTER 2

WHAT ARE THE CYBER RISKS TO CLOUD EMAIL?

We explain the potentially significant cyber risks associated with cloud email for modern organizations

Modern email attacks have evolved from early-generation computer viruses stored in file attachments to comprehensive exploits that use intelligent strategies to find, collect and target important assets in an enterprise. This evolution has led enterprise security teams to increase their focus on threats from email, which today implies the use of public cloud-hosted email.

The Major Threat: Business Email Compromise

Scams and cons have always been popular crimes: even the father of John Rockefeller Sr., the billionaire founder of Standard Oil, was a **known scam artist** operating under an alias, as he sold elixirs and worked unethical land deals. Like all con artists, he worked within the confines of his time—and one can only imagine what the senior Rockefeller might have done with access to email.

Today, con artists and scammers have access to modern email infrastructure. As we all know, they take full advantage of email's free and open nature and the generally trusting nature of most email users, even in business contexts. In fact, BEC involves compromising email accounts and content for financial gain, usually with a transfer of funds.

The FBI reports a **typical cadence** to the modern BEC attack in the context of a timeline with four different steps by the intruders:

- **Step 1: Target Identification –** This involves research to create profiles for good targets. Employees working in finance-related positions are particularly vulnerable to this type of targeting.
- **Step 2: Target Grooming –** This includes spear phishing and supporting social engineering to begin establishing a context and a relationship in which to create the attack. This can take days or weeks to complete.
- **Step 3: Information Exchange –** In this step, the target is convinced the requested transfer or other operation is legitimate, and is usually provided with instructions for wiring money from a legitimate account to some established unauthorized recipient.

- **Step 4: Wire Transfer –** This is the ultimate goal for more BEC attacks, where funds move from the bank of the target organization to the malicious attackers, often connected to organized crime.

Figure 2. BEC Steps by Attackers

While BEC is certainly a major factor in the risk equation for corporate email use, the possibilities for committing fraud, abuse and other offensive attacks using email are considerably more involved

These four steps are useful to help defenders establish safeguards against the identification, grooming, information exchange, and transfer components of an attack. The good news is that excellent commercial options, including from major vendors such as Abnormal Security, are now available to provide practical and effective cyber risk reduction in these areas.

What is Email Fraud?

While BEC is certainly a major factor in the risk equation for corporate email use, the possibilities for committing fraud, abuse, and other offensive attacks using email are considerably more involved. This is an important observation for security teams, because while preventing funds transfer and other financial losses is essential, the obligation to defend email systems involves much more, such as:

- ***Phishing –*** This can be used as the basis for virtually any type of attack, including as the first step in nation-state advanced persistent threats (APTs).
- ***Spam –*** While often perceived as a nuisance, Spam email can be connected to fraudulent objectives, and with bulk sending, it often catches a percentage of victims.
- ***Spoofing –*** This is a common attack where email headers are forged, allowing for a wide assortment of attacks on recipients.

To address these ongoing cyber risks and protect the email channel, enterprises must partner with solutions providers who utilize innovative technologies, such as artificial intelligence and machine learning. In fact, it has become a mandatory aspect of most enterprise security programs to work with such vendors to reduce both the likelihood of receiving these attacks, as well as the consequence of such attacks if they should happen to reach end users.

CHAPTER 3

HOW IS ARTIFICIAL INTELLIGENCE USED TO ADDRESS EMAIL THREATS?

Enterprise security teams are excited about using the most advanced technologies to improve protection posture. While such innovation creates many new opportunities to reduce cyber risk, it also drives the need for practitioners to develop a reasonable working-level understanding of how these new technologies work, especially when some complexity is involved.

In this section, we focus on the most prominent of new technologies for cybersecurity—namely, artificial intelligence or AI.

How Does AI Work for Security?
The broad discipline known as AI references an assortment of technologies, algorithms, methods, and foundational math.

