

Keysight Solution Introduction

ThreatARMOR

<i>Eric Tsai</i>
<i>Regional Sales Manager / NSS</i>





Introduction

KEYSIGHT TECHNOLOGIES

80+

years of innovation,
measurement
science expertise

1700+

US and foreign
patents issued
or pending

29

of the Top 30 Tech
companies use
Keysight

Market Leader with 80+ Years of Expertise

\$4.3B

in revenue

100+

Countries with
Customers

78

of the Global 100
companies are
Keysight customers

A Recognized Industry Leader



Test & Measurement
Company of the Year



AresONE-400GE
Test System



Gold: New Products
& Services – Nemo
IoT Meter v1



Global Radio Frequency
Test & Measurement
Market Leadership Award



CloudLens –
Product of the
Year



Ixia - Hot Company
Cloud Security &
Leader Enterprise
Security



#21 on the 2018
Forbes JUST
100 Companies



Cyber Security Vendor
Achievement of the
Year



Best Security
Hardware Product -
Vision ONE with
Active SSL



Global Technology
Innovation Award
NB-IoT Massive UE
Emulation Test
System

Around the World We're Ready to Help You Change It

150 locations

Conducting business in
more than 100 countries

13,000+ employees

ASIC design center and
proprietary fabrication facility

Technology centers for MMICs,
optical components and
microelectronic packaging

Over 1,700
patents

>4,000 products

R&D centers
in 15 countries
around the world

40 service hubs



Network, Applications and Security

KEYSIGHT TECHNOLOGIES

Network Applications and Security

We challenge the infrastructure, harden security
and visualize the applications



TEST

Harden infrastructure
Validate app performance
Verify provisioning



SECURITY

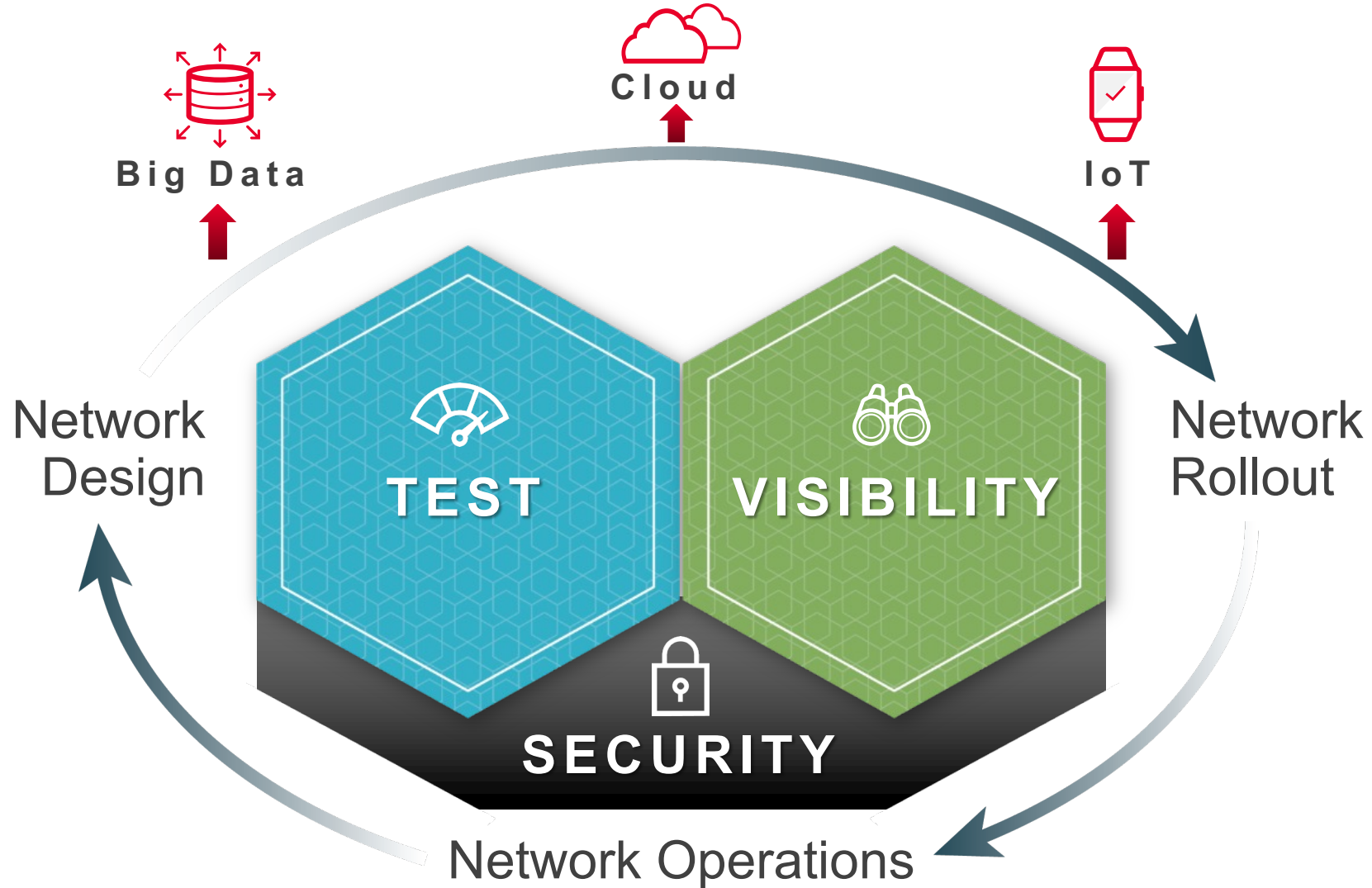
Surface vulnerabilities
Provide resilient security
Reduce attack surface



VISIBILITY

Provide 100% visibility
Deliver real-time intelligence
Eliminate blind spots

Delivering value across network lifecycle



Market Trends + Customer Challenges



Application Traffic Growth

- Keeping pace with ever changing application landscape
- User experience of real-time, business critical applications
- Realistic representation of your network
- Roll-out of 40G, 25G and 100G upgrades



Encrypted Traffic

- Encryption the default approach to securing Internet interactions
- Emergence of LS1.3
- New encryption standards -2/4K keys, ECC ciphers
- SSL/IPsec inspection is becoming main stream



Virtualization & Cloud

- Acceleration of NFV/SDV adoption
- Live-network testing
- Quality of Service provisioning
- Deployment and automation in various private and public cloud



Network Security

- Increasing threat landscape
- Data leakage and theft
- Cyber Security Training & Process
- User & Device based policing to over come BYOD and IoT



Industrial Control Systems & IoT

- ICS moving to Ethernet/IP increases threat exposure
- Security & performance of the distributed IoT delivery infrastructure



