



An toàn thông tin tại Doanh nghiệp SME Thách thức và Giải pháp

Nguyễn Minh Đức – Founder & CEO of CyRadar

2021

1

Khảo sát về vấn đề ATTT đối với SME



Survey

2

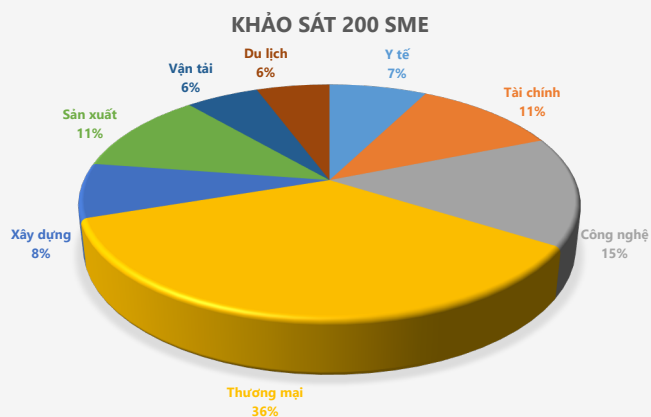
Khảo sát về an toàn thông tin đối với SMB



200 SMEs

45% CEO

55% IT Manager

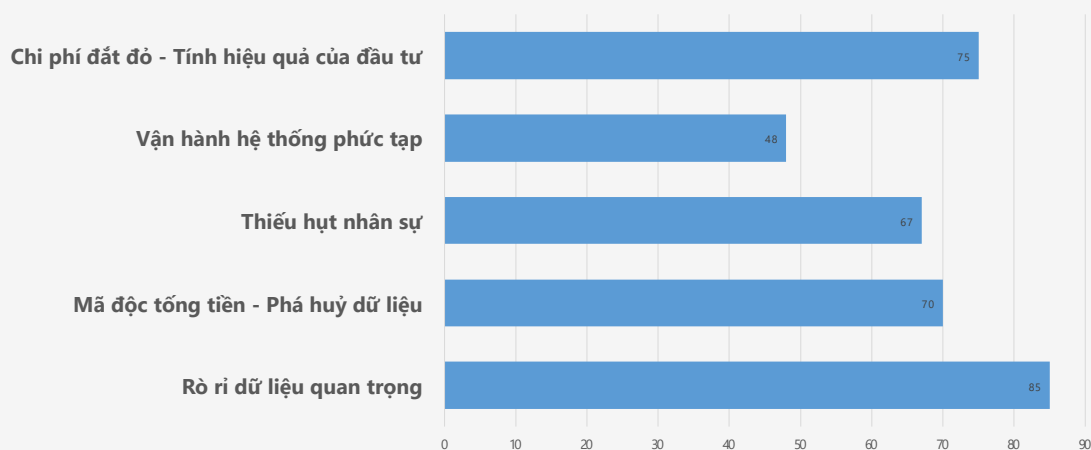


3

Khảo sát về an toàn thông tin đối với SME



Top 5 lo lắng của SME về vấn đề ATTT



4

Khảo sát về an toàn thông tin đối với SME



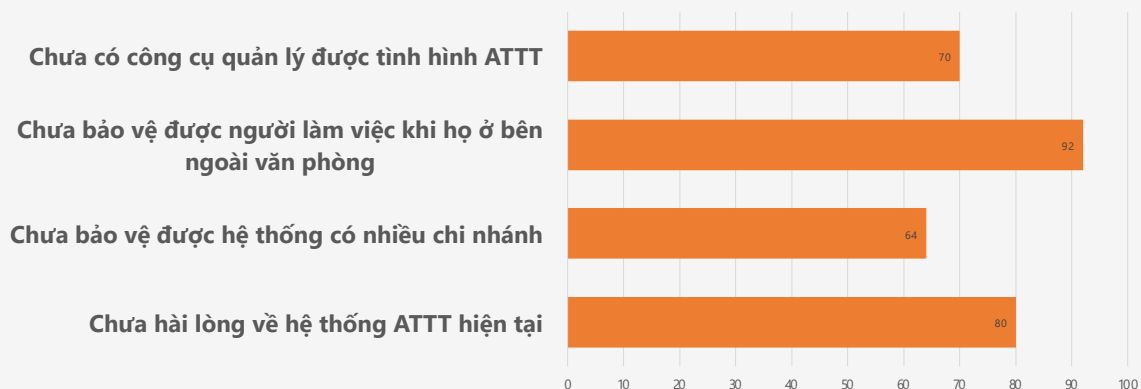
Kỳ vọng khi đầu tư ATTT của SMB

5

Khảo sát về an toàn thông tin đối với SME



Hiện trạng hệ thống ATTT



6

Thách thức



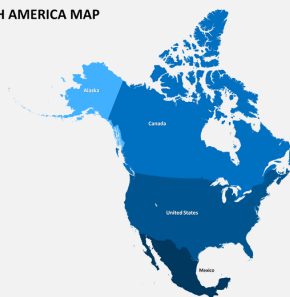
Cyber Security Challenges

7

Damage



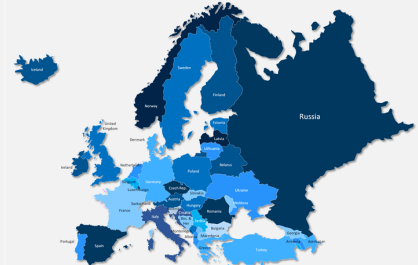
NORTH AMERICA MAP



ASIA MAP



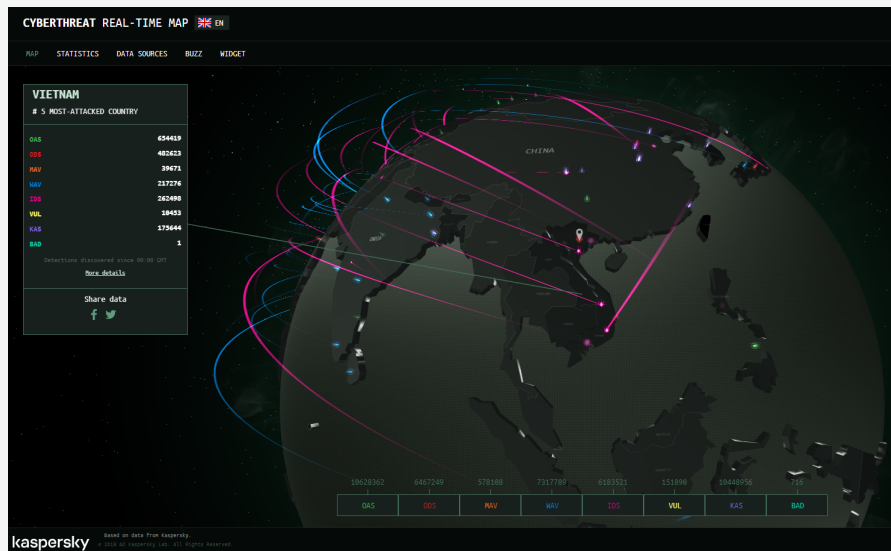
EUROPE MAP



Cybersecurity Ventures Report

8

Challenges



9

Mã hoá tổng tiền



WannaCry

10

CyRadar

Phishing

From: Vietnam People's Public Security <leaminsoo@osolutions.club>
 Subject: **Gửi trong Công an Nhân dân Việt Nam**
 Reply to: Vietnam People's Public Security <majunggil@vpx.com>
 To: [Redacted]



Chào mừng bạn đến với Công an Nhân dân Việt Nam!