The first applications of AI for cybersecurity emerged in the early 2010s with work from experts such as **Stuart McClure,** then working at Cylance. The idea was then, and remains now, that the application of security-relevant data could be used to sufficiently inform learning algorithms to support the prediction of vulnerabilities or threats. This remains the canonical approach to using AI, and specifically machine learning, for cybersecurity.

The general strategy for machine learning in cybersecurity involves a training set obtained from security-relevant data, which is then analyzed by a learning algorithm associated with a hypothesis—usually whether some threat or vulnerability is present. As one would expect, the hypothesis is informed by features (attributes of the environment) and generates a predicted value (see Figure 3).

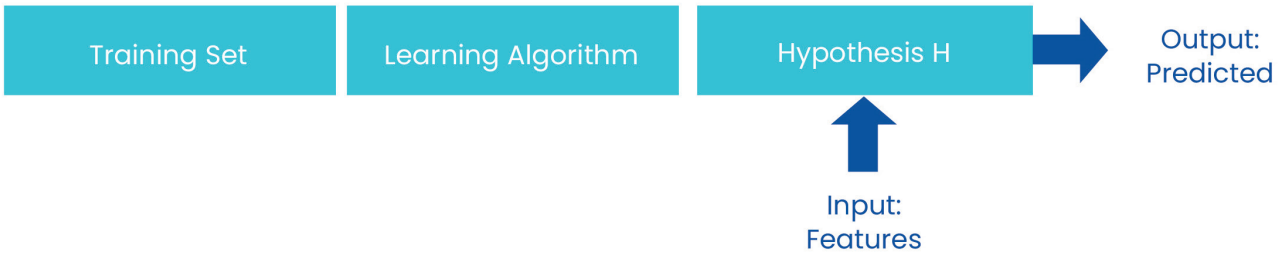

Figure 3. Canonical Use of Machine Learning for Cybersecurity

While most taxonomies for AI include a wide variety of strategies ranging from expert systems to complex neural networks, most cybersecurity applications of AI use machine learning, often based on simple linear regression.

While most taxonomies for AI include a wide variety of strategies ranging from expert systems to complex neural networks, most cybersecurity applications of AI use machine learning, often based on simple linear regression. This involves reviewing a series of input attributes related to the processing environment and then predicting, based on learned outcomes, whether a security issue exists.

Can AI Be Used to Protect Cloud Email?

One of the more promising areas in which AI has been applied to cybersecurity threats is the use of email—in particular, cloud email. Such an application is well-suited to AI due to the high volume of available data and the high likelihood of clear usage patterns being detected in normal user behavior. Combining these with good algorithms and strong computing platforms generally produces valuable results.

The canonical approach to machine learning can be used to illustrate the tailoring required for cloud email security. Training sets are derived from data collected during cloud email usage and learning algorithms are tailored to the cloud security email use cases of interest, including phishing and BEC. The hypothesis is then whether email attack evidence exists, and, finally, the output is whether to take action (see Figure 4).