Security

NETWORK, APPLICATIONS AND SECURITY

Security Breaches Cost more than \$\$\$

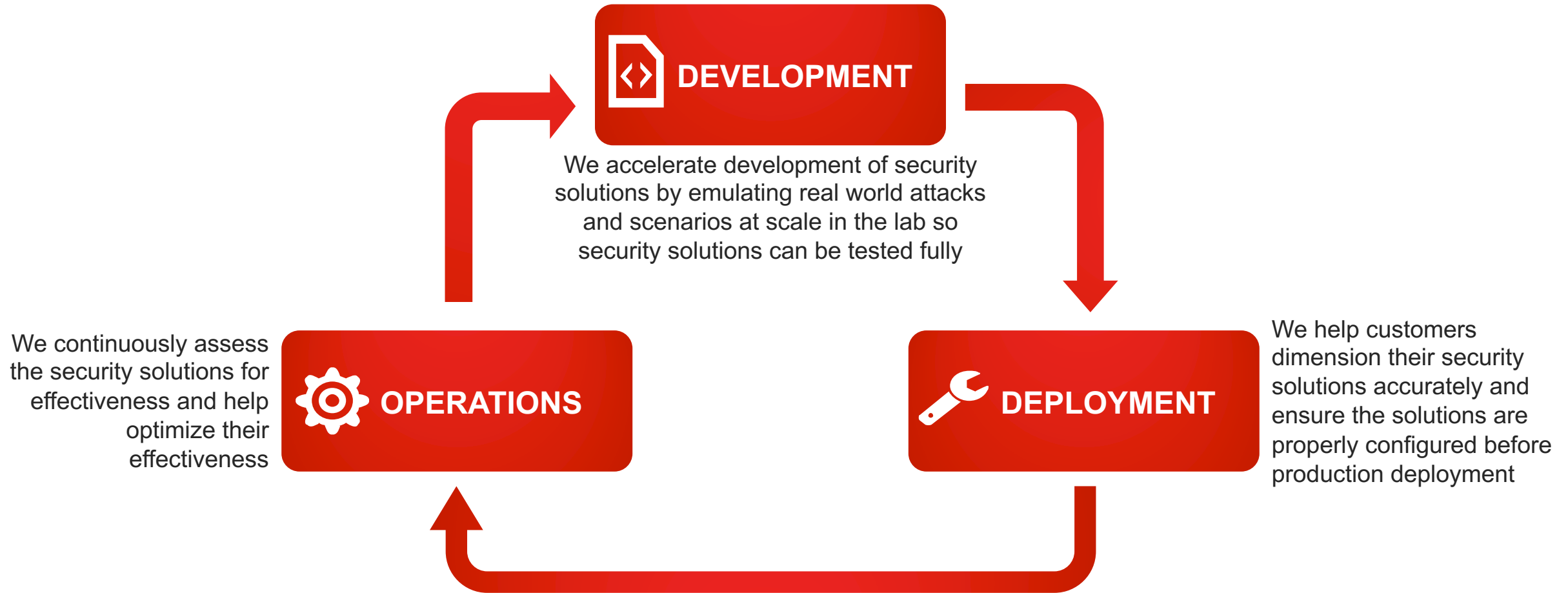
Miss a Threat, Make a Headline

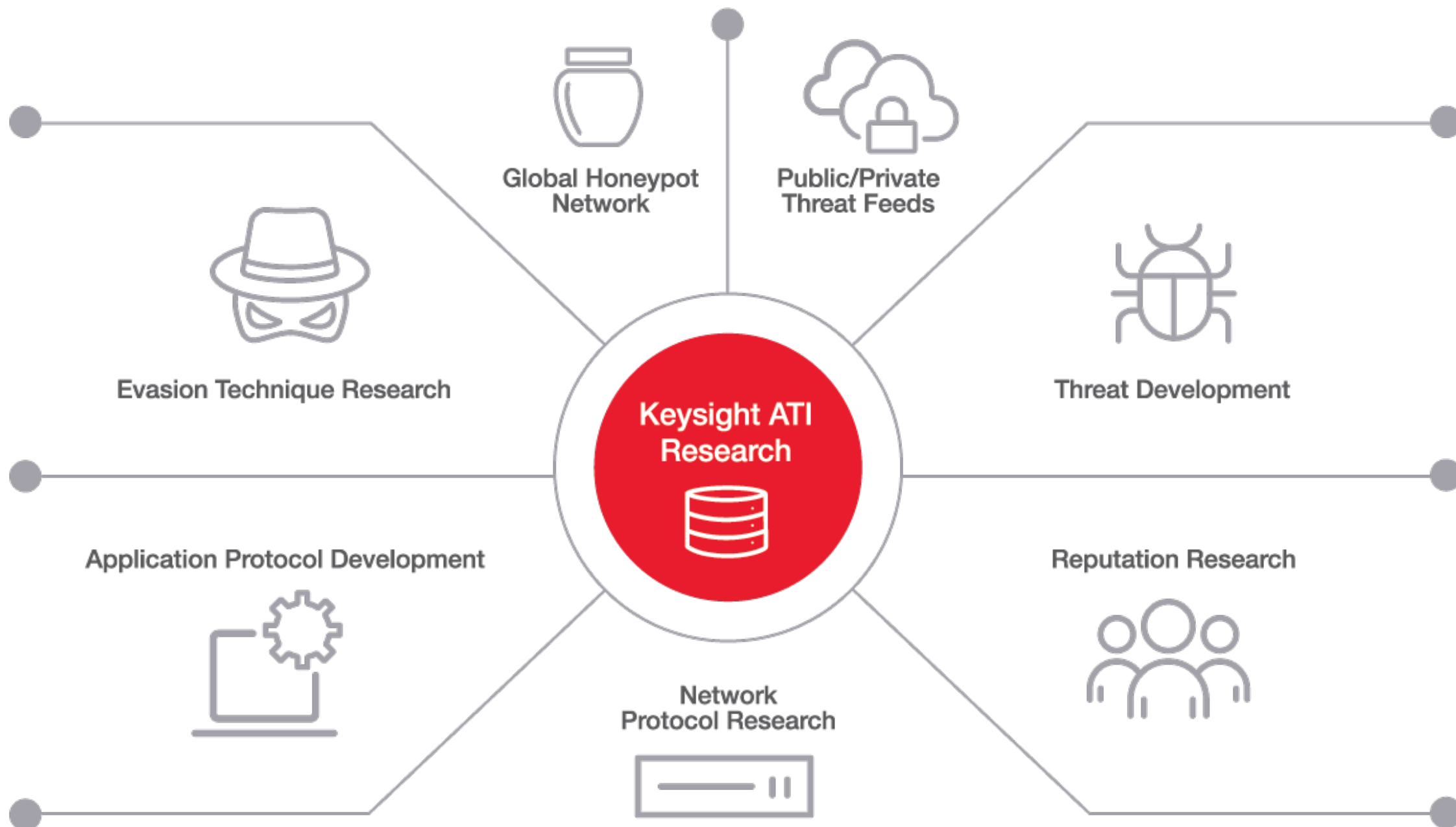


4.1B Data records breached in the first half of 2019¹.

Industry experts but the impact of each data record stolen at \$150.

Security Lifecycle





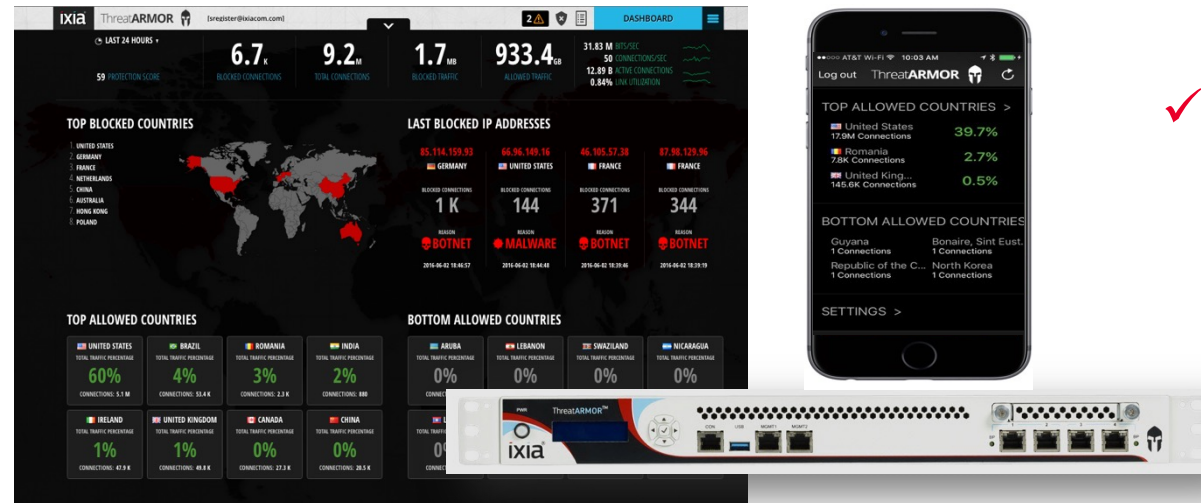
SecOps Efficiency

CHALLENGES

- Constant barrage of threats yields alert fatigue
- Important attacks get lost in the noise
- Attack surface is difficult to contain

KEYSIGHT SOLUTIONS

Line-rate blocking of known-bad sites and untrusted countries reduces alert fatigue



ThreatARMOR

VALUE

- ✓ 30-minute setup, no complex policies
- ✓ 100% proof for all blocked sites
- ✓ Blocks up to 80% of alert-generating traffic



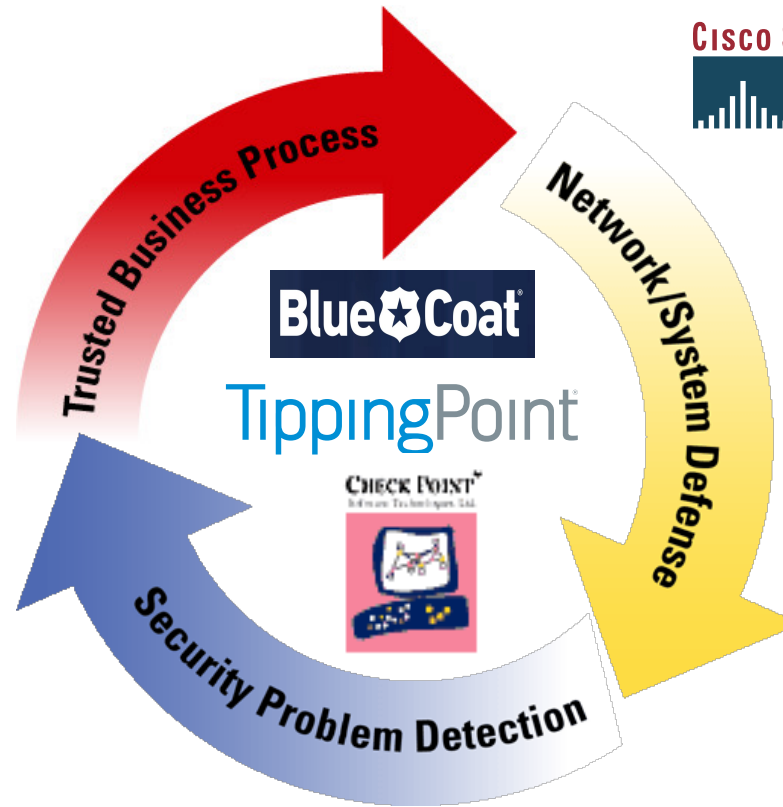
ThreatARMOR

PRODUCT INFORMATION

What are our Security Deployment?

"IT'S WHAT WE DO"

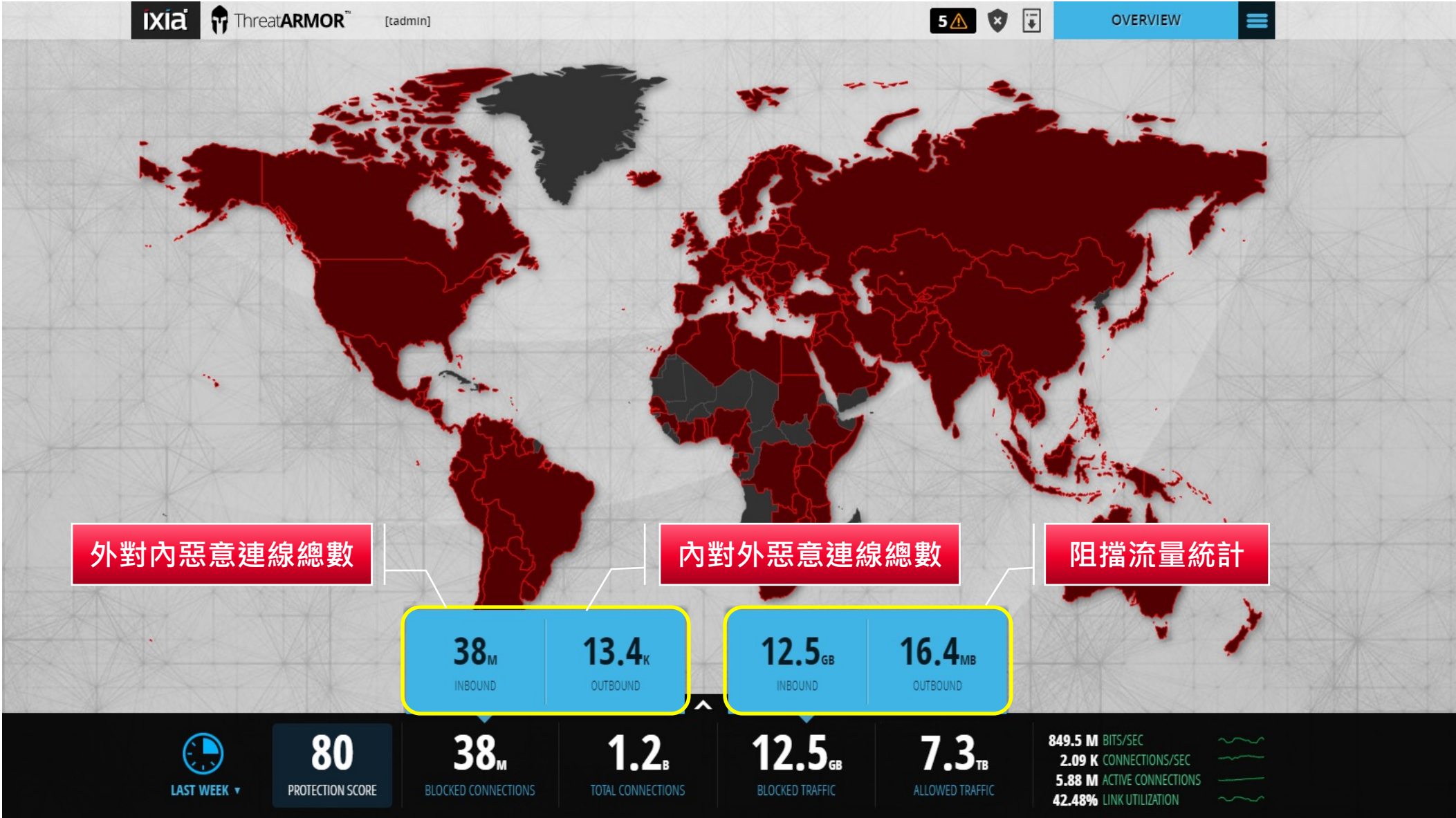
- Authentication
- Access Management
- Data Privacy & Integrity
- Transaction Integrity
- Data Loss Prevention



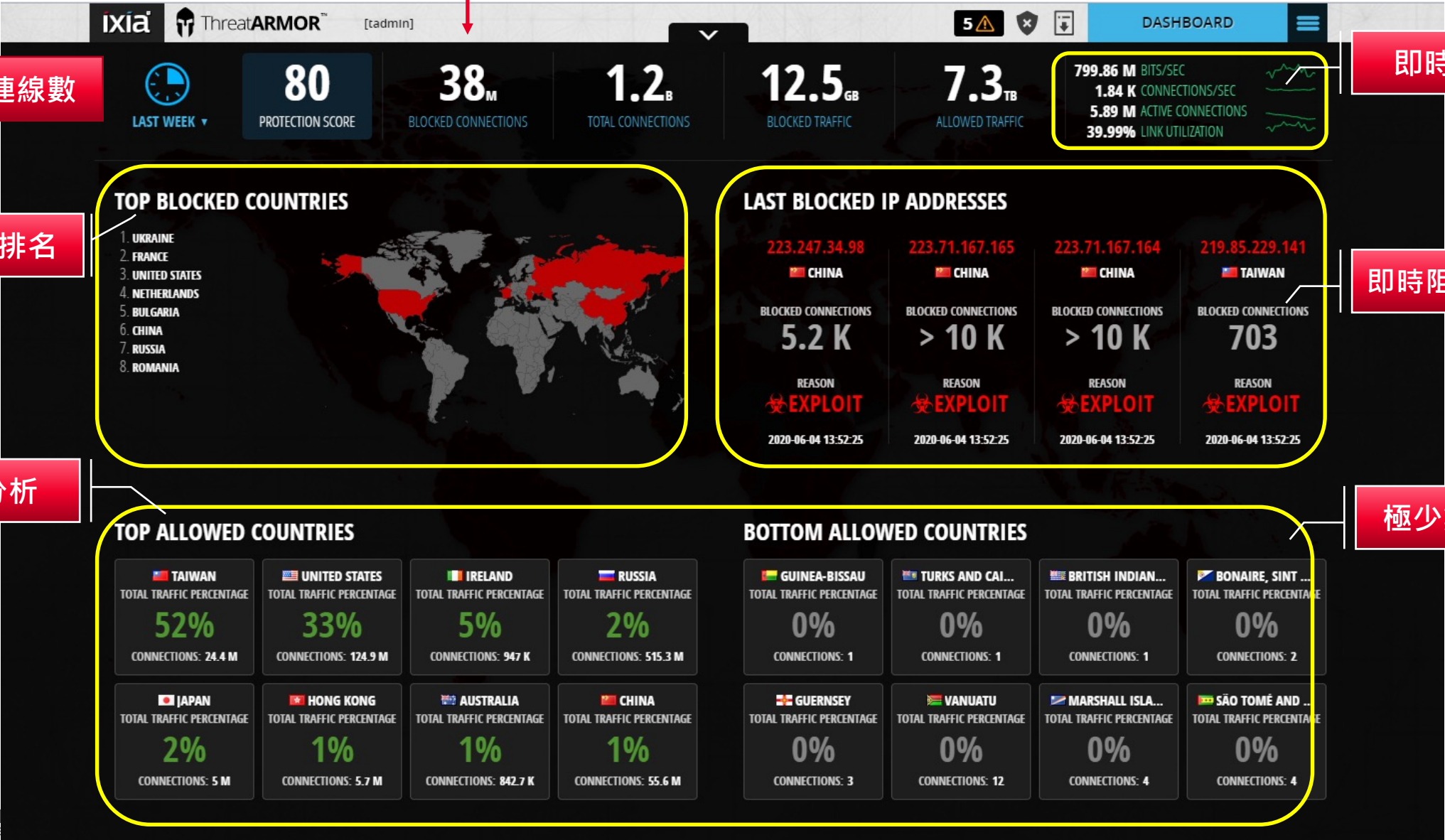
- Firewall / IPS / WAF
- Anti-Virus/Anti-Spam
- DDOS
- APT & EDR
- Encryption(VPN)

- Threat Intelligence and Analysis
- Vulnerability Assessment
- Penetration Test · PT
- Forensics
- SIEM (Security Information and Event Management)

全球資安情資分析防禦系統- Dashboard



全球資安情資分析防禦系統- Dashboard



累計阻擋連線數

即時狀態資訊

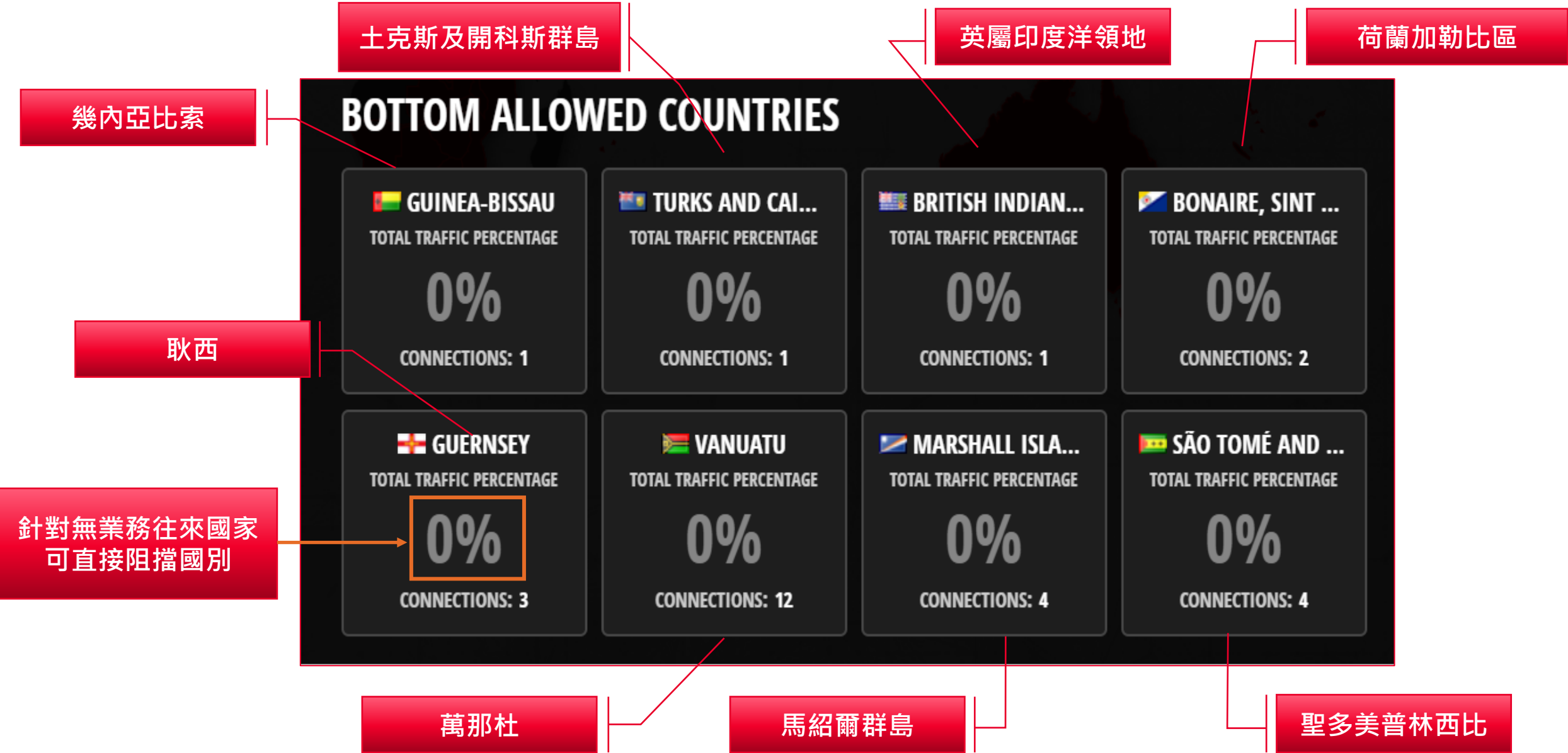
依國家地理排名

即時阻擋攻擊顯示

威脅潛勢分析

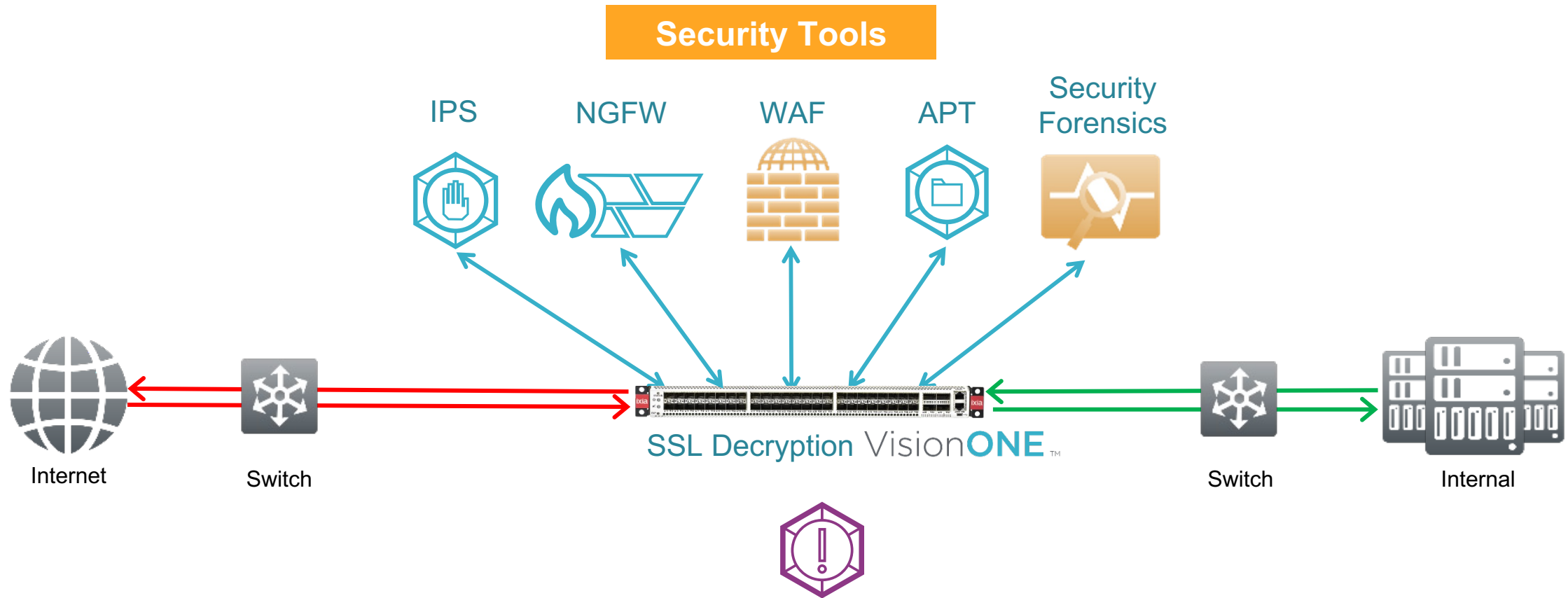
極少數連線統計

全球資安情資分析防禦系統- Dashboard



SSL inspection see all Traffic?

MANY APPLICATIONS CAN'T BE DECRYPTED

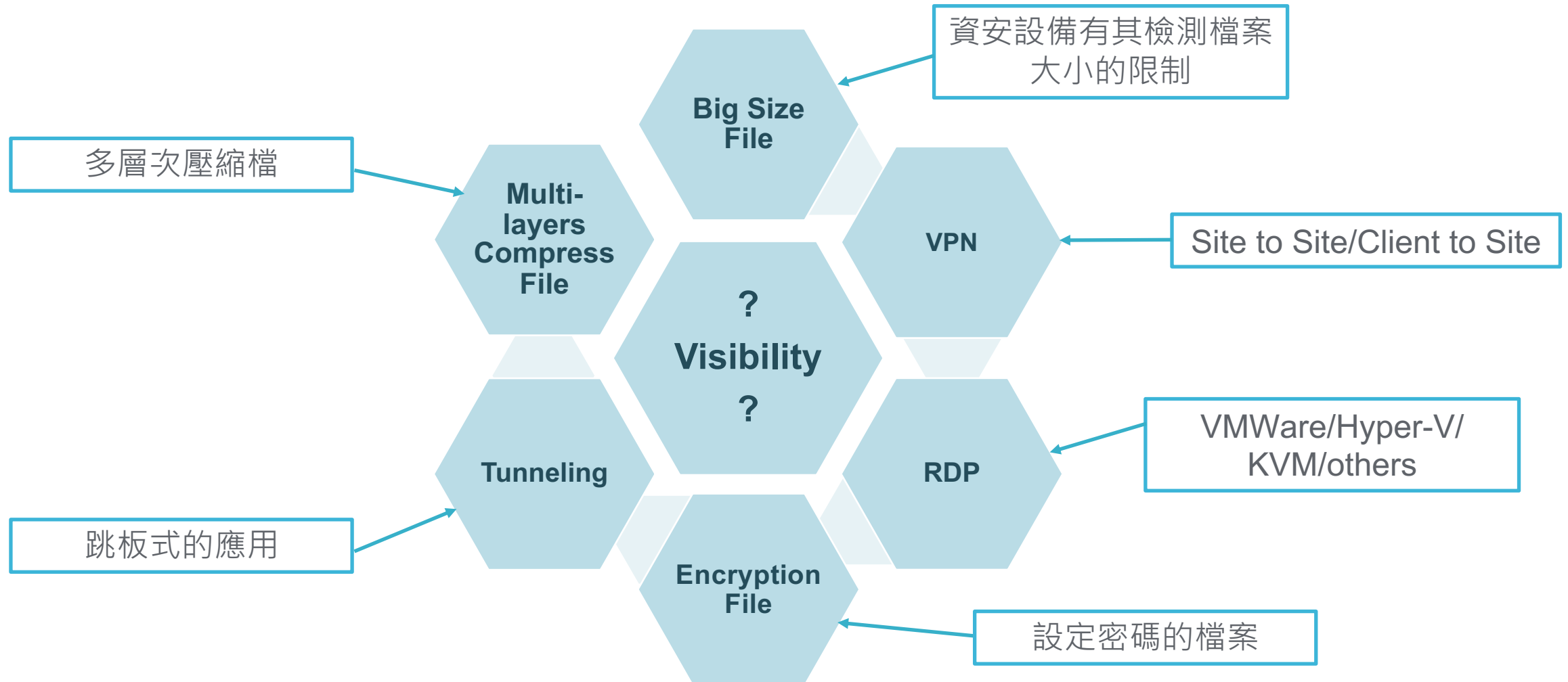


Line 、 Skype 、 Facebook messenger 、 Whatsapp 、 Dropbox...etc

Can't not be decrypted

No solutions for those conditions

GATEWAY SECURITY SOLUTIONS CAN'T OFFER THE SOLUTIONS



全球資安情資分析防禦系統 – File Risk - Malware

DASHBOARD \ BLOCKED IP ADDRESSES

taiwan

LAST WEEK

IP Address	Country	Reason	Last Blocked On	Last Direction
36.231.22.63	Taiwan	變	2019-03-24 21:25:44	Inbound
202.39.65.221	Taiwan	變	2019-03-24 21:25:32	Inbound
112.105.7.78	Taiwan	變	2019-03-24 21:25:06	Inbound
150.117.232.80	Taiwan	變	2019-03-24 21:24:54	Inbound
61.56.213.97	Taiwan	變	2019-03-24 21:24:54	Outbound
114.33.168.226	Taiwan	變	2019-03-24 21:24:51	Inbound
122.121.128.33	Taiwan	變	2019-03-24 21:23:41	Inbound
118.233.224.13	Taiwan	變	2019-03-24 21:23:21	Inbound
218.35.40.76	Taiwan	變	2019-03-24 21:23:15	Inbound
1.34.26.79	Taiwan	變	2019-03-24 21:22:53	Inbound
59.126.219.219	Taiwan	變	2019-03-24 21:22:51	Inbound
220.134.105.171	Taiwan	變	2019-03-24 21:21:50	Inbound
118.232.221.21	Taiwan	變	2019-03-24 21:21:41	Inbound
123.195.224.218	Taiwan	變	2019-03-24 21:21:22	Inbound
218.161.105.151	Taiwan	變	2019-03-24 21:20:46	Inbound
1.165.31.122	Taiwan	變	2019-03-24 21:19:53	Outbound
114.32.20.226	Taiwan	變	2019-03-24 21:18:59	Inbound
1.173.32.88	Taiwan	變	2019-03-24 21:18:50	Inbound
140. .144.169	Taiwan	變	2019-03-24 21:18:48	Outbound
123.241.1.43	Taiwan	變	2019-03-24 21:18:35	Inbound
118.232.155.172	Taiwan	變	2019-03-24 21:18:19	Inbound
210.209.138.142	Taiwan	變	2019-03-24 21:17:31	Inbound
218.173.131.20	Taiwan	變	2019-03-24 21:17:19	Inbound

Showing last 10000 blocked IP addresses for TAIWAN

LOAD MORE RESULTS

EXPORT TO CSV

IP:140. .144.169

MALWARE

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION STATS | IP INFORMATION

THREATS DETECTED: 1 MALWARE

IDENTIFIED PHP/ZONIE.A

THREAT URL

LAST SCAN DATE

FILE CHECKSUM

Reverse DNS: FTPYZU.EDU.TW

Last Blocked On: 2019-03-24 21:18:48

30.3 KB

391

109

19.7 MB

BLOCKED TRAFFIC

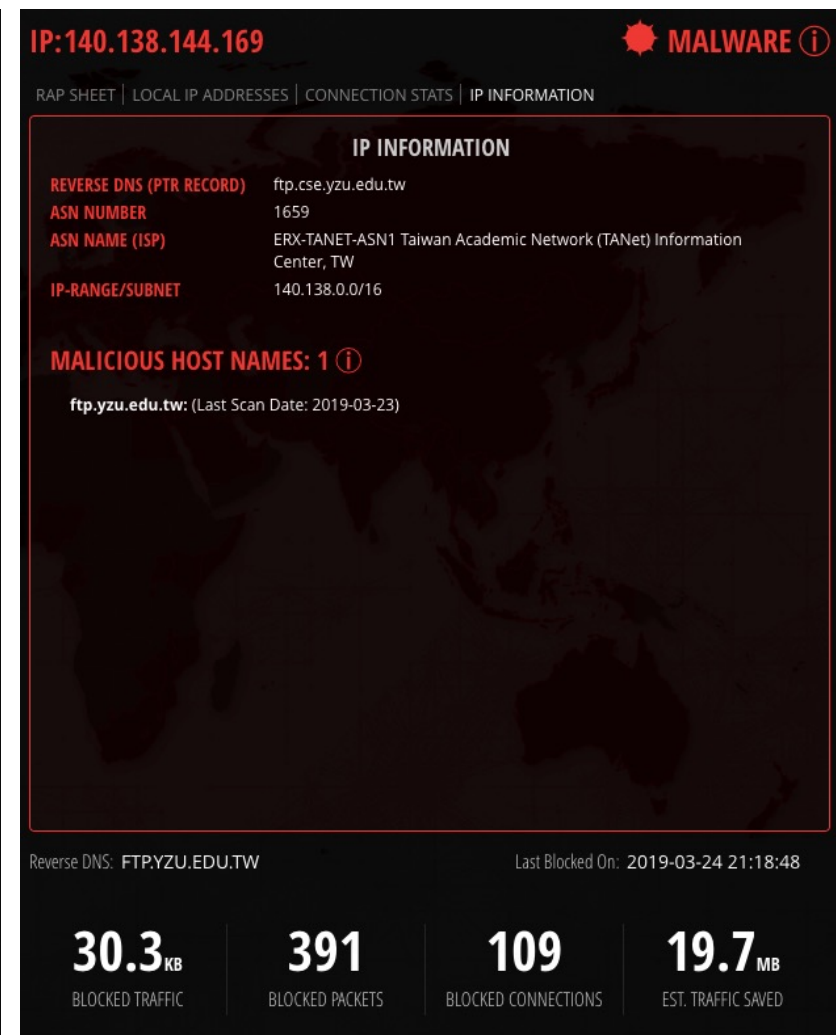
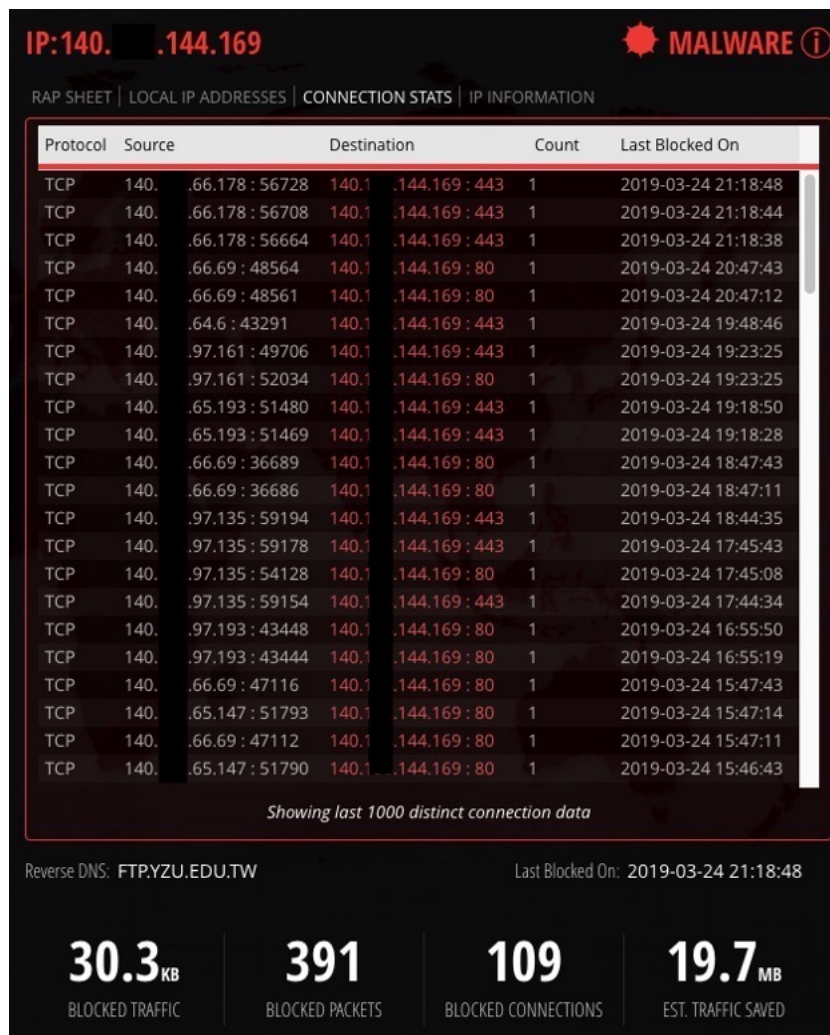
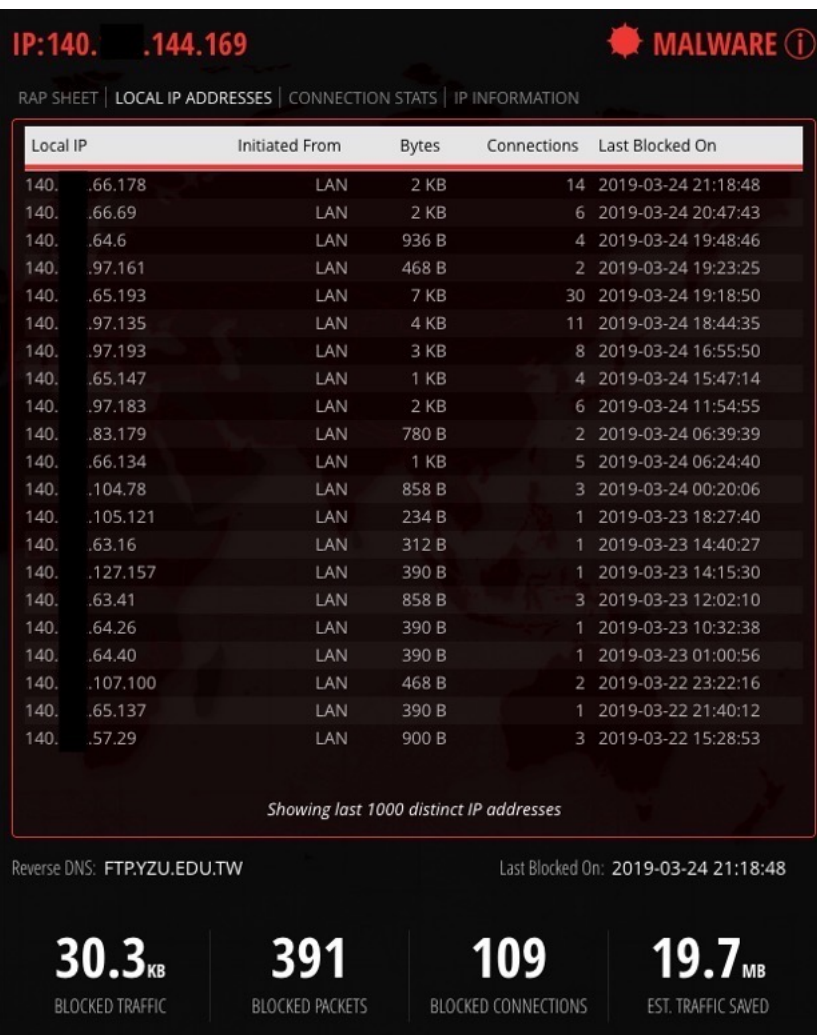
BLOCKED PACKETS

BLOCKED CONNECTIONS

EST. TRAFFIC SAVED

情資分析指出此Malware潛藏在此檔案

全球資安情資分析防禦系統 – File Risk - Malware



內部多個IP皆是連線至此具有malware的檔案
且連線除了藉由80 Port, 還有443的加密連線

全球資安情資分析防禦系統- Malware

DASHBOARD \ BLOCKED IP ADDRESSES

taiwan

×

LAST WEEK

IP Address	Country	Reason	Last Blocked On	Last Direction
123.241.1.43	Taiwan	受	2019-03-24 21:18:35	Inbound
118.232.155.172	Taiwan	受	2019-03-24 21:18:19	Inbound
210.209.138.142	Taiwan	受	2019-03-24 21:17:31	Inbound
218.173.131.20	Taiwan	受	2019-03-24 21:17:19	Inbound
114.33.56.108	Taiwan	受	2019-03-24 21:15:14	Inbound
114.34.25.245	Taiwan	受	2019-03-24 21:14:36	Inbound
203.222.0.125	Taiwan	受	2019-03-24 21:14:21	Inbound
182.235.60.137	Taiwan	受	2019-03-24 21:14:15	Inbound
114.29.242.3	Taiwan	受	2019-03-24 21:14:09	Inbound
36.235.136.165	Taiwan	受	2019-03-24 21:13:31	Outbound
218.32.96.210	Taiwan	受	2019-03-24 21:12:00	Inbound
59.126.194.167	Taiwan	受	2019-03-24 21:11:01	Inbound
60.251.67.124	Taiwan	受	2019-03-24 21:09:14	Inbound
211.72.206.50	Taiwan	●	2019-03-24 21:09:03	Outbound
103.118.24.39	Taiwan	●	2019-03-24 21:08:32	Outbound
210.60.77.8	Taiwan	●	2019-03-24 21:07:10	Outbound
59.127.215.220	Taiwan	受	2019-03-24 20:57:53	Inbound
210.242.73.220	Taiwan	●	2019-03-24 20:56:43	Outbound
114.33.212.57	Taiwan	受	2019-03-24 20:55:02	Inbound
60.248.176.111	Taiwan	受	2019-03-24 20:54:15	Inbound
60.250.203.27	Taiwan	受	2019-03-24 20:53:59	Inbound
203.77.80.159	Taiwan	●	2019-03-24 20:53:52	Inbound
220.134.139.98	Taiwan	受	2019-03-24 20:53:01	Inbound

Showing last 10000 blocked IP addresses for TAIWAN

REFRESH

LOAD MORE RESULTS

EXPORT TO CSV

IP:211.72.206.50

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION S

THREATS DETE

FOUND JS/REDIR

THREAT URLhttp://www.ict.com.tw/DSP/Dres

LAST SCAN DATE2019-03-23 20:19:59

FILE CHECKSUMSHA256 - 65595765b5f46379fc3a6f43af89

TROJ/RANSOM-DAF

THREAT URLhttp://www.mari.com.tw/y78fj34

LAST SCAN DATE2019-03-17 08:20:25

FILE CHECKSUMSHA256 - 06e665583f54e8824f6ddb4a809

Reverse DNS: VWEB9.URL.COM.TW

1.4MB

19.1K

BLOCKED TRAFFIC

BLOCKED PACKETS

DRESEARCH

Homepage

News

Products

Systems

TeleObserver

VIDIA

RemoteRec

Hardware

Software

TriMedia

MDS

Consulting

Download

TeleObserver®

The TeleObserver line consists of a series of compact devices for the transmission of video images. The videos can be transmitted by mobile phone (GSM), telephone lines or ISDN. TeleObserver is available for mobile as well as stationary operation. Simple operating software in your receiver PC allows all compatible devices to work comfortably together.

Camera 2

Camera 3

Camera 4

Port 1

Port 2

Port 3

Port 4

Port 5

Port 6

Port 7

Port 8

Port 9

Port 10

Port 11

Port 12

Port 13

Port 14

Port 15

Port 16

Port 17

Port 18

Port 19

Port 20

Port 21

Port 22

Port 23

Port 24

Port 25

Port 26

Port 27

Port 28

Port 29

Port 30

Port 31

Port 32

Port 33

Port 34

Port 35

Port 36

Port 37

Port 38

Port 39

Port 40

Port 41

Port 42

Port 43

Port 44

Port 45

Port 46

Port 47

Port 48

Port 49

Port 50

Port 51

Port 52

Port 53

Port 54

Port 55

Port 56

Port 57

Port 58

Port 59

Port 60

Port 61

Port 62

Port 63

Port 64

Port 65

Port 66

Port 67

Port 68

Port 69

Port 70

Port 71

Port 72

Port 73

Port 74

Port 75

Port 76

Port 77

Port 78

Port 79

Port 80

Port 81

Port 82

Port 83

Port 84

Port 85

Port 86

Port 87

Port 88

Port 89

Port 90

Port 91

Port 92

Port 93

Port 94

Port 95

Port 96

Port 97

Port 98

Port 99

Port 100

Port 101

Port 102

Port 103

Port 104

Port 105

Port 106

Port 107

Port 108

Port 109

Port 110

Port 111

Port 112

Port 113

Port 114

Port 115

Port 116

Port 117

Port 118

Port 119

Port 120

Port 121

Port 122

Port 123

Port 124

Port 125

Port 126

Port 127

Port 128

Port 129

Port 130

Port 131

Port 132

Port 133

Port 134

Port 135

Port 136

Port 137

Port 138

Port 139

Port 140

Port 141

Port 142

Port 143

Port 144

Port 145

Port 146

Port 147

Port 148

Port 149

Port 150

Port 151

Port 152

Port 153

Port 154

Port 155

Port 156

Port 157

Port 158

Port 159

Port 160

Port 161

Port 162

Port 163

Port 164

Port 165

Port 166

Port 167

Port 168

Port 169

Port 170

Port 171

Port 172

Port 173

Port 174

Port 175

Port 176

Port 177

Port 178

Port 179

Port 180

Port 181

Port 182

Port 183

Port 184

Port 185

Port 186

Port 187

Port 188

Port 189

Port 190

Port 191

Port 192

Port 193

Port 194

Port 195

Port 196

Port 197

Port 198

Port 199

Port 200

Port 201

Port 202

Port 203

Port 204

Port 205

Port 206

Port 207

Port 208

Port 209

Port 210

Port 211

Port 212

Port 213

Port 214

Port 215

Port 216

Port 217

Port 218

Port 219

Port 220

Port 221

Port 222

Port 223

Port 224

Port 225

Port 226

Port 227

Port 228

Port 229

Port 230

Port 231

Port 232

Port 233

Port 234

Port 235

Port 236

Port 237

Port 238

Port 239

Port 240

Port 241

Port 242

Port 243

Port 244

Port 245

Port 246

Port 247

Port 248

Port 249

Port 250

Port 251

Port 252

Port 253

Port 254

Port 255

Port 256

Port 257

Port 258

Port 259

Port 260

Port 261

Port 262

Port 263

Port 264

Port 265

Port 266

Port 267

Port 268

Port 269

Port 270

Port 271

Port 272

Port 273

Port 274

Port 275

Port 276

Port 277

Port 278

Port 279

Port 280

Port 281

Port 282

Port 283

Port 284

Port 285

Port 286

Port 287

Port 288

Port 289

Port 290

Port 291

Port 292

Port 293

Port 294

Port 295

Port 296

Port 297

Port 298

Port 299

Port 300

Port 301

Port 302

Port 303

Port 304

Port 305

Port 306

Port 307

Port 308

Port 309

Port 310

Port 311

Port 312

Port 313

Port 314

Port 315

Port 316

Port 317

Port 318

Port 319

Port 320

Port 321

Port 322

Port 323

Port 324

Port 325

Port 326

Port 327

Port 328

Port 329

Port 330

Port 331

Port 332

Port 333

Port 334

Port 335

Port 336

Port 337

Port 338

Port 339

Port 340

Port 341

Port 342

Port 343

Port 344

Port 345

Port 346

Port 347

Port 348

Port 349

Port 350

Port 351

Port 352

Port 353

Port 354

Port 355

Port 356

Port 357

Port 358

Port 359

Port 360

Port 361

Port 362

Port 363

Port 364

Port 365

Port 366

Port 367

Port 368

Port 369

Port 370

Port 371

Port 372

Port 373

Port 374

Port 375

Port 376

Port 377

Port 378

Port 379

Port 380

Port 381

Port 382

Port 383

Port 384

Port 385

Port 386

Port 387

Port 388

Port 389

Port 390

Port 391

Port 392

Port 393

Port 394

Port 395

Port 396

Port 397

Port 398

Port 399

Port 400

Port 401

Port 402

Port 403

Port 404

Port 405

Port 406

Port 407

Port 408

Port 409

Port 410

Port 411

Port 412

Port 413

Port 414

Port 415

Port 416

Port 417

Port 418

Port 419

Port 420

Port 421

Port 422

Port 423

Port 424

Port 425

Port 426

Port 427

Port 428

Port 429

Port 430

Port 431

Port 432

Port 433

Port 434

Port 435

Port 436

Port 437

Port 438

Port 439

Port 440

Port 441

Port 442

Port 443

Port 444

Port 445

Port 446

Port 447

Port 448

Port 449

Port 450

Port 451

Port 452

Port 453

Port 454

Port 455

Port 456

Port 457

Port 458

Port 459

Port 460

Port 461

Port 462

Port 463

Port 464

Port 465

Port 466

Port 467

Port 468

Port 469

Port 470

Port 471

Port 472

Port 473

Port 474

Port 475

Port 476

Port 477

Port 478

Port 479

Port 480

Port 481

Port 482

Port 483

Port 484

Port 485

Port 486

Port 487

Port 488

Port 489

Port 490

Port 491

Port 492

Port 493

Port 494

Port 495

Port 496

Port 497

Port 498

Port 499

Port 500

Port 501

Port 502

Port 503

Port 504

Port 505

Port 506

Port 507

Port 508

Port 509

Port 510

Port 511

Port 512

Port 513

Port 514

Port 515

Port 516

Port 517

Port 518

Port 519

Port 520

Port 521

Port 522

Port 523

Port 524

Port 525

Port 526

Port 527

Port 528

Port 529

Port 530

Port 531

Port 532

Port 533

Port 534

Port 535

Port 536

Port 537

Port 538

Port 539

Port 540

Port 541

Port 542

Port 543

Port 544

Port 545

Port 546

Port 547

Port 548

Port 549

Port 550

Port 551

Port 552

Port 553

Port 554

Port 555

Port 556

Port 557

Port 558

Port 559

Port 560

Port 561

Port 562

Port 563

Port 564

Port 565

Port 566

Port 567

Port 568

Port 569

Port 570

Port 571

Port 572

Port 573

Port 574

Port 575

Port 576

Port 577

Port 578

Port 579

Port 580

Port 581

Port 582

Port 583

Port 584

Port 585

Port 586

Port 587

Port 588

Port 589

Port 590

Port 591

Port 592

Port 593

Port 594

Port 595

Port 596

Port 597

Port 598

Port 599

Port 600

Port 601

Port 602

Port 603

Port 604

Port 605

Port 606

Port 607

Port 608

Port 609

Port 610

Port 611

Port 612

Port 613

Port 614

Port 615

Port 616

Port 617

Port 618

Port 619

Port 620

Port 621

Port 622

Port 623

Port 624

Port 625

Port 626

Port 627

Port 628

Port 629

Port 630

Port 631

Port 632

Port 633

Port 634

Port 635

Port 636

Port 637

Port 638

Port 639

Port 640

Port 641

Port 642

Port 643

Port 644

Port 645

Port 646

Port 647

Port 648

Port 649

Port 650

Port 651

Port 652

Port 653

Port 654

Port 655

Port 656

Port 657

Port 658

Port 659

Port 660

Port 661

Port 662

Port 663

Port 664

Port 665

Port 666

Port 667

Port 668

Port 669

Port 670

Port 671

Port 672

Port 673

Port 674

Port 675

Port 676

Port 677

Port 678

Port 679

Port 680

Port 681

Port 682

Port 683

Port 684

Port 685

Port 686

Port 687

Port 688

Port 689

Port 690

Port 691

Port 692

Port 693

Port 694

Port 695

Port 696

Port 697

Port 698

Port 699

Port 700

Port 701

Port 702

Port 703

Port 704

Port 705

Port 706

Port 707

Port 708

Port 709

Port 710

Port 711

Port 712

Port 713

Port 714

Port 715

Port 716

Port 717

Port 718

Port 719

Port 720

Port 721

Port 722

Port 723

Port 724

Port 725

Port 726

Port 727

Port 728

Port 729

Port 730

Port 731

Port 732

Port 733

Port 734

Port 735

Port 736

Port 737

Port 738

Port 739

Port 740

Port 741

Port 742

Port 743

Port 744

Port 745

Port 746

Port 747

Port 748

Port 749

Port 750

Port 751

Port 752

Port 753

Port 754

Port 755

Port 756

Port 757

Port 758

Port 759

Port 760

Port 761

Port 762

Port 763

Port 764

Port 765

Port 766

Port 767

Port 768

Port 769

Port 770

Port 771

Port 772

Port 773

Port 774

Port 775

Port 776

Port 777

Port 778

Port 779

Port 780

Port 781

Port 782

Port 783

Port 784

Port 785

Port 786

Port 787

Port 788

Port 789

Port 790

Port 791

Port 792

Port 793

Port 794

Port 795

Port 796

Port 797

Port 798

Port 799

Port 800

Port 801

Port 802

Port 803

Port 804

Port 805

Port 806

Port 807

Port 808

Port 809

Port 810

Port 811

Port 812

Port 813

Port 814

Port 815

Port 816

Port 817

Port 818

Port 819

Port 820

Port 821

Port 822

Port 823

Port 824

Port 825

Port 826

Port 827

Port 828

Port 829

Port 830

Port 831

Port 832

Port 833

Port 834

Port 835

Port 836

Port 837

Port 838

Port 839

Port 840

Port 841

Port 842

Port 843

Port 844

Port 845

Port 846

Port 847

Port 848

Port 849

Port 850

Port 851

Port 852

Port 853

Port 854

Port 855

Port 856

Port 857

Port 858

Port 859

Port 860

Port 861

Port 862

Port 863

Port 864

Port 865

Port 866

Port 867

Port 868

Port 869

Port 870

Port 871

Port 872

Port 873

Port 874

Port 875

Port 876

Port 877

Port 878

Port 879

Port 880

Port 881

Port 882

Port 883

Port 884

Port 885

Port 886

Port 887

Port 888

Port 889

Port 890

Port 891

Port 892

Port 893

Port 894

Port 895

Port 896

Port 897

Port 898

Port 899

Port 900

Port 901

Port 902

Port 903

Port 904

Port 905

Port 906

Port 907

Port 908

Port 909

Port 910

Port 911

Port 912

Port 913

Port 914

Port 915

Port 916

Port 917

Port 918

Port 919

Port 920

Port 921

Port 922

Port 923

Port 924

Port 925

Port 926

Port 927

Port 928

Port 929

Port 930

Port 931

Port 932

Port 933

Port 934

Port 935

Port 936

Port 937

Port 938

Port 939

Port 940

Port 941

Port 942

Port 943

Port 944

Port 945

Port 946

Port 947

Port 948

Port 949

Port 950

Port 951

Port 952

Port 953

Port 954

Port 955

Port 956

Port 957

Port 958

Port 959

Port 960

Port 961

Port 962

Port 963

Port 964

Port 965

Port 966

Port 967

Port 968

Port 969

Port 970

Port 971

Port 972

Port 973

Port 974

Port 975

Port 976

Port 977

Port 978

Port 979

Port 980

Port 981

Port 982

Port 983

Port 984

Port 985

Port 986

Port 987

Port 988

Port 989

Port 990

Port 991

Port 992

Port 993

Port 994

Port 995

Port 996

Port 997

Port 998

Port 999

Port 1000

Port 1001

Port 1002

Port 1003

Port 1004

Port 1005

Port 1006

Port 1007

Port 1008

Port 1009

Port 1010

Port 1011

Port 1012

Port 1013

Port 1014

Port 1015

Port 1016

Port 1017

Port 1018

Port 1019

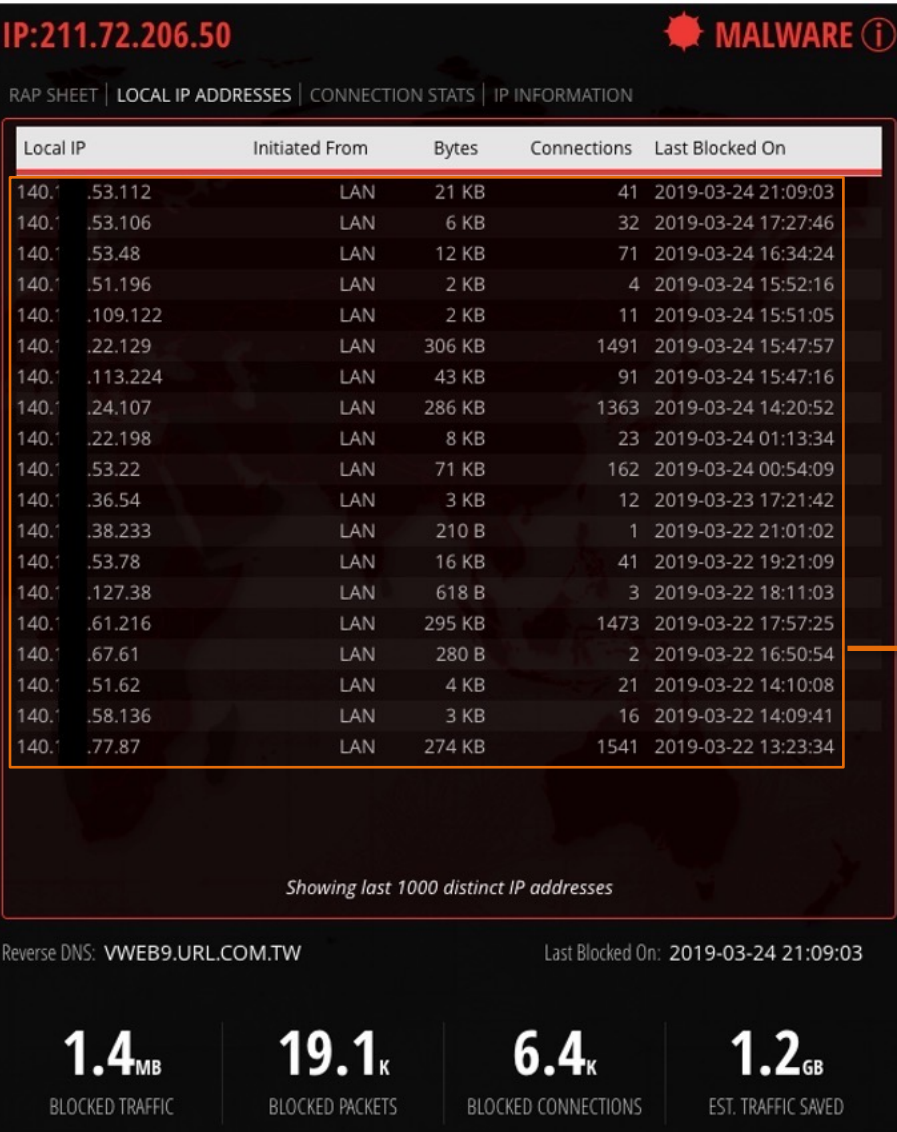
Port 1020

Port 1021

Port 1022

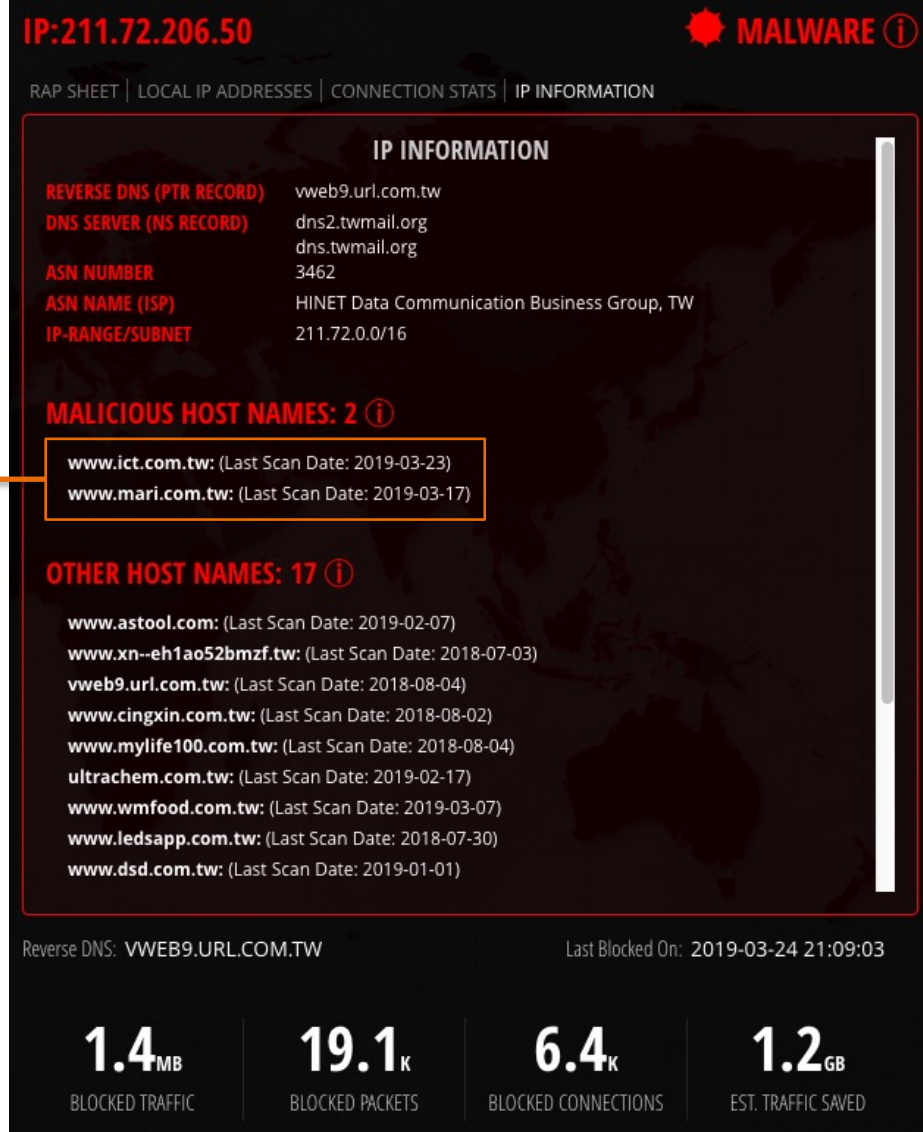
Port 102

全球資安情資分析防禦系統- Malware





除了ict.com.tw, 尚有另一具有風險的domain => mari.com.tw

內部為數不少的IP皆是對外連線至同一目的地



全球資安情資分析防禦系統- Malware – exe file

IP:117.56.6.155  **MALWARE** 

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION STATS | IP INFORMATION

THREATS DETECTED: 4 MALWARE

HORSE GENERIC4_C.CGCE
THREAT URL http://117.56.6.155:80/jinling/svreen-saver-tdb.exe
LAST SCAN DATE 2019-03-24 09:33:27
FILE CHECKSUM SHA256 - c77f6bc631f0b037a625cdb00efcf43a053e6667fde432431ac9155d1676c20d

HORSE GENERIC4_C.CGCE
THREAT URL http://tech2.npm.edu.tw:80/jinling/svreen-saver-tdb.exe
LAST SCAN DATE 2019-03-24 09:21:57
FILE CHECKSUM SHA256 - c77f6bc631f0b037a625cdb00efcf43a053e6667fde432431ac9155d1676c20d

HORSE GENERIC4_C.CGCE
THREAT URL http://tech2.npm.edu.tw/jinling/svreen-saver-tdb.exe
LAST SCAN DATE 2019-03-24 04:00:53
FILE CHECKSUM SHA256 -

Reverse DNS: 117-56-6-155.HINET-IP.HINET.NET Last Blocked On: 2019-03-24 18:17:29

420_B
BLOCKED TRAFFIC

6
BLOCKED PACKETS

2
BLOCKED CONNECTIONS

361.9_{KB}
EST. TRAFFIC SAVED



全球資安情資分析防禦系統- Exploit – MSSQL/MYSQL

IP:140. .142

EXPLOIT ⓘ

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION STATS | IP INFORMATION

Local IP	Initiated From	Bytes	Connections	Last Blocked On
2.239.215.28	LAN	896 B	8	2019-03-24 17:58:59
210.56.20.53	LAN	256 B	2	2019-03-24 15:03:15
181.120.81.194	LAN	128 B	1	2019-03-24 07:14:11
98.112.73.22	LAN	64 B	1	2019-03-23 22:15:12
193.77.58.231	LAN	384 B	3	2019-03-23 06:28:58
193.77.58.48	LAN	256 B	2	2019-03-23 06:26:41

Showing last 1000 distinct IP addresses

Reverse DNS: N/A

Last Blocked On: 2019-03-24 17:58:59

2KB

BLOCKED TRAFFIC

31

BLOCKED PACKETS

17

BLOCKED CONNECTIONS

3.1MB

EST. TRAFFIC SAVED

LOAD MORE RESULTS

IP:140. .142

EXPLOIT ⓘ

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION STATS | IP INFORMATION

Protocol	Source	Destination	Count	Last Blocked On
TCP	2.239.215.28 : 1433	140. : 56038	1	2019-03-24 17:58:59
TCP	2.239.215.28 : 1433	140. : 55991	1	2019-03-24 17:58:49
TCP	2.239.215.28 : 1433	140. : 55809	1	2019-03-24 17:58:06
TCP	2.239.215.28 : 1433	140. : 55553	1	2019-03-24 17:57:16
TCP	2.239.215.28 : 1433	140. : 55272	1	2019-03-24 17:56:18
TCP	210.56.20.53 : 1433	140. : 60511	1	2019-03-24 15:03:15
TCP	181.120.81.194 : 1433	140. : 49410	1	2019-03-24 07:14:11
TCP	98.112.73.22 : 1433	140. : 56358	1	2019-03-23 22:15:12
TCP	2.239.215.28 : 1433	140. : 51655	1	2019-03-23 20:17:15
TCP	2.239.215.28 : 1433	140. : 51263	1	2019-03-23 20:15:57
TCP	210.56.20.53 : 1433	140. : 58612	1	2019-03-23 17:35:10
TCP	193.77.58.231 : 1433	140. : 64084	1	2019-03-23 06:28:58
TCP	193.77.58.231 : 1433	140. : 64076	1	2019-03-23 06:28:57
TCP	193.77.58.231 : 1433	140. : 63758	1	2019-03-23 06:28:03
TCP	193.77.58.48 : 1433	140. : 63206	1	2019-03-23 06:26:41
TCP	193.77.58.48 : 1433	140. : 62864	1	2019-03-23 06:25:37
TCP	2.239.215.28 : 1433	140. : 65185	1	2019-03-23 05:12:24

Showing last 1000 distinct connection data

Reverse DNS: N/A

Last Blocked On: 2019-03-24 17:58:59

2KB

BLOCKED TRAFFIC

31

BLOCKED PACKETS

17

BLOCKED CONNECTIONS

3.1MB

EST. TRAFFIC SAVED

EXPORT TO CSV

IP:140. .142

EXPLOIT ⓘ

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION STATS | IP INFORMATION

IP INFORMATION

ASN NUMBER

38844

ASN NAME (ISP)

National University, TW

IP-RANGE/SUBNET

140. /17

Reverse DNS: N/A

Last Blocked On: 2019-03-24 17:58:59

2KB

BLOCKED TRAFFIC

31

BLOCKED PACKETS

17

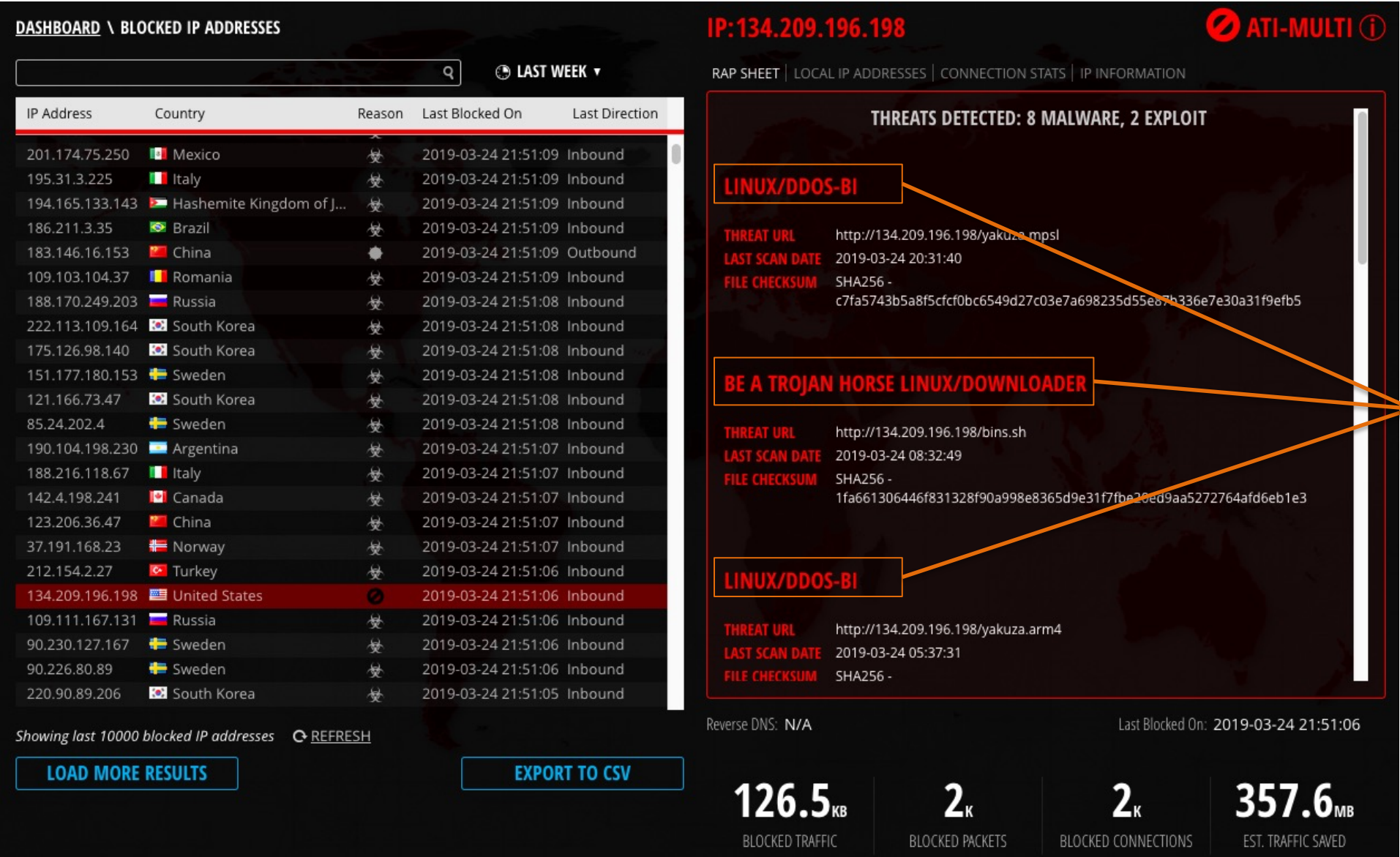
BLOCKED CONNECTIONS

3.1MB

EST. TRAFFIC SAVED

來自單位內部本身的威脅!

全球資安情資分析防禦系統- Anti-Multi – DDOS/Malware...etc



Multiple Types Attacks

多重複合式威脅, DDoS往往只為了吸引被攻擊者的注意, malware的感染才是取得控制權的目的

全球資安情資分析防禦系統- Malware – Anti-Sandboxing

DASHBOARD \ BLOCKED IP ADDRESSES

LAST WEEK

IP Address	Country	Reason	Last Blocked On	Last Direction
220.194.237.43	China	Malware	2019-03-24 21:51:29	Inbound
188.152.180.97	Italy	Malware	2019-03-24 21:51:29	Inbound
134.209.75.211	United States	Malware	2019-03-24 21:51:29	Inbound
134.209.75.202	United States	Malware	2019-03-24 21:51:29	Inbound
123.170.79.133	China	Malware	2019-03-24 21:51:29	Inbound
104.231.203.150	United States	Malware	2019-03-24 21:51:29	Inbound
84.216.173.130	Sweden	Malware	2019-03-24 21:51:29	Inbound
80.217.202.163	Sweden	Malware	2019-03-24 21:51:29	Inbound
58.48.152.65	China	Malware	2019-03-24 21:51:29	Inbound
36.231.22.63	Taiwan	Malware	2019-03-24 21:51:29	Inbound
218.94.97.26	China	Malware	2019-03-24 21:51:28	Inbound
193.56.28.132	United Kingdom	Malware	2019-03-24 21:51:28	Inbound
141.98.81.100	Panama	Malware	2019-03-24 21:51:28	Inbound
134.209.75.214	United States	Malware	2019-03-24 21:51:28	Inbound
134.209.75.46	United States	Malware	2019-03-24 21:51:28	Inbound
123.17.201.121	Vietnam	Malware	2019-03-24 21:51:28	Inbound
113.59.43.98	China	Malware	2019-03-24 21:51:28	Outbound
111.35.156.186	China	Malware	2019-03-24 21:51:28	Inbound
110.201.1.141	China	Malware	2019-03-24 21:51:28	Inbound
59.63.204.30	China	Malware	2019-03-24 21:51:28	Inbound
27.223.29.116	China	Malware	2019-03-24 21:51:28	Inbound
210.50.222.146	Australia	Malware	2019-03-24 21:51:27	Inbound
185.234.217.217	Ireland	Malware	2019-03-24 21:51:27	Inbound
171.221.120.54	Vietnam	Malware	2019-03-24 21:51:27	Inbound

Showing last 10000 blocked IP addresses

LOAD MORE RESULTS

EXPORT TO CSV

IP:113.59.43.98

MALWARE

RAP SHEET | LOCAL IP ADDRESSES | CONNECTION STATS | IP INFORMATION

THREAT URL

LAST SCAN DATE

FILE CHECKSUM

THREAT URL

LAST SCAN DATE

FILE CHECKSUM

STATIC ANALYSIS

Reverse DNS: N/A

156KB
BLOCKED TRAFFIC

2.1K
BLOCKED PACKETS

