The Seven Essentials of a Modern Email Security Platform

How businesses can reduce the time from phishing attack detection to response from hours and days to just seconds.

IRONSCALES

World's 1st *Automated Phishing* Prevention, Detection & Response Platform

Introduction

Did you know that any organization, regardless of size and the number of in-house security personnel employed, can now automatically prevent, detect and respond to all types of sophisticated phishing techniques in real-time. Now imagine how much time, money and resources it could save your company and how much burden might be alleviated from your Security and IT teams?

The reality of email security today, however, is that many businesses do not yet know that such technology exists or that it is possible to replace or supplement their existing solutions with ease. Therefore, most businesses continue to rely on static secure email gateways (SEGs) or the baked in security of email service providers, such as Office 365 and G-Suite. While such technologies are proven to reduce some risk, the frequency at which the email threat landscape now evolves, the high-rate of micro-targeted attacks and the speed at which threat intelligence must be consumed, has significantly reduced the effectiveness of both types of solutions.

This playbook introduces CISOs, security teams and analysts, and business decision makers to the seven essentials of a modern email security platform, while providing objective explanation as to why each essential is necessary and how they work together. At the conclusion of this paper, the reader will have a greater understanding of:

1. Why existing cloud and email security solutions are not built for advanced email phishing threat detection and response
2. How employees can become a vital layer of detection when incorporated holistically
3. Why the open decentralization of human intelligence is the future of email security
4. The importance of a closed feedback loop between technical and non technical controls
5. The ability to easily integrate or replace your existing email security stack, while keeping deployment seamless

The Pros & Cons of Traditional Email Security Tools

In order to fully understand why there must be seven essentials of a modern email security platform, one must first understand the pros and cons traditional email security tools and how and why such technologies struggle with the pace at which today's email threat landscape evolves, the high-rate of micro-targeted attacks and the speed at which threat intelligence must be consumed.

While secure email gateways, awareness training, DMARC and manual incident response tools have all proven to reduce risk, each of these technologies alone only solves a small piece of what is a very large and complex email security puzzle.

Secure Email Gateways	**Pro**: Proven track record of detecting known signature based attacks (messages containing links and attachments) **Cons:** Not built to detect more targeted and sophisticated file-less attacks such as Business Email Compromise (BEC), spoofing and impersonation. Also, once an email has landed inside of a mailbox, SEGs struggle to detect and remove the message.
Security Awareness Training	**Pro:** Great for building awareness and reducing employee click rates. **Con:** Attackers now deploy social engineering techniques that bypass technical defenses, making it almost impossible for busy employees to detect or recognize as malicious.
DMARC (Domain-based Message Authentication, Reporting and Conformance)	**Pro:** Built to identify a very specific and complex type of spoofing (exact domain spoofing) **Cons:** Only works when both the sender and the receiver are compliant and the type of attack that it is built to stop, exact domain spoofing, represents only a tiny subset of all email spoofing attacks.
Manual Incident Response Tools (Scripts, YARA rules, Signatures, Search based tools)	**Pro:** Proven to "clawback" known malicious emails that have already landed in an inbox. **Cons:** Requires significant analyst time to investigate and prompt remediation when time is critical and is also inefficient at identifying and stopping polymorphic attacks.

Introducing the Seven Essentials of a Modern Email Security Platform

Email phishing attacks have evolved from a mere nuisance in the early 2000s into the modern-day preferred attack vector for 9 out of 10 cyberattacks. Because of email's inherent insecurities and with upwards of 156 million phishing emails sent every day, most organizations now recognize the need for robust email security and phishing mitigation tools to ensure business continuity and tangibly reduce risk.