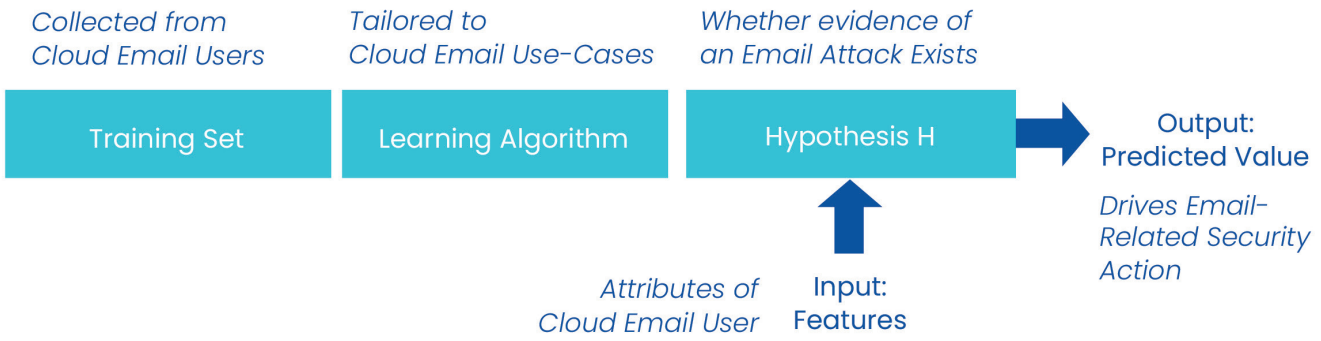

Figure 4. Tailoring Machine Learning to Cloud Email Security

By doing so, artificial intelligence can make decisions much faster and more effectively than users or security professionals. And as a result, the security algorithms can be trusted to detect and prevent email attacks, even those that have never before been detected by traditional tools.

In essence, these algorithms are constantly learning from the inputs so that they can make correct decisions about the most dangerous threats targeting organizations today.

While the role of AI in security is promising, enterprise teams are advised to develop insights into what truly meaningful AI technology is and what might be considered less relevant aspects of AI—including claims that are more marketing hype than operational reality. By understanding what AI is and how it works, security leaders can ensure that they have the knowledge they need to keep their organizations protected now and in the future.

CHAPTER 4

HOW DOES ABNORMAL SECURITY ADDRESS CLOUD EMAIL ATTACKS?

How the Abnormal Security platform detects and blocks the full range of cyberthreats to cloud email.

Using innovative security platforms to reduce the risk of email threats is no longer optional. Rather, modern email security solutions are a mandatory component of all protection architectures. This is not to say that complementary options such as procedural controls and security awareness are ineffective, but the intensity and velocity of inbound email attacks have increased to the point where sophisticated technology solutions must be engaged.

How Does the Abnormal Security Platform Work?
The cybersecurity platform from Abnormal Security leverages artificial intelligence (AI) to detect the presence of fraud or other attacks in enterprise email systems. The platform works by collecting and analyzing data from identities and their email communications for the purpose of making decisions—as with any AI system—which, in this case, focuses on whether a threat is present in the communications.

Abnormal analyzes key information including:

- ***Sender Identity –*** This has always been an important consideration in email security, but advanced AI can leverage more data and better algorithms to make determinations about the integrity of the sender.
- ***Message Content –*** This has also been a critical aspect of email security systems for many years, but as malicious email content has become more complex and contextual, the AI in the Abnormal platform can make better determinations related to security. This is especially true for text-based emails that have no typical indicators of compromise, as is often the case with socially engineered attacks.

Abnormal uses over 40,000 signals to identify and remediate malicious messages.

- ***Attachments and Links –*** The attachments and links included in any email must be viewed as potentially dangerous, especially links to websites that could include malware or other threats to the recipient or recipient's organization. Abnormal takes this a step further by understanding where second-stage links direct and their potentially malicious nature.

The Abnormal platform uses a web of prediction models—including natural language processing (NLP), natural language understanding (NLU), computer vision, and **BERT Large Language Model (LLM)**—to detect suspicious activity by analyzing topic, tone, sentiment, behavior, content and more. In fact, Abnormal uses over 40,000 signals to identify, and remediate malicious messages.

The solution also analyzes and understands the communication behavior of every identity for every customer to develop user-specific profiles. With this information, Abnormal can build a baseline of known-good behavior, which it then leverages to detect attacks by identifying unusual activity that deviates from the baseline.

HOW IS THE ABNORMAL SECURITY PLATFORM DEPLOYED?

The cloud-based platform can be natively integrated with the cloud email services in use at the enterprise—either **Microsoft 365** or **Google Workspace** via Microsoft or Google APIs. This is different from a traditional secure email gateway (SEG) approach as it requires no email rerouting (changes to MX records) and deploys quickly with no interruption to email flow.

