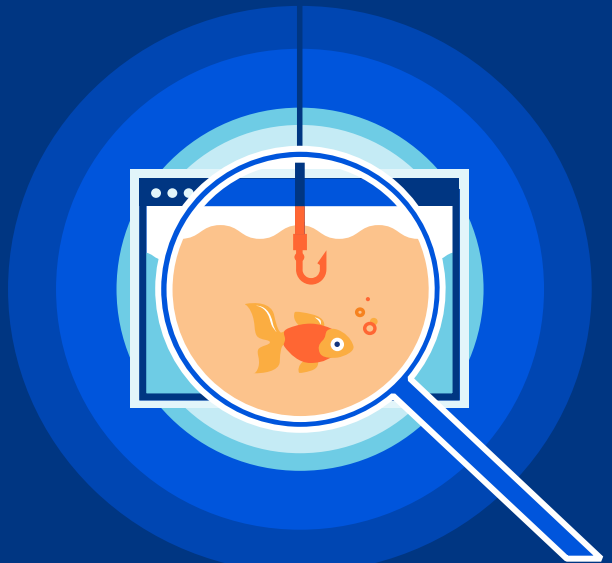
CLOUDFLARE

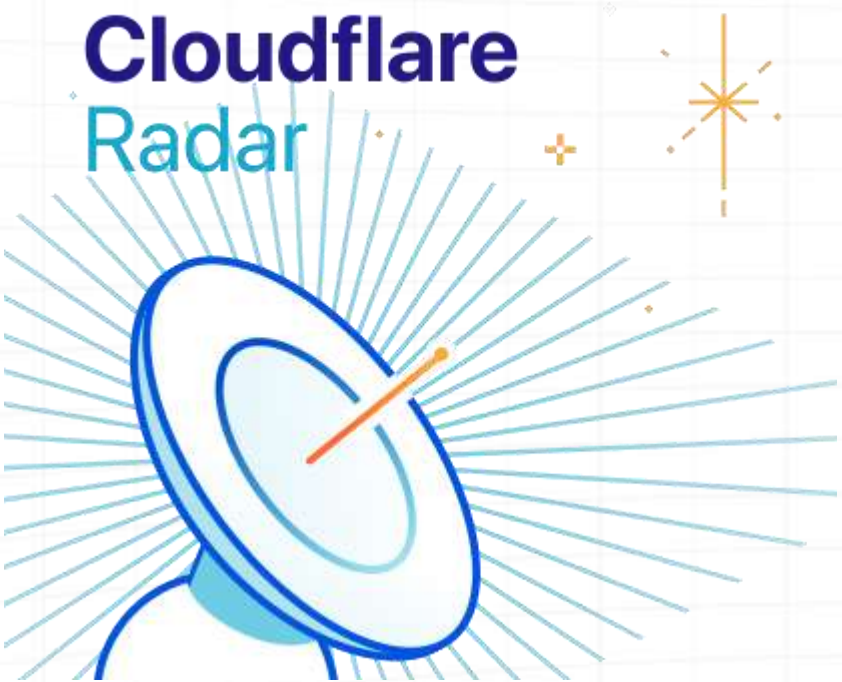
The (hard) key to stop phishing

How Cloudflare stopped a targeted attack and you can too



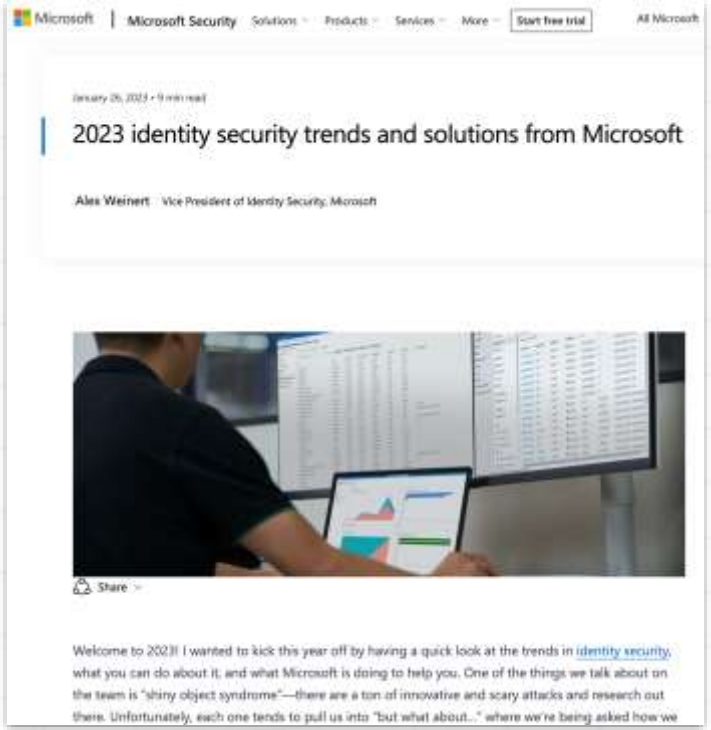
CLOUDFLARE
Anand Guruprasad
Solutions Leader, Canada

2023 Vancouver International Privacy & Security Summit



Time Horizon: 2023

Recent News



https://www.microsoft.com/en-us/security/blog/2023/01/26/2023-identity-security-trends-and-solutions-from-microsoft/

- >99.9 percent of accounts that are compromised don't have MFA enabled
- "It is critical not just to use multifactor authentication, but to use the right multifactor authentication"
- Just 35% reported their organizations have a comprehensive knowledge of relevant threat actors and their tactics, technique, and procedures (TTPs)

https://www.itbrew.com/stories/2023/02/21/most-cybersecurity-leaders-are-making-decisions-without-understanding-their-attackers