Bạn phải báo cáo cho tòa nhà chính của Cảnh sát Việt Nam tại thành phố Hà Nội vào ngày 13 tháng 3, lúc 3:00 chiều. Nếu không chứng minh danh tính của bạn. Đồng thời, tôi thông báo cho bạn rằng để tham gia vào cuộc điều tra, bạn cần bảo vệ hoặc nộp đơn vào trạm cho một luật sư miễn phí. Yêu cầu sự tham gia của luật sư, bạn phải thông báo trước cách khác. Chỉ tiết lộ các chi tiết của chúng tôi, cũng như một ứng dụng mẫu được đính kèm trong thư này.

Số doanh nghiệp của bạn: #5382 17 820
 Đặt ngày xuất hiện tại đơn danh sát: 2019-03-13
 Xin vui lòng đọc họ sơ vụ án một cách cẩn thận! Chúng tôi đính kèm kho lưu trữ với tất cả các tài liệu cần thiết cho bạn.

Địa chỉ: 44 Yết Kí - Hồ? Kiếm - H? N? Website: www.mps.gov.vn hoặc www.bocongan.gov.vn

1 attachment: Documents.rar (40 KB)

GTELNVKX-DECRYPT - Notepad

File Edit Format View Help

*** GANDCRAB V5.0.4 ***

*****UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED*****

*****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .GTELNVKX

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.

The server with your key is in a closed network TOR. You can get there by the following ways:

0. Download Tor browser - <https://www.torproject.org/>

1. Install Tor browser

2. Open Tor Browser

3. Open link in TOR browser: <http://gandcrabfe6mef.onion/90de5b72926546e>

4. Follow the instructions on this page

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES

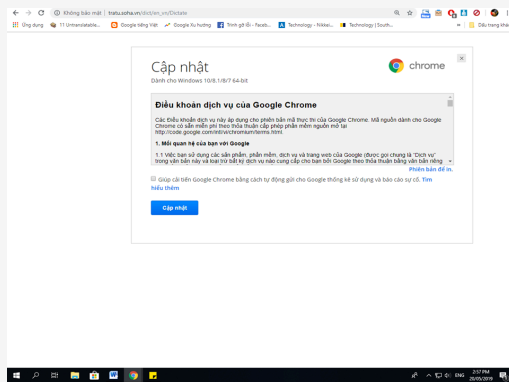
GandCrab

11

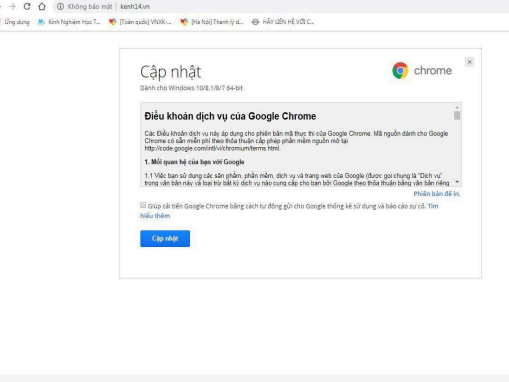
CyRadar

Ăn cắp dữ liệu

Computer 1



Computer 2



12

CyRadar



Cyber Security Problems

13

Problems

CyRadar

SME



Cost

86% SMB pay for security < 10% total cost - EiQ Network survey



Targeted

58% victims are SMB - Ponemon Institute research



Internet

88% malware (ransomware, spyware, ...) spread by email – Symantec report

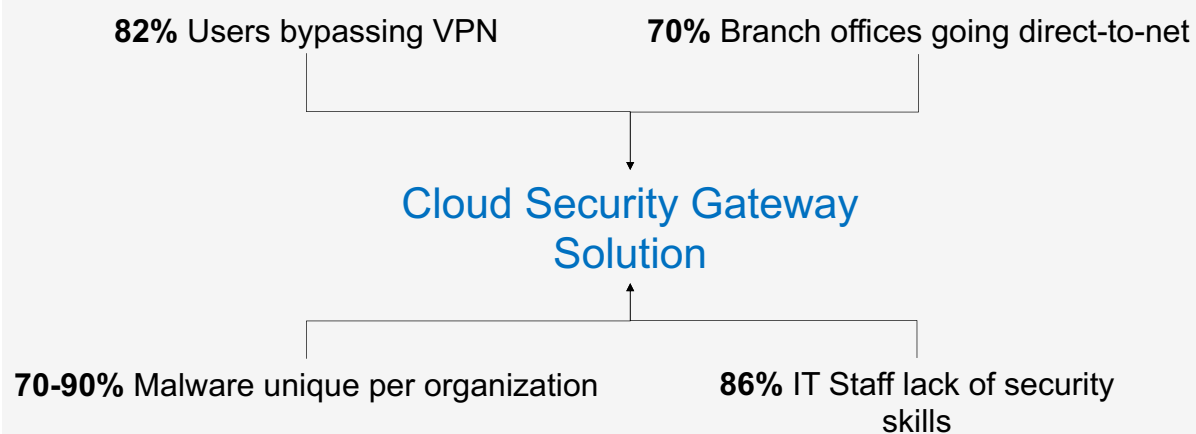


Deployment difficulty

Traditional solution require complicated deployment, expensive operation, ...

14

Xu hướng



Source: Cisco Insights 2017

15

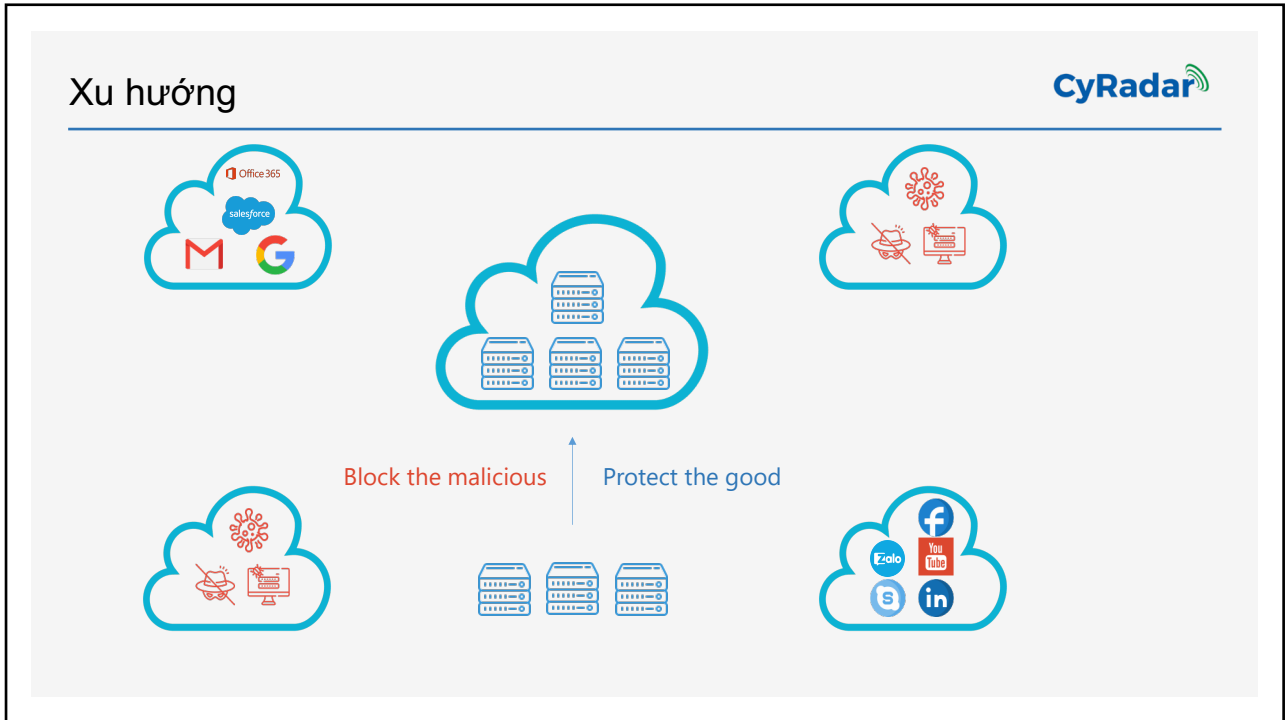
Giải pháp



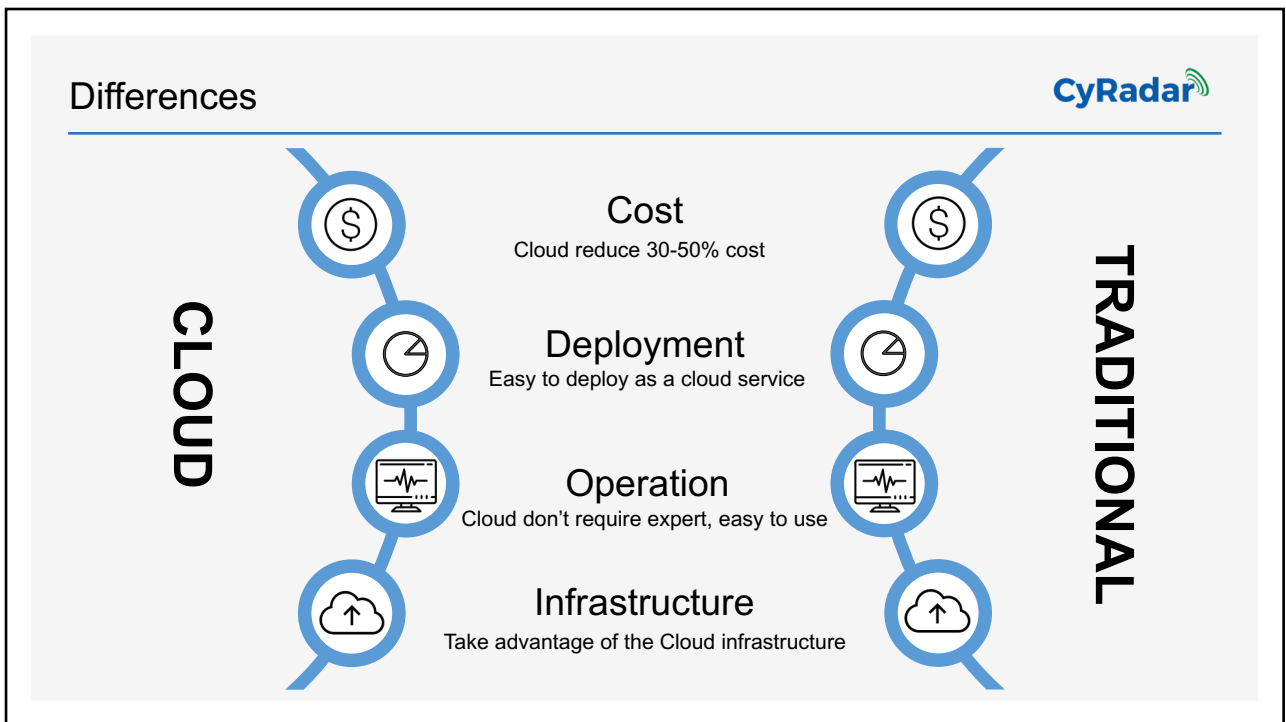
Cloud Secure Gateway

CyRadar Internet Shield Cloud

16



17



18

CyRadar Internet Shield

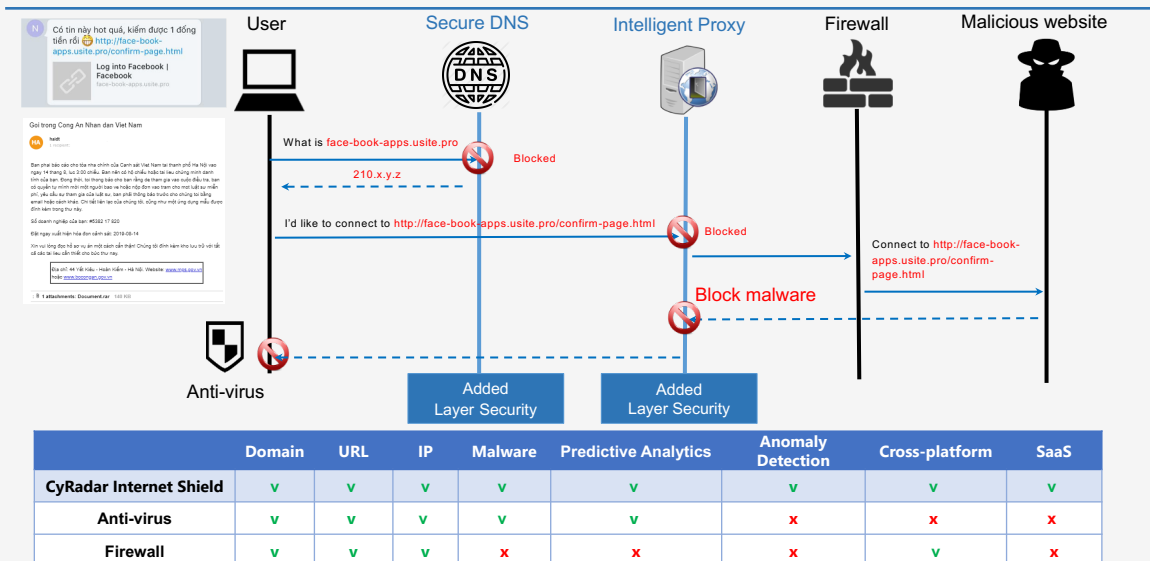


- Sản phẩm xuất sắc năm 2020
- Top 3 sản phẩm xuất sắc nhất Viet Solutions 2020
- Đồng hành cùng SMEdx - Chương trình hỗ trợ DN Vừa và Nhỏ Chuyển đổi số

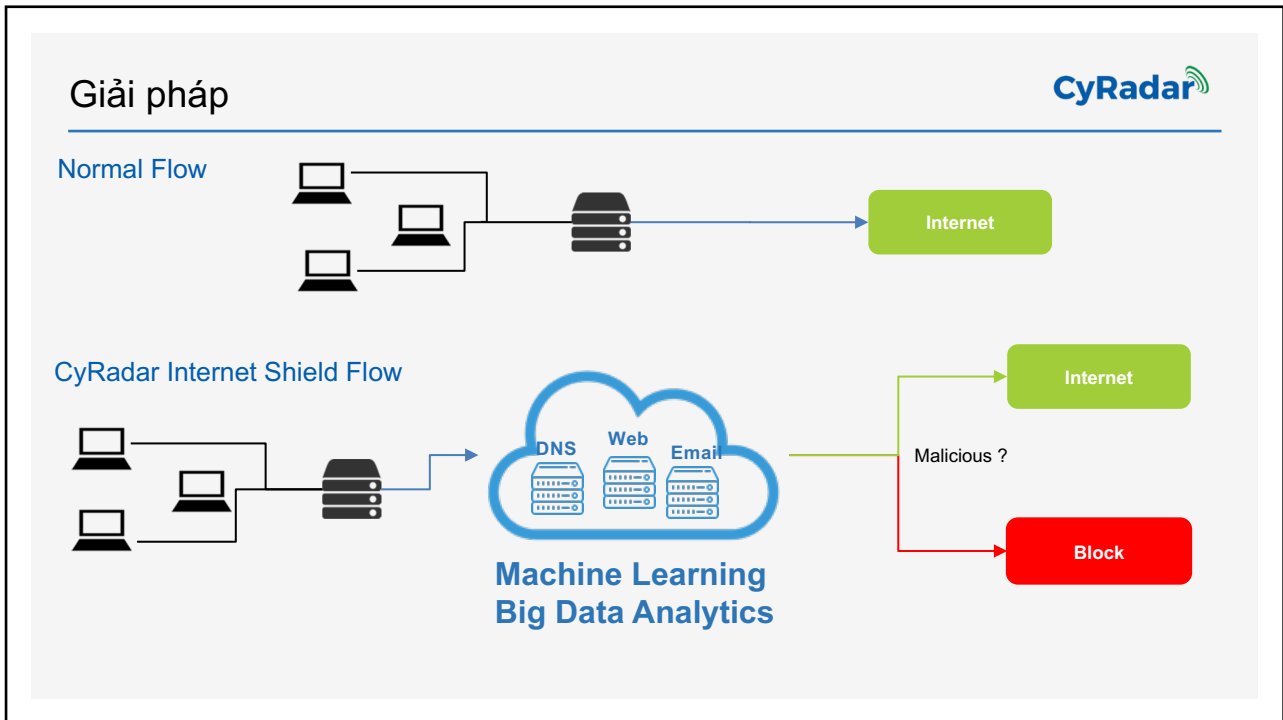


19

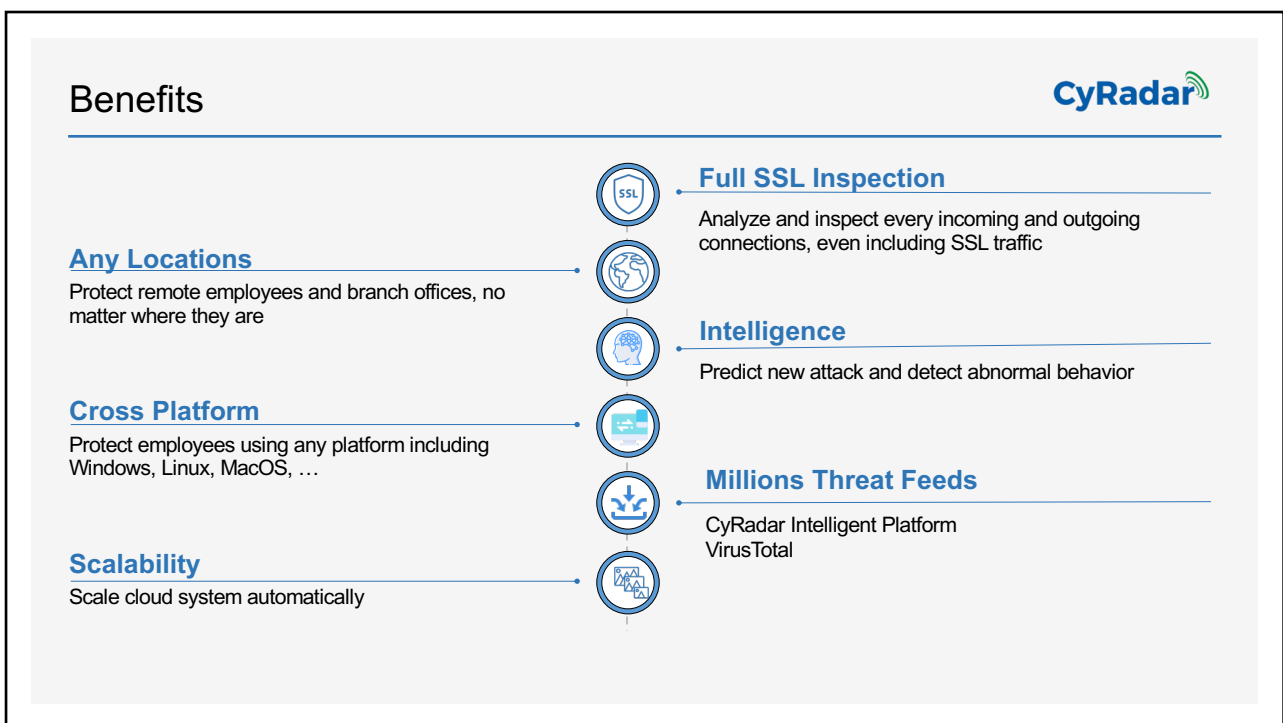
Tại sao lại là CyRadar Internet Shield?



20



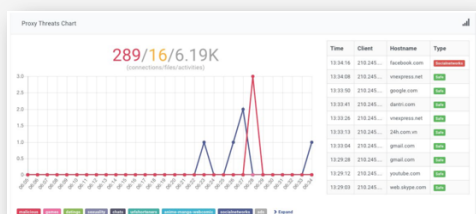
21



22

Tính năng

CyRadar



Anti-Malware

- ☒ Ransomware
- ☒ C&C Server
- ☒ Coin miner

Advanced Threat Prevention

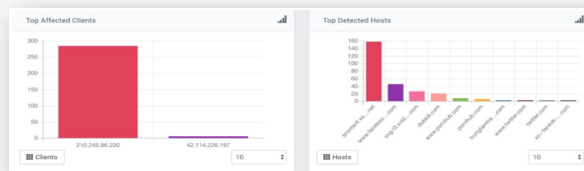
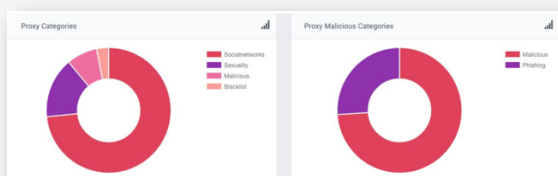
- ☒ Advanced Sandbox
- ☒ Inline Content Inspection
- ☒ Abnormal behavior

Anti-Phishing

- ☒ Stealing Credential Information
- ☒ Stealing Online Payment Information

User control

- ☒ Application Control
- ☒ Internet Access Policy
- ☒ User Behavior Analysis



23

Dễ dàng sử dụng

CyRadar

CyRadar

Chào mừng bạn sử dụng CyRadar Internet Shield

Chào HaiDT,

Tài khoản của bạn đã được đăng ký làm tài khoản sử dụng của dịch vụ CyRadar Internet Shield Cloud.

Tên đăng nhập sử dụng: [@gmail.com](#)

Bạn hãy [thiết lập mật khẩu](#) để truy cập internet.

Tải xuống và kích hoạt phần mềm [CyRadar Internet Shield Agent](#) để thiết lập cấu hình tại máy cá nhân.

Nếu bạn gặp bất kỳ khó khăn nào trong việc sử dụng bản dùng thử của mình, vui lòng liên hệ với contact@cyradar.com của CyRadar.

Cảm ơn,

Công ty Cổ phần An toàn thông tin CyRadar

CyRadar Internet Shield Agent

- 1 Giới Thiệu
- 2 Web Proxy
- 3 Bảo Vệ TLS/SSL
- 4 Kích Hoạt

CyRadar Internet Shield Agent

Cảm ơn bạn đã sử dụng phần mềm CyRadar Internet Shield Agent. Mời bạn bấm vào nút "Kích Hoạt" để bắt đầu quá trình cài đặt.

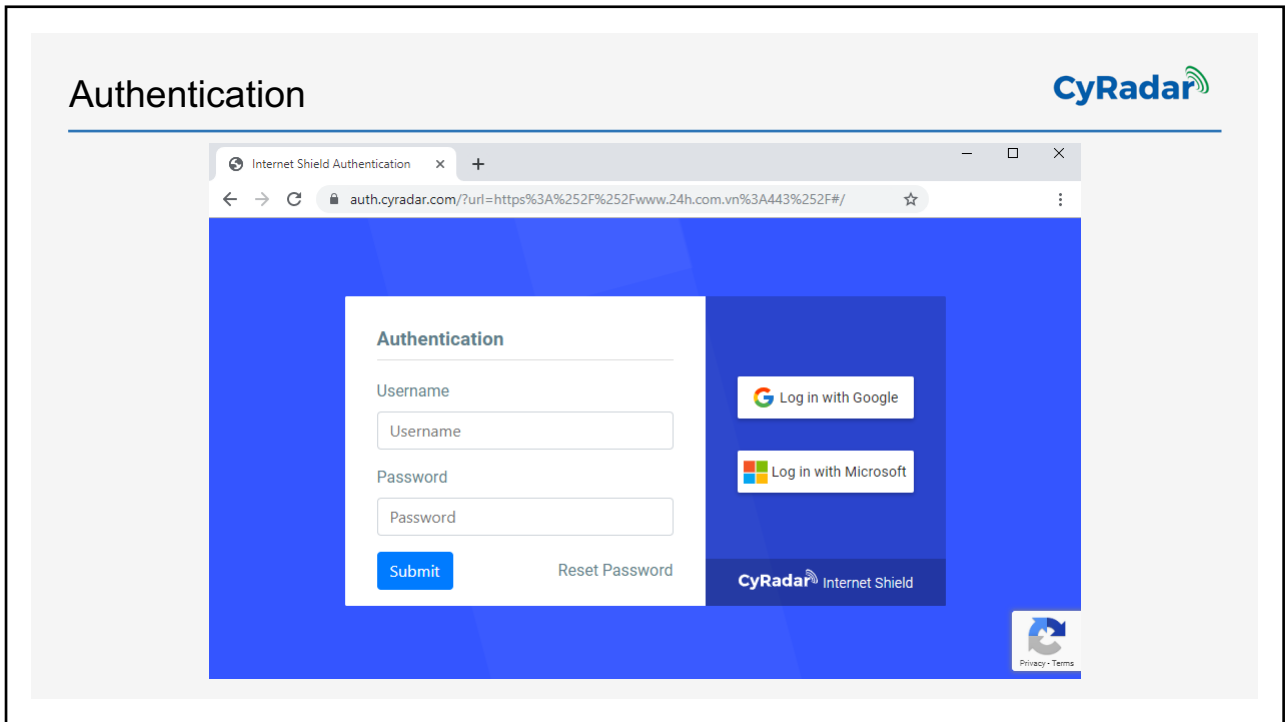


Tiếng Việt

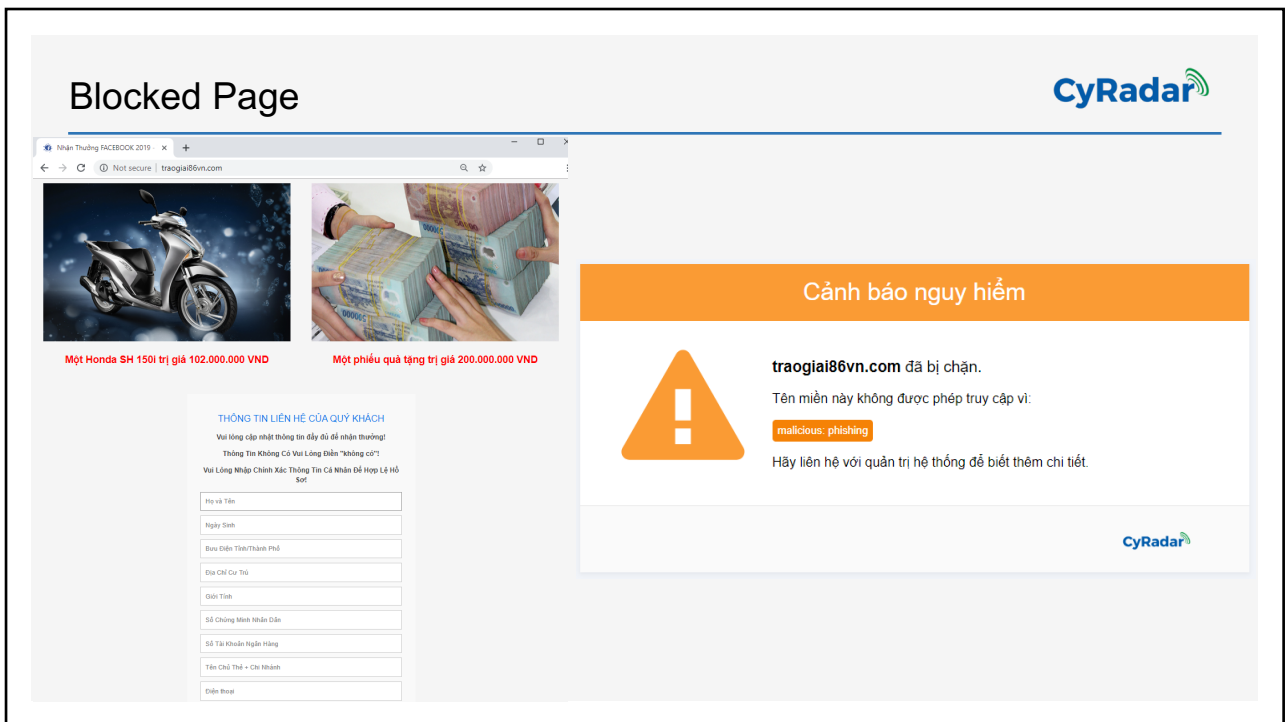
Hủy Kích Hoạt

Kích Hoạt

24



25



26

Blocked Page

CyRadar

Lazada "Payment Advice Issued"

Lazada lazada@anonymousemail.me via orbit.etermailimpact.info to me

Dear Duc,

Your payment advice is issued at the request of our customer.

The advice is for your reference only.

Please download your payment advice [here](#).

Your faithfully,

Lazada Team.

This is an auto-generated email, f

Any replies to this email will be di

Arcabit	Trojan.Generic.D4D2D44	20170530
Avast	Win32:WanaCry-A [Trj]	20170530
AVG	FileCryptor.OYP	20170530
Avira (no cloud)	TR/AD.RansomHeur.aexdn	20170530
AVware	Trojan.Win32.GenericBT	20170530
Baidu	Win32.Trojan.WannaCry.c	20170527
BitDefender	Trojan.GenericKD.5057860	20170530
Bkav	W32.RansomwareTBE.Trojan	20170530
CAT-QuickHeal	Ransom.WannaCrypt.A4	20170530

Powered by
CyRadar

The file is blocked



ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5
babe8e080e41aa is blocked.

The above file is not allowed on this network because of potential security risks.

Please visit [Virus Total](#) for more details.

27

Daily Report

CyRadar

CyRadar

CyRadar	31/07/2019 - 08/08/2019	
Kết nối độc hại	Vi phạm chính sách	Kết nối internet
0	4	3153

Các mối đe dọa

Không có người dùng bị lây nhiễm mã độc

Vi phạm chính sách

Top 10 người dùng vi phạm chính sách		
Người dùng	Số lượng	
hung	2	
123.16	2	

Tình trạng sử dụng internet

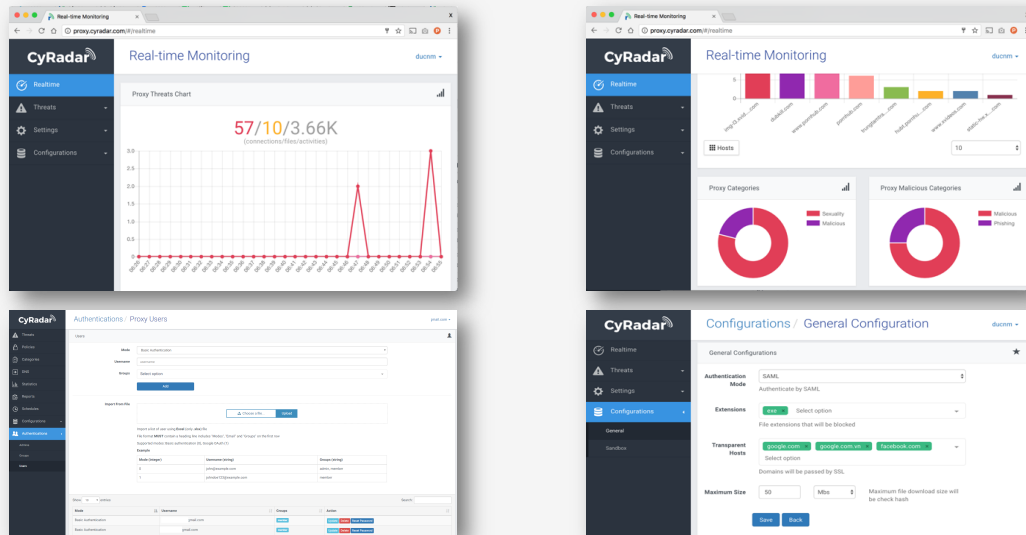
Top 10 tên miền được truy cập		
Tên miền	Số lượng	
ad[.]admicro[.]vn	597	
coccoc[.]com	391	
tratu[.]coviet[.]vn	188	
weworld[.]base[.]vn	161	
www[.]youtube[.]com	105	
vnexpress[.]net	99	
ds[.]polyad[.]net	97	
news[.]zing[.]vn	71	
www[.]phucanh[.]vn	70	
soha[.]vn	69	

Để biết thêm thông tin chi tiết, vui lòng bấm vào đây để chuyển đến trang cuối

Để biết thêm thông tin chi tiết, vui lòng bấm vào đây để chuyển đến trang quản trị.

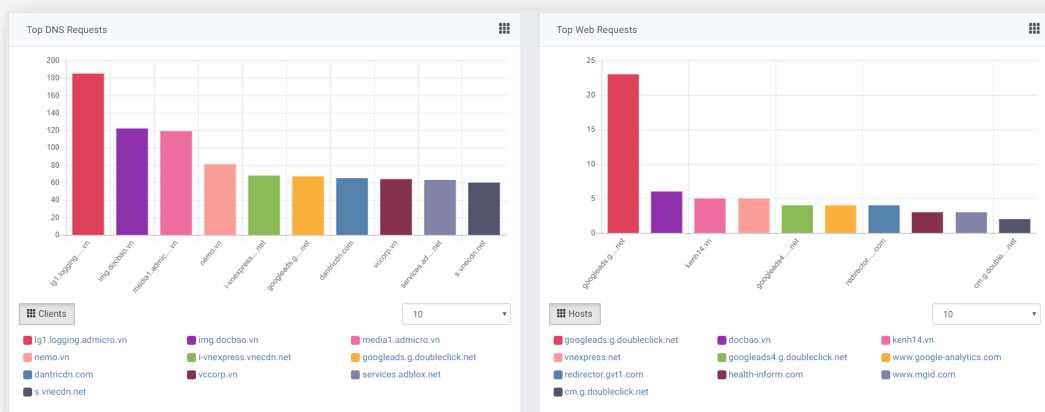
28

Dashboard



29

Internet Usage Insights



30

Miễn phí dùng thử 3 tháng

CyRadar



31

Thank you for your attention!

More questions about CyRadar Internet Shield?

Email: contact@cyradar.com

Web: <https://cyradar.com/products/internet-shield/vi/>

CyRadar

32