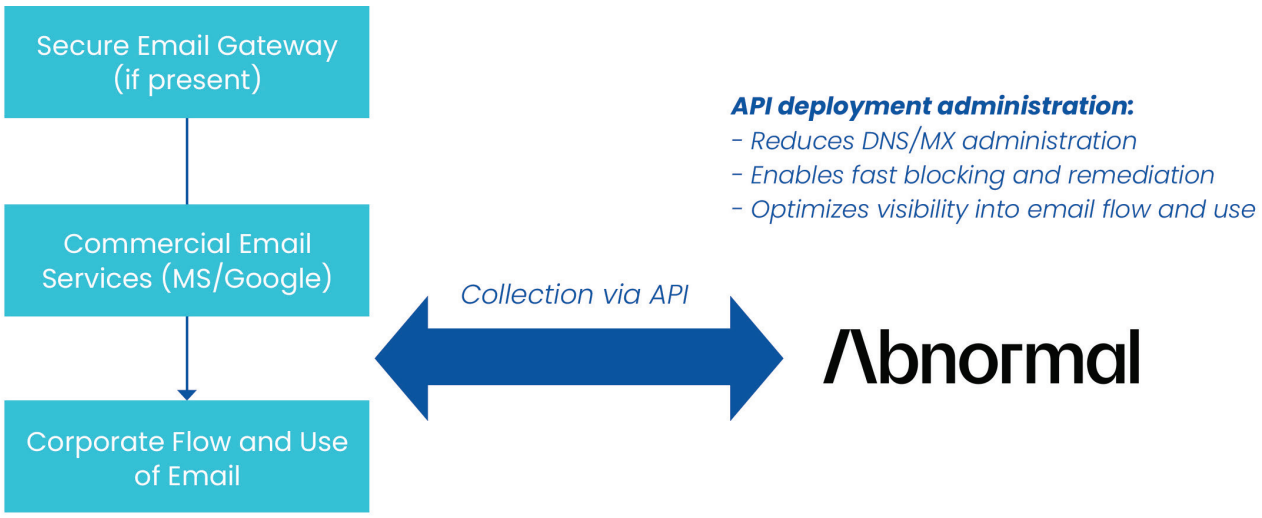

Figure 5. Abnormal Security Deployment to Cloud Service Infrastructure

The Abnormal solution triages, remediates and builds a repository of email detections available to third-party solutions like SIEM, SOAR and XDR platforms. These detections include the results of analyses performed

on user-reported phishing emails through **Abuse Mailbox** or potentially compromised email accounts identified by **Account Takeover Protection.** This interoperability increases the visibility and fidelity of events identified across the security stack, helping security teams better understand potential threats—and reducing response times as well as time spent on the investigation.

Customers can leverage out-of-the-box integrations to platforms, such as Splunk, QRadar, Microsoft Sentinel, Cortex XSOAR, Okta and many more. The Abnormal platform also offers REST APIs, allowing customers to build custom integrations with any third-party solution.

How Does Abnormal Leverage APIs and AI to Help Your Organization?

Abnormal's API integrations with cloud email platforms grant complete visibility into both external and internal email flows within the organization. This enables a better understanding of internal email patterns and contextual signals, crucial for detecting and addressing modern attacks that frequently originate from within the organization.

Combining the insights provided by this API integration with the powerful AI outlined above allows Abnormal to help organizations simplify email security, streamline operations, and prevent email attacks with the highest efficacy.

In the final section, we expand on why buyers would be wise to consider Abnormal Security as a valuable partner to future-proof their cloud email infrastructure from cyber threats.

CHAPTER 5

WHAT IS THE FUTURE OF CLOUD EMAIL SECURITY?

Some of the defensive and offensive trends for cloud email.

Unlike many security controls that have risen to prominence and then faded, protecting email has remained an essential aspect of enterprise security strategies. This follows the significant rise in email threats, as well as the continued dominance of email as the primary means for business communication, project coordination, and data sharing—regardless of organizational size, sector, or scope.

Keeping enterprises safe requires security leaders to stay up-to-date on the next-generation issues that will be relevant for **cloud-based email systems** in the immediate, near, and longer-term future.

OFFENSIVE ATTACK TRENDS FOR CLOUD EMAIL

Next-generation attacks on cloud email will build on existing methods toward more automated campaigns designed to produce multiple threat consequences. These attacks will continue to be performed by a wide range of threat actors, from nation-state-sponsored groups to new hackers. We anticipate that key aspects of future cloud email attacks will include the following:

- ***Autonomous Attacks –*** Malicious threats will emerge from autonomous weapons that use machine learning to identify cloud email vulnerabilities and predict outcomes.
- **Email Platform Attacks –** Future cloud email vulnerabilities will emanate from side channels, like connected third-party applications, that can leak information in unpredictable and uncontrolled ways.
- ***Email Assistant Attacks –*** The future email assistant will likely involve AI-based software that helps users perform email tasks—and will hence be vulnerable to attack.

One constant we expect to remain is that cloud email will persist as one of the primary means by which users communicate. It would be unwise to expect email to go away in any substantive manner or that hosting might shift away from public cloud infrastructure.

With advances in both offense and defense, especially using AI, the only way progress can be made in our cybersecurity industry will be for the defense to progress more quickly.

DEFENSIVE ATTACK TRENDS FOR CLOUD EMAIL

Next-generation defenses for cloud email will have to be designed to handle the types of attacks described above, especially in the context of more autonomous campaigns. Specific types of defensive strategies likely to be required in this context include the following capabilities:

- ***Predictive Modeling –*** Predictive modeling is essential to AI, and it stands to reason that this will be an important component of intelligent active defense for cloud email.
- ***Advanced Analytics –*** Data analytics will continue to be a major aspect of cloud email defense, albeit with increasingly advanced approaches.
- ***Coordinated Defenses –*** One should expect to see more coordination between different cloud email instances for sharing intelligence and cooperation on mitigations.

These defenses will have to be particularly good because the offense is always ahead of the defense: attackers only need to find one strategy that works, whereas organizations must continually defend against all tactics. With advances in both offense and defense, especially using AI, the only way progress can be made in our cybersecurity industry will be for the defense to progress more quickly. This will be a challenge.

HOW ABNORMAL SECURITY ADDRESSES EMAIL ATTACKS

The good news is that Abnormal Security is particularly well-positioned for both present-day cyberthreats to cloud email services, as well as future issues that are likely to emerge. Abnormal is an AI-based cloud email security platform that learns the behavior of every identity in your environment and analyzes the risk of every event to block even the most sophisticated email attacks.

The solution takes a fundamentally different approach to email security that is based on three core pillars:

- ***Identity-Aware –*** Ingests thousands of diverse signals derived from API integration with your cloud email platform to build profiles of every employee, vendor, application, and email tenant in your environment.
- ***Context-Aware –*** Monitors internal and external email traffic and continuously analyzes how identities behave in relation to one another to identify normal behavior.
- ***Risk-Aware –*** Correlates identity understanding and contextual norms to determine the risk level of every, event and identify anomalies with high precision.

These pillars enable Abnormal to provide the next generation of email security that delivers the highest rate of **attack detection and prevention,** identifying both known and never-before-seen threats with or without indicators of compromise.

WRAPPING UP

Throughout this book, we've explored myriad topics related to cloud email and the email threat landscape. We began by discussing why the modern and evolving workplace requires focused and ongoing attention to cloud email threats. Then, we dove into a few of the greatest ongoing cyber risks associated with cloud email. Our third chapter explained how AI technology is particularly useful for mitigating threats to cloud email environments, and our penultimate post examined how Abnormal's platform leverages AI to detect and block the full spectrum of email attacks. Finally, we reviewed some of the most important cloud email security trends.

We hope this book helps support your efforts to improve email security in your organization. For even more valuable information, please visit the **Abnormal Security Resource Center.**

See how Abnormal leverages behavioral AI to protect your organization from the full spectrum of email attacks. **Schedule a demo** today.

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm providing unbiased industry insights and recommendations to security solution providers and Fortune 500 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth insights, market analysis, consulting and personalized content based on thousands of engagements with clients and non-clients alike—all from a former practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman (lgoodman@tag-cyber.com) if you'd like to discuss this report. We will respond promptly.