Mighty Guides

Sponsored by

IRONSCALES
SAFER TOGETHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

How to Stay Ahead of the Growing Email Security Threat

A Guide to Securing Your Google Workspace Email

Table of Contents

Introduction

Email is a necessity, yet simply clicking a link can expose you or your organization to infection. The Verizon 2021 Data Breach Investigations Report found that phishing was present in 36% of breaches with Business Email Compromises (BECs) as the second-most common form of Social Engineering. These trends continue even though companies spend more time and money on email security than ever before.

This eBook investigates why more layers of email security fail to prevent these sophisticated attacks and discusses an innovative new approach to email security that is meeting with success.

All the best,
David Rogelberg
Editor,
Mighty Guides Inc.

Foreword

We commissioned this Mighty Guide so that you could hear from your peers in the field about the experiences they've had with securing their own web-based email, specifically Google Workspace. They detail their experiences to date, including where existing solutions have fallen short. Enjoy the book!

Regards,
Eyal Benishti
CEO,
IRONSCALES

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

IRONSCALES
SAFER TOGETHER

IRONSCALES is an email security company focused on fighting back against today's modern phishing attacks. Our self-learning, AI-driven platform continuously detects and remediates advanced threats like Business Email Compromise (BEC), credential harvesting, Account Takeover (ATO), and more. Our powerfully simple email security solution is fast to deploy, easy to manage, and keeps our customers safe.

Founded in Tel Aviv, Israel in 2014 by alumni of the Israel Defense Force's elite Intelligence Technology unit, IRONSCALES is headquartered in Atlanta, Georgia, with an additional office in London. We are proud to support thousands of customers globally with our award-winning, analyst-recognized platform.

IRONSCALES
SAFER TOGETHER

Meet Our Experts

Eyal Benishti
CEO,
IRONSCALES

Steven Parker
CISO,
TBC Corporation

Pieter VanIperen
SVP, Global Head of
Cloud Security,
21st Century Fox

Shitanshu Kumar
Director, Security Engineering
Operations & Compliance,
iQor

Lance Auman
Lead Security Engineer,
iHerb LLC

Jared Couillard
VP,
IT and Security Officer,
Cohere Health

Bob Fabien Zinga
Head of Information Security,
Directly

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IRONSCALES
SAFER TOGETHER

Chapter One

Why GWS Email Security Falls Short

Google Workspace has become a popular cloud-based email platform. It has also become a significant target for phishing attacks. Malware, known viruses, and even spam are typically stopped in Google Workspace filtering, but socially engineered attacks, like phishing and tightly targeted attempts like spear phishing, are rarely blocked or flagged as they traverse the Google Workspace platform.

As with most email providers, Google Workspace honors the Sender Policy Framework (SPF). These are text records configured in a sender's domain that provide a mechanism to identify messages that are approved to be sent "from" an organization. The record includes the source IP ranges of the multiple platforms sending such messages, like customer order emails or marketing department campaigns. Google checks incoming message domains to determine if the source IP is included in that originating SPF record. If not, then the email may be flagged as spam or potentially malicious.

Domain-based Message Authentication, Reporting & Conformance (DMARC) extends this functionality by checking inbound "@company.com" emails to validate Domain Key Identified Mail (DKIM), a certificate published by company.com, in conjunction with the associated SPF record.If the two records are found to be in alignment with inbound email, then the message is considered legitimate and allowed to pass. An organization can choose to audit those messages while still learning their environment but ultimately will want to assign the record to be rejected to effectively block spoofed messages.

Google Workspace

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

"Google Workspace provides basic protection, but there are too many ways to slip past these defenses. The platform lacks an automated way to pull malicious messages from your inboxes, causing security to race the clock before a user can unwittingly click the link."

Lance Auman

Lead Security Engineer,
iHerb LLC

IRONSCALES
SAFER TOGETHER

As one might imagine, SPF, DKIM, and DMARC compliance can be effective in protecting against inbound spoofed emails, but they also put a significant administrative burden on security teams to report, configure, and maintain. The full suite can require significant time, effort, and expense to ensure that vital ecommerce emails, marketing campaigns, or other approved methods of sending as a given organization are not impeded or blocked.

> Attacks through email are becoming more sophisticated—and more common. It's still the number one vehicle for cybercriminals to get inside an organization.

Eyal Benishti
CEO, IRONSCALES

Google employs Transport Layer Security (TLS) when sending and receiving email messages and further encrypts data at rest while in a user inbox. In this manner, Google ensures the integrity of email in general, but Google does control the reliability of sender email, including whether the sender truly is who they purport to be. Messages traverse the platform through multiple layers of security filters, but spoofed messages are still delivered unless IT departments fully configure DMARC compliance.

In fact, most email security solutions fail to protect against socially engineered attacks because they focus on the wrong things. Their reliance on policy configurations and monitoring of large scale data patterns limits them to finding known security threats. For all the time it takes to configure and maintain them, these tools offer little protection against well-engineered, targeted phishing and BEC attacks.

To protect against those kinds of attacks, you need something entirely different.

"Google Workspace utilizes a shared security model for keeping users' data safe. This puts the onus of data security on the organization. Especially with a platform that is so easy to use, it is essential to address these security risks or face a potential loss of data."

Steven Parker
CISO,
TBC Corporation

Key Points

- Most email security solutions depend on policy configuration and static signature databases to identify threats. They require a lot of policy management and upkeep to stay current with the latest threats. The speed at which attackers change their attack strategies makes keeping up impossible.
- Google Workspace offers no protection against socially engineered attacks, leaving customers to identify any security threats in their inbox.
- Most email security solutions fail to protect against socially engineered attacks because they focus on the wrong things. For all the time it takes to configure and maintain them, these tools offer little protection against well-engineered, targeted phishing and BEC attacks.

"Email attacks have changed, email delivery has changed, and so security is changing to keep pace."

Pieter VanIperen

SVP, Global Head of Cloud Security,
21st Century Fox

Chapter Two

How an Integrated Cloud Email Security solution stays ahead of evolving threats to GWS: focus on the inbox

There is one place where both technical and human elements of the email security challenge come together: the individual email user's inbox.

An integrated cloud email security solution (ICES) combines technical and human detection and response into a single platform that investigates email traffic at the inbox level. Here's how it works:

- **Technical detection and response**. Every email user has a unique pattern of inbound email. To identify an attack that has never been seen before and has no known signature, you must monitor and analyze email traffic across the entire organization, right down to each individual user's inbox. An ICES platform does this automatically, in real-time, using artificial intelligence (AI)–powered detection and response technology. Powerful AI algorithms, optimized for this specific task with visibility across every user, every inbox, and every email are the keys to blocking socially engineered email attacks. IRONSCALES can catch up to 99 percent of socially engineered attacks using this process.

Google Workspace

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

"Google Workspace includes some security features that need to be optimally configured and still may not be enough protection. Organizations that wish to protect most effectively protect against increasing and more sophisticated phishing attacks will need to partner with vendors that specialize in services like Integrated Cloud Email Security."

Bob Fabien Zinga

Head of Information Security, Directly

IRONSCALES
SAFER TOGETHER

- **Human detection and response**. For maximum effectiveness, you also need a machine-human feedback loop that includes both security analysts and email users. This feedback loop enables users to flag suspicious emails they receive and analysts to quickly assess the flagged messages. Users receive real-time notifications on items they flag and any valid attack emails that land in their inbox. The platform itself becomes a continuous training tool for users, keeping them aware of and alerting them to the possibility that they may be the target of a phishing attack. This feedback loop also continuously refines the AI detection and response algorithms. By integrating human and technology elements in this way, IRONSCALES can bump the catch rate close to 100 percent.

> Most email security solutions try to detect an indication of compromise. This is intelligence-based threat detection. But if an attacker is using social engineering to make someone do something they are not supposed to do, the only way you are going to know that and block it is if you are inside that email user's mailbox.
>
> 
>
> **Eyal Benishti**
> CEO, IRONSCALES

An ICES platform should be deployable in minutes and require little to no configuration. IRONSCALES ingests and analyzes ninety days of email history to establish a baseline pattern for each user's mailbox. Within minutes, its AI algorithms gain deep inbox-level awareness of email usage patterns in any email environment—cloud, on-premises, or hybrid.

"ICESs utilize advanced methods of protecting users against malicious emails before they get to their inbox. They are the next generation of email security tools."

Steven Parker

CISO,
TBC Corporation

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IRONSCALES
SAFER TOGETHER

ICES platforms can perform basic email security functions, such as spam detection, malware and virus detection, and attachment inspection but also some more advanced protections. One feature, that is included in most secure email gateways but not a component of Google Workspace, is to detonate email links and attachments in a secure sandboxed environment that tracks and reports on all associated indicators of compromise such as registry settings, file hashes, or called DNS names.

> We apply machine learning at the mailbox level to learn unique patterns of each individual email user. We detect unusual emails this way. We use the platform to create a community of security teams that work collaboratively but anonymously to identify difficult-to-detect trends.

Eyal Benishti
CEO, IRONSCALES

Sandboxing is a computationally time-consuming process and therefore is unable to examine all inbound messages. This means that for a given attack, many emails may have already been delivered before they are determined to be malicious. Unlike Google Workspace, an ICES can automatically remove those messages out of affected user inboxes, ideally before an unwitting user is able to do unintentional damage.

ICESs should also include supporting features that fall outside the general purview of email providers such as Google Workspace. Security teams can emulate known phishing emails to create realistic simulations for users as a mechanism to test security awareness. Users that fall prey can click themselves into ad hoc training segments that augment routine security training.

"Though Google Workspace has numerous security features, human errors or phishing-prone users can easily invite attacks just by clicking a malicious link. Inline solutions like ICESs can further secure an organization against attacks."

Shitanshu Kumar

Director, Security Engineering Operations & Compliance, iQor

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IRONSCALES
SAFER TOGETHER

The real strength of an ICES, however, is the ability for the sophisticated AI to detect complex attacks that may combine multiple attack types at once.

This all sounds great, but do you really need another email security tool?

Email security protocols like DMARC offer some core defenses, but not without significant administrative overhead. Google Workspace offers a baseline of security protections, but it pales much beyond mitigating simple threats such as spam or malware-laden attachments. Secure email gateways offer more security features but with an added expense and complexity that, in the end, is still too anemic to counter modern threat actors. To gain maximum protection against sophisticated socially engineered phishing and BEC email attacks, you need a top-performing ICES.

"In the rising era of email-delivered ransomware, the stakes continue to grow that a single click can cripple your organization. Google Workspace, alone, simply does not provide sufficient security breadth or depth to keep pace with the modern threat environment."

Lance Auman

Lead Security Engineer,
iHerb LLC

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IRONSCALES
SAFER TOGETHER

Key Points

- To identify an attack that has never been seen before and has no known signature, you must monitor and analyze email traffic across the entire organization, right down to each individual user's inbox.
- For maximum effectiveness, the ICES needs to provide a machine-human feedback loop that includes both security analysts and email users. Users receive real-time notifications on items they flag and any valid attack emails that land in their inbox. The platform itself becomes a continuous training tool for users.
- The best ICESs can be implemented in minutes and require no configuration. IRONSCALES ingests and analyzes ninety days of email history to establish a baseline for each user's mailbox within minutes.

"ICESs are becoming an essential part of the future of cloud email security because they use sophisticated anomaly detection techniques to protect against Business Email Compromise (BEC) and account takeover attacks."

Bob Fabien Zinga

Head of Information Security,
Directly

Chapter Three

How an ICES like IRONSCALES keeps your GWS email more secure at a lower cost

A good ICES saves time and money in ways that can benefit both business adopters and security service providers.

For businesses, an ICES significantly lowers the risk of being victimized by a sophisticated phishing attack that may be ransomware, part of a more subtle attack designed first to infiltrate and then to exfiltrate sensitive data or a targeted BEC attack designed to take your money.

> Instead of augmenting an email security gateway, you can get rid of it altogether.
>
> 
>
> **Eyal Benishti**
> CEO, IRONSCALES

In addition to risk reduction, the IRONSCALES ICES is easy to implement, requires no configuration or policy maintenance, catches a high percentage of attacks automatically through AI algorithms, and remediates a significant percentage of email anomalies.

Google Workspace

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

"With a proper ICES, businesses are more likely to stop a phishing attack before it starts. This means less time is spent investigating a breach, cleaning up infected machines, and dealing with other consequences. That reduction in time also means a reduction in cost."

Pieter VanIperen

SVP, Global Head of Cloud Security,
21st Century Fox

IRONSCALES
SAFER TOGETHER

These all contribute to a significant savings in labor required to manage email security. We have found that IRONSCALES can reduce time spent in manual email analysis by 90 percent.

Further, it can reduce the complexity of your security stack by consolidating the quantity of security platforms required, along with their time-consuming complexity and cost.

For service providers, an ICES is a low-cost technology that managed services providers (MSPs) and managed security services providers (MSSPs) can add to their portfolio of security offerings. It provides a highly effective managed email security solution that quickly adapts to the unique usage patterns and threat environments of their clients.

To learn more about how an ICES can simplify your security stack, reduce the burden of email security monitoring and remediation, lower costs, and greatly improve your security posture please visit ironscales.com.

"Freeing security staff from securing an email platform is a force multiplier, allowing them to broaden scope to secure the rest of your security stack, devices, and critical applications."

Lance Auman

Lead Security Engineer,
iHerb LLC

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IRONSCALES
SAFER TOGETHER

Key Points

- To provide companies with the security and value they need, an ICES must be easy to implement, require no configuration or policy maintenance, and catch/automatically remediate a high percentage of attacks through AI algorithms.
- An ICES significantly lowers the risk of being victimized by a sophisticated phishing attack that may be ransomware, part of a more subtle attack designed first to infiltrate and then exfiltrate sensitive data, or a targeted BEC attack designed to take your money.
- IRONSCALES is a low-cost technology that MSPs and MSSPs can easily add to their portfolio of security offerings. It is a highly effective managed email security solution that quickly adapts to the unique usage patterns and threat environments of their clients.

"As platforms are more connected, and therefore more vulnerable than ever before, leveraging an ICES is no longer just nice to have. It is necessary to support a safe and reliable environment for your end users."

Jared Couillard

VP, IT & Security Officer,
Cohere Health

Learn More About Our Experts

Eyal Benishti, CEO, IRONSCALES

As chief executive officer of IRONSCALES, Eyal Benishti pioneered the development of the world's first self-learning anti-phishing email security solution for automatic prevention, detection, and autonomous incident response to cyberattacks. Before founding IRONSCALES in 2013, Eyal was a security researcher and malware analyst and held many R&D roles. He holds a bachelor's degree in computer science and mathematics from Bar-Ilan University in Israel.

Steven Parker, CISO, TBC Corporation

Steven Parker is an innovative, business focused, information security professional with 20 plus years' experience implementing information security programs from a risk-based perspective for a variety of verticals. He has served in executive and senior management positions, with responsibilities including strategy development and execution, strategy and tactical alignment, and risk and crisis management, and holds the following certifications: CISSP, C|CISO, CISA, CFE, and ITILv3.

Pieter VanIperen, SVP, Global Head of Cloud Security, 21st Century Fox

Pieter VanIperen is a software architect, security expert, ethical hacker, and adjunct professor of Code Security at NYU. He has founded/co-founded multiple startups and is currently the Managing Partner at PWV Consultants where he leads a group in design and technology. He authored the HAZL programming language and served as the CTO of several digital and Fortune 500 companies. His expert consulting and advisory work spans several industries.

Shitanshu Kumar, Director, Security Engineering Operations & Compliance, iQor

Shitanshu Kumar, CRISC, CISM, CEH, is an information security professional with over 17 years' experience in information security, risk management, operations, government compliance, and product management. He received the CISOConnect Cyberwarrior award in 2021 and the Defenders 100, CIOAxis InfosecMaestros, and CISO 100 India awards three years running, from 2019 to 2021. He works across the security lifecycle with a focus on developing holistic security solutions.

Lance Auman, Lead Security Engineer, iHerb LLC

Lance Aumen has over 25 years of proven experience managing, architecting, securing, and supporting complex information systems in large enterprises across multiple verticals. In his current role, he serves as the lead security engineer for iHerb, a multi-billion-dollar global ecommerce platform. In prior roles, he served as Security Architect for Irvine USD, VP of Information Security for Penfed Credit Union, and Infrastructure Director for San Francisco USD.

Jared Couillard, VP, IT and Security Officer, Cohere Health

Jared Couillard is an accomplished IT executive with extensive success establishing and maintaining the enterprise vision, strategy, and program to secure information assets and technologies. He is skilled in cyber security, threat intelligence, INFO-SEC, and policy creation and has 12+ years leading IT and security organizations in the healthcare and fintech sectors, covering everything from standing up foundational security programs to attaining HiTrust and SOC2 certifications.

Bob Fabien Zinga, Head of Information Security, Directly

Bob Fabien "BZ" Zinga leads and manages a cross-functional annually-audited information security program and serves as Information Warfare Commander and Commanding Officer in the US Navy Reserve. Throughout his career, he has been setting the vision, driving the strategy and governance framework, establishing effective policies and standards, and managing the cybersecurity risk and compliance functions within higher education, state and federal governments, and defense and technologies industries.

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IRONSCALES
SAFER TOGETHER

Partner with IRONSCALES

Phishing attacks are the biggest threat your customers face today. IRONSCALES offers a powerfully simple anti-phishing solution that is fast to deploy, easy to use, and protects your customers against today's most dangerous phishing threats.

Partner Benefits

- Short sales cycles
- Bulk pricing
- Easy access to POCS and demos
- Ongoing training & support
- Multi-tenant MSSP deployments

> "IRONSCALES' comprehensive artificial-intelligence phishing protection is aligned with our Dark Rhino promise on delivering value through innovation, so this partnership is a big win for us and our customers.
>
> Kevin Casey,
> CEO of Dark Rhino Security

www.srccybersolutions.com +91 120 232 0960 / 1 sales@srccybersolutions.com

Learn more at http://www.srccybersolutions.com