Recent News

FORTUNE RANKINGS MAGAZINE NEWSLETTERS PODCASTS MORE SEARCH SIGN IN

COMMENTARY | CYBERSECURITY

The cost of cybersecurity insurance is soaring–and state-backed attacks will be harder to cover. It's time for companies to take threats more seriously

BY SHMULIK YEHEZKEL

The rise in state-backed cyber attacks has put off insurers.

https://fortune.com/2023/02/15/cost-cybersecurity-insurance-soaring-state-backed-attacks-cover-shmulik-yehezkel/

- "The average price for cyber insurance in the U.S. rose 79% in the second quarter of 2022, after more than doubling during each of the previous two quarters"
- Underwriters now take a fine-toothed comb to commercial cybersecurity practices, and regulators are starting to do the same

https://www.propertycasualty360.com/2022/01/18/cyberattacks-lead-to-increased-scrutiny-how-can-companies-stay-ahead-of-the-curve-414-216174/

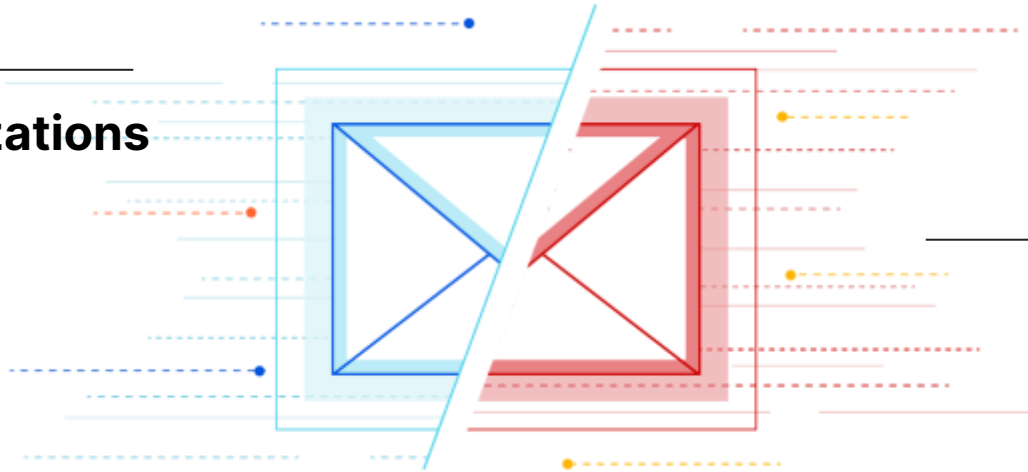
CLOUDFLARE

Email is the ...

#1 way organizations communicate

70%

of organizations use cloud email solutions today. (Gartner)

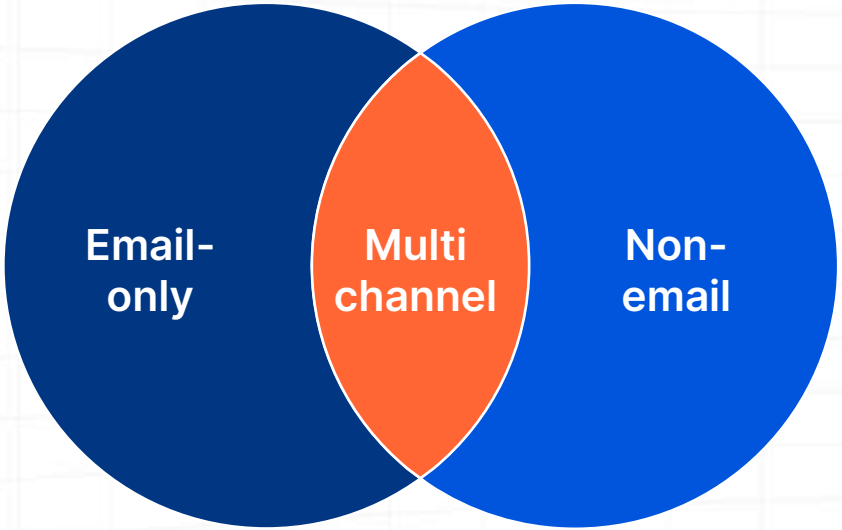


#1 threat attack vector

91%

of all cyber attacks begin with a phishing email. (Deloitte)

Phishing attack vectors
Different channels, different outcomes



Account takeover

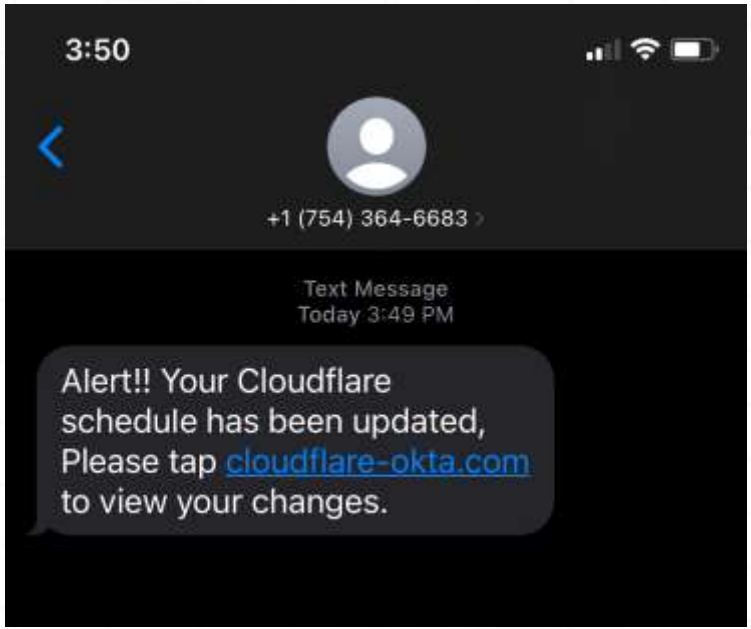
A link in bigger supply chain attack

Data exfiltration, e.g. PII and IP

Malware attacks, e.g. ransomware

One day in August…

What Cloudflare employees saw



Threat Group and Tactics

Attack Tactics

SMishing

Phishing Text Message Sent to Victim

Credentials Sent to Threat Actor

Phishing site sends credentials and MFA token via Telegram to attacker

Deploy Remote Access Toolkit

Allow persistent threat and potential for ransomware through lateral movement

Left of Boom | **Right of Boom**

Credential Harvest

Phishing site harvests
1. Credentials
2. MFA One Time Passcodes

Data Exfiltration

Threat actor exfiltrate data attempts privilege escalation

Campaign Results

https://threatpost.com/0ktapus-victimize-130-firms/180487/

~130 Organizations Targeted
~10k Compromised Credentials
~5k Compromised MFA Codes

https://www.group-ib.com/blog/0ktapus/

Lessons Learned

Cloudflare's Zero Trust platform leveraged to mitigate this and similar attacks

#	Our response
1	●1 min after attack, SIRT was informed; no evidence of compromise via directory provider logs ●9 min after attack, SIRT sent an internal warning to all employees across chat & email
2	●3 min after attack, SIRT added domain to SWG to block access. Later, isolated access to all newly registered domains and seized control of domain. ●37 min after attack, DigitalOcean shutdown the attacker's server via our collaboration
3	●1-37 min after attack, SIRT killed active sessions via ZTNA, plus 48 min after attack, SIRT reset credentials & initiated scans for the identities & devices with unverified 2FA per our activity logs
4	●Intel from server indicated actor was targeting other orgs, including Twilio, and SIRT shared intel ●SIRT blocked IPs used by threat actor from accessing any Cloudflare service

Reinforced the importance of what we're doing well, and everything you can do, too

1. **Adopt a phishing-resistant MFA**
   Not all MFA provides the same level of security

2. **Implement selective enforcement**
   with identity- and context-centric policies

3. **Enforce strong auth everywhere**
   All users and apps; even legacy non-web systems

4. **Adopt Zero Trust via one platform**
   Easier, faster operations & improved security posture

5. **Establish paranoid, blame-free culture**
   Report suspicions early and often

Five recommendations

Recommendation 1: Implement phishing-resistant MFA

Not all MFA provides the same level of security

Time-based one-time password apps

Vulnerable to phishing via MitM (on-path) attacks

FIDO2-compliant security keys

Verification with public-key cryptography and Identification embedded into physical media devices

FIDO2 not automatically compatible

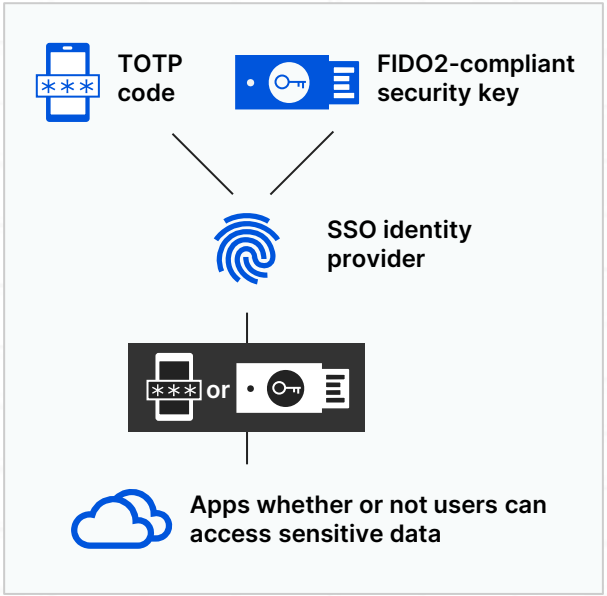
with all Internet, SaaS or self-hosted applications

Best practice from Cloudflare IT

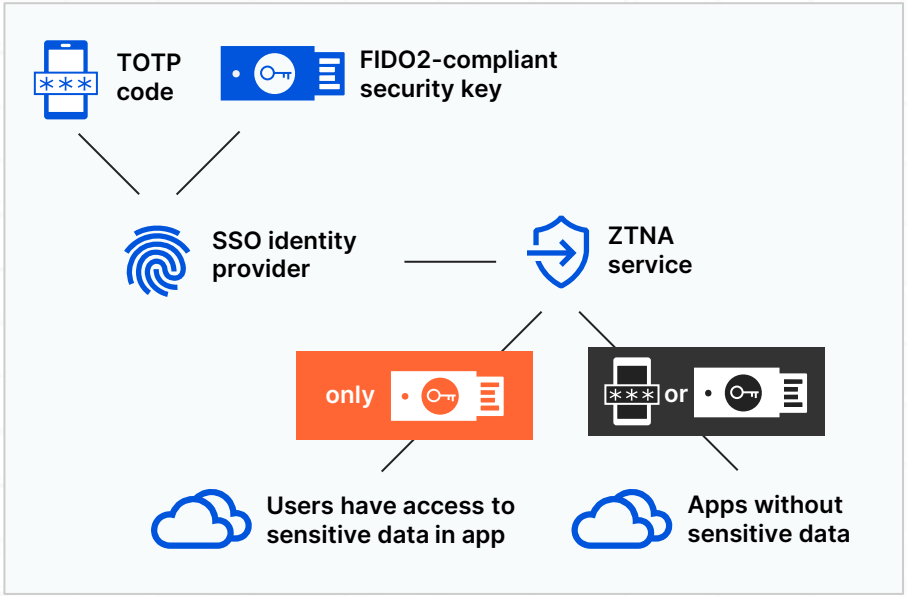
- Plan to support mobile devices and authentication with WebAuthn in the mobile context.
- To meet FedRAMP compliance, we also opted to purchase two sets of keys for each employee, one NFC key for mobile, and one Nano YubiKey for laptop (FIPS if applicable)

Recommendation 2: Implement selective enforcement with identity- and context-centric policies

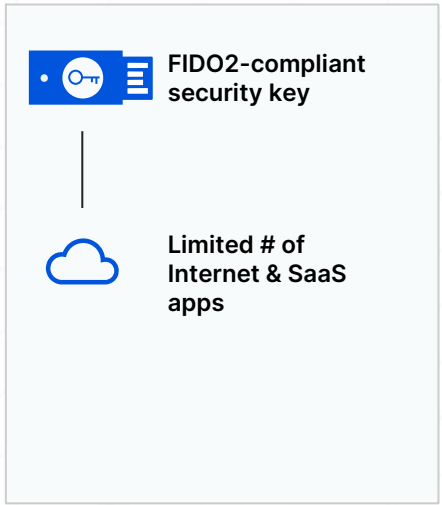
Many IAM solutions don't support selective enforcement



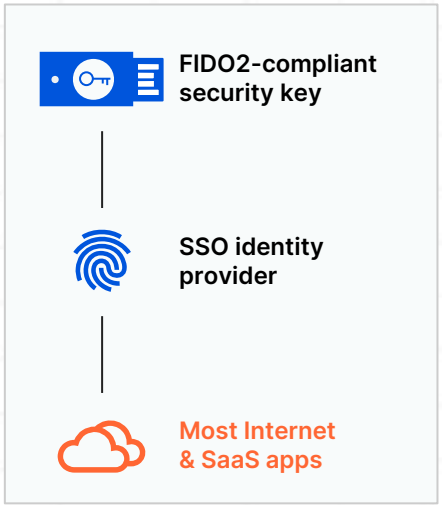
Best practice from Cloudflare IT: ZTNA makes it easy per user, app, geo or group



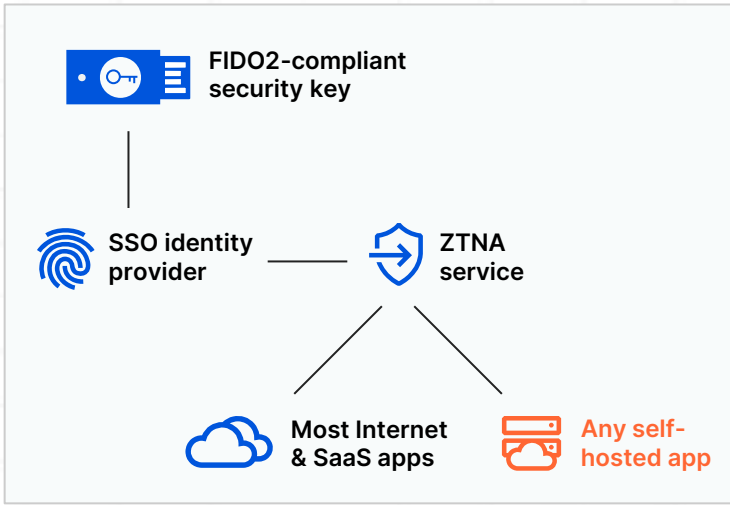
Recommendation 3: Enforce strong auth everywhere
All users and apps; even legacy non-web systems



First best practice from Cloudflare IT:
Centralize your IAM



Second best practice from Cloudflare IT:
Use ZTNA vs. custom development



Recommendation 4: Adopt Zero Trust via one platform

How ZT services can help

Block phishing domain w/SWG

Kill active, compromised sessions w/ZTNA

Search ZTNA/SWG logs for impacted users
see who clicked what to take better action

Run suspicious sites & email links thru RBI
including newly seen or new domains

Block sites before campaigns launch w/CES
scan web for phishing sites

First best practice from Cloudflare IT

- **Enable easier, faster operations** by consolidating ZTNA with SWG into one platform.
- **Prevent further attack spread** and next steps like ransomware.

Second best practice from Cloudflare IT

- **Improve security posture** by expanding platform with RBI, CES, CASB and DLP.

Recommendation 5: Establish paranoid, blame-free culture

Report suspicions early and often

Best practices from Cloudflare IT:

"See something, say something"

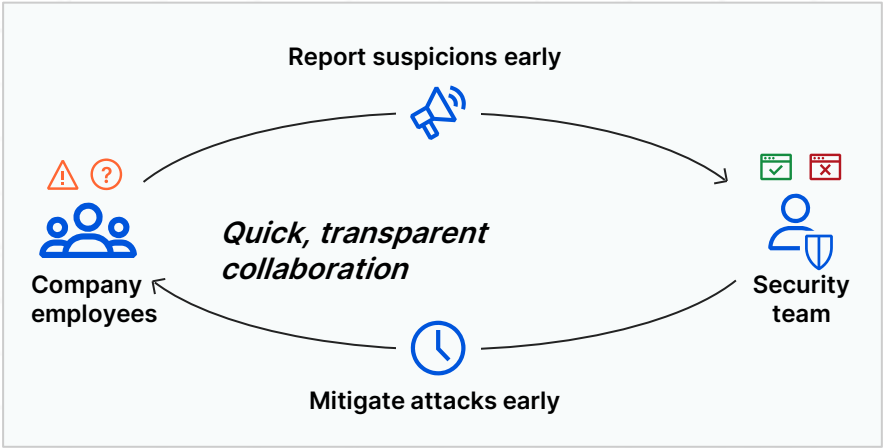
Create comfortable relationship with SIRT to strengthen first line of internal defense

Benign reports are okay

Most reports will be benign; reinforce from leadership this is expected and ideal

Genuine mistakes are okay

Critical during an actual attack to move quickly; accidents will not be reprimanded

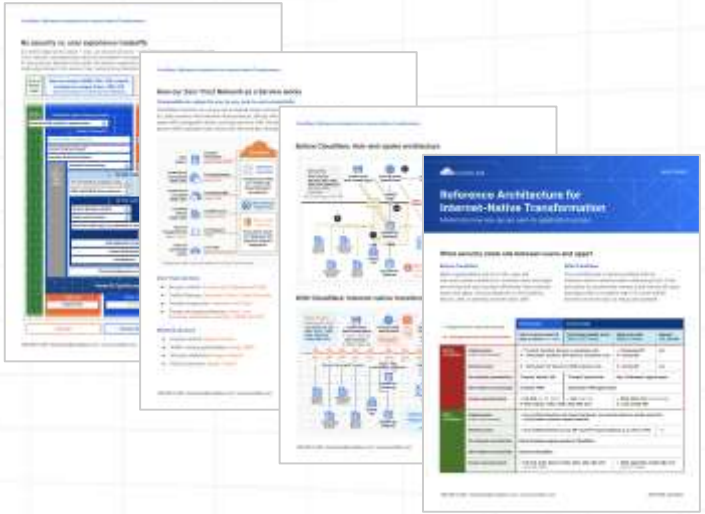


SIRT = Security Incident Response Team

Resources

Further reading: Plan your ZT journey at your own pace
Cloudflare whitepapers to help modernize security

Vendor-agnostic Roadmap:
https://zerotrustroadmap.org/



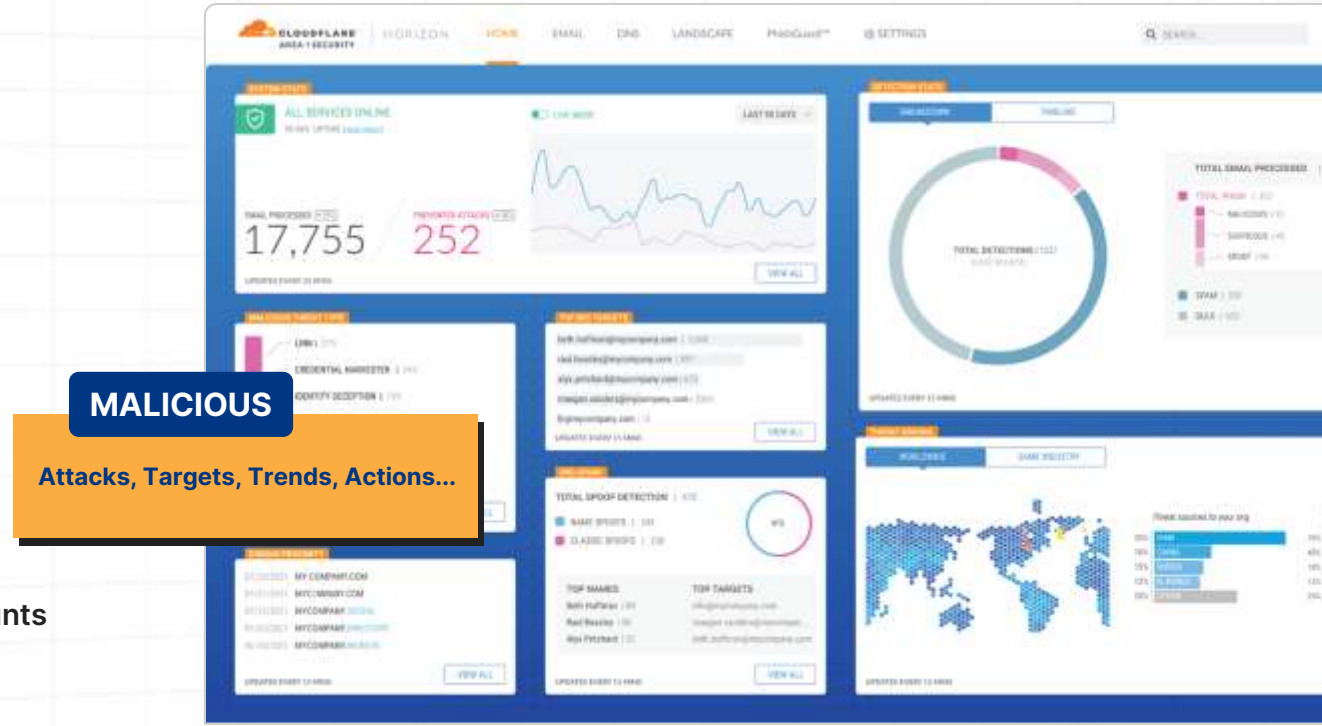
Cloudflare's Reference architecture to Internet-native transformation

Try it out: Phishing risk assessment

See It.
Believe It.

As little as 5 minutes to set up
(Includes 4 mins for Zoom / Webex / Team)

- Missed Attacks
- Targeted Users
- Fraudulent Payouts
- Compromised Vendors & Accounts



CLOUDFLARE

Thank You!