To mitigate the widespread risks of email phishing attacks, a modern email security platform must have these seven essentials:

1. Advanced malware and phishing/URL link detection
2. Mailbox-level threat detection (spoofing and impersonation protection)
3. Human-centric phishing detection
4. Post-email delivery protection (automatic incident detection & response workflow)
5. Decentralized crowd sourced intelligence (human vetted intelligence sharing)
6. Closed feedback loop
7. One platform, seamless deployment and integration

"Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities." - **Gartner**

"The combination of automated, technology-driven pre-incident protection, post-incident protection and incident response is by far the fastest and most effective approach – quantifiably reducing the organization's risk from phishing attacks by more than 70%, with ongoing upside." – **Aberdeen Research**

Essential #1

ADVANCED MALWARE & PHISHING URL/LINK PROTECTION

In the past anti-malware protection such as attachment & URL scanning may have been sufficient but today attackers are using more devious and sophisticated attacks by harvesting credentials of users through fake login pages using legitimate domains that go undetected. To detect and prevent against zero-days and phishing websites that attempt to steal users credentials, email security must provide more than basic signature detection and blacklists.

Advanced malware protection must now not only continuously inspect all inbound links and attachments but also utilize computer vision to detect in real-time visual deviations and determine whether or not a login page is legitimate, automatically blocking access to verified malicious URLs.

"While the core capabilities of anti-spam and signature-based antimalware may have been sufficient in the past, the threat landscape has shifted to more targeted attacks by hackers with increasing sophistication and nation-state connections, and those motivated by monetized cyber intrusions." - **Gartner**

Essential #2

MAILBOX-LEVEL THREAT DETECTION
(spoofing and impersonation protection)

Prevention technology must work in conjunction with advanced detections to identify sender impersonations, spoofing and business email compromise (BEC) that bypass gateway security tools. Absent of strong threat indicators (i.e. a one-to-one email from a legit domain to another that does not contain malware or malicious links discussing legit business activities), makes blacklists and blocked email-lists ineffective.

To detect malicious emails with and without payloads, the technology must have the capacity to dynamically self-learn mailbox and communication habits too using machine learning. This will allow for the detection of anomalies based on both email data and metadata (content and context) to improve trust and authentication of email communications.

"Impersonation attacks are the most difficult to detect and most critical to be solved in the secure email gateway. Email is not designed to truly authenticate sender identity. Efforts like DMARC to authenticate domains are not granular enough to authenticate users and do not address spoofing, cousin or look-alike domain usage." - **Gartner**

Essential #3

HUMAN CENTRIC PHISHING DETECTION

Technical detection alone is not enough, as email phishing is a human and machine problem that requires a human and machine solution. However, many businesses are not investing in advanced phishing protection education that can empower employees to identify and mitigate socially engineered attacks, such as business email compromise. When layered into a holistic defense system, employees can become a vital layer of detection.

By decentralizing and distributing reported incidents from employees to security teams, companies can mitigate the risk of malicious emails by working in collaboration, within the same platform. And collaboration isn't limited to just YOUR employees: imagine having the input and value of others, including leading SOCs and other enterprise security resources.

"Defending as a pack has advantages over defending yourself in isolation." - **Gartner**

Essential #4:

POST EMAIL DELIVERY RESPONSE
(automatic incident detection & response workflow)

No prevention and detection will stop every single phishing attack, and with time being of the essence for phishing mitigation, any email security technology must provide end users(employees) with automated incident response and remediation across all affected mailboxes.

Such technology must also be able to collect email threat data and alerts from different sources, including other SOC teams around the world and employee reports, so that incident analysis and triage can be performed automatically to improve efficiency. This helps to streamline responses according to a standard workflow while making it quick and easy for security analysts to classify reported email incidents at the click of a button.

"In an era of continuous compromise, enterprises need to shift from a mindset of "incident response" — wherein incidents are thought of as occasional, one-off events — to a mindset of continuous response." - **Gartner**

"The median time the first user open of phishing emails is less than 2 mins." - **Verizon DBIR report**

Essential #5

DECENTRALIZED ACTIONABLE CROWD SOURCED INTELLIGENCE

(human vetted intelligence sharing)

Decentralized intelligence sharing within a platform that is actionable through automation, empowers organizations to proactively prepare for trending email phishing attacks.

By leveraging an entire virtual global analyst community, decentralization of intelligence sharing can also help businesses utilize data to prepare for what the next attack will look like and to proactively prevent similar or trending attacks from infiltrating or repeat attacks from occurring. This virtual SOC model exponentially improves as the global analyst community grows.

"You probably should not be using threat intelligence unless you can act on it. If you can't act on it, it's probably not worth consuming that data..."

"...The Holy Grail for threat intelligence, like anything in security, is automation, of course, but not all organizations are equipped to go there just yet." - **Jason Trost, vice president of threat research at threat intel firm Anomali**

Essential #6

CLOSED FEEDBACK LOOP

Orchestrating threat intelligence from technical and non technical controls into a continuous feedback loop is critical in preventing phishing emails from going undetected due to lack of communication between controls.

By continuously feeding machines intelligence from multiple sources, both internal and external, such as analysts decisions and employee reports, 3rd party threat feeds, sandbox/threat emulation and crowd sourced intelligence, email security can adapt and get smarter by predicting, preventing, detecting and responding in real-time.

To reduce risk, machines driving the platform must constantly and in real-time be made aware of:

1. Content – what is being detected by different content scanners of different companies
2. Context – what is being detected at the mailbox level
3. Collaboration of Experts – what is being detected by decentralized threat intelligence (i.e., humans)

"We can't escape the fact that humans and machines complement each other and together they can outperform each alone. ML reaches out to humans for assistance to address intent uncertainty. ML aids humans by supporting administrator awareness and providing assistance to higher-tier SOC analysts." - **Gartner**

Essential #7

ONE PLATFORM, SEAMLESS DEPLOYMENT & INTEGRATION

Email security is saturated with point solutions and scattered semi-automated tools that require organizations to purchase multiple non-integrated technologies, straining budgets and requiring lots of analyst time and resources.

Combining all of the essential functionalities to combat modern email threats into one single platform that can easily integrate or replace your existing email security stack, while keeping deployment seamless, scalable and the total cost of ownership low is a major benefit to security teams.

"Supplement gaps in the advanced threat defense capabilities of an incumbent SEG by adding a specialized product tailored for this purpose, if replacement is not an option. Not all SEG vendors include best-of-breed advanced threat defense capabilities." **- Gartner**

Summary

In conclusion, the frequency at which the email threat landscape now evolves, the high-rate of micro-targeted attacks and the speed at which threat intelligence must be consumed, has significantly reduced the effectiveness of secure email gateways and the security baked into G-Suite and Office 365.

To truly mitigate the risk of email phishing attacks, businesses must look towards technology that provides advanced malware and phishing link detection; mailbox level spoofing and impersonation protection, human-centric phishing detection, post-email delivery protection and decentralized intelligence that is seamless to deploy and works within a closed feedback loop.

About IRONSCALES

IRONSCALES multi-layered advanced phishing threat protection platform combines technical controls to block as many phishing attacks as possible and end-user controls to help users detect more sophisticated attacks at the mailbox-level, while incorporating employees as part of the defense strategy to detect what is missed by technology.

Our advanced threat protection platform uniquely combines human intelligence with machine learning and AI to automatically prevent, detect and respond to advanced email threats and predict future attacks, so if one control fails, there are others to compensate while maintaining an adaptive security architecture.

IRONSCALES is proven to reduce the time from phishing threat discovery to attack remediation from days, weeks or months to just seconds or minutes.

Reduce phishing risk with IRONSCALES advanced phishing threat protection platform, which leads the email security industry in speed, efficacy and durability.

Visit our website | Follow us on Twitter | Follow us on LinkedIn

IRONSCALES
World's 1st *Automated Phishing*
Prevention, Detection & Response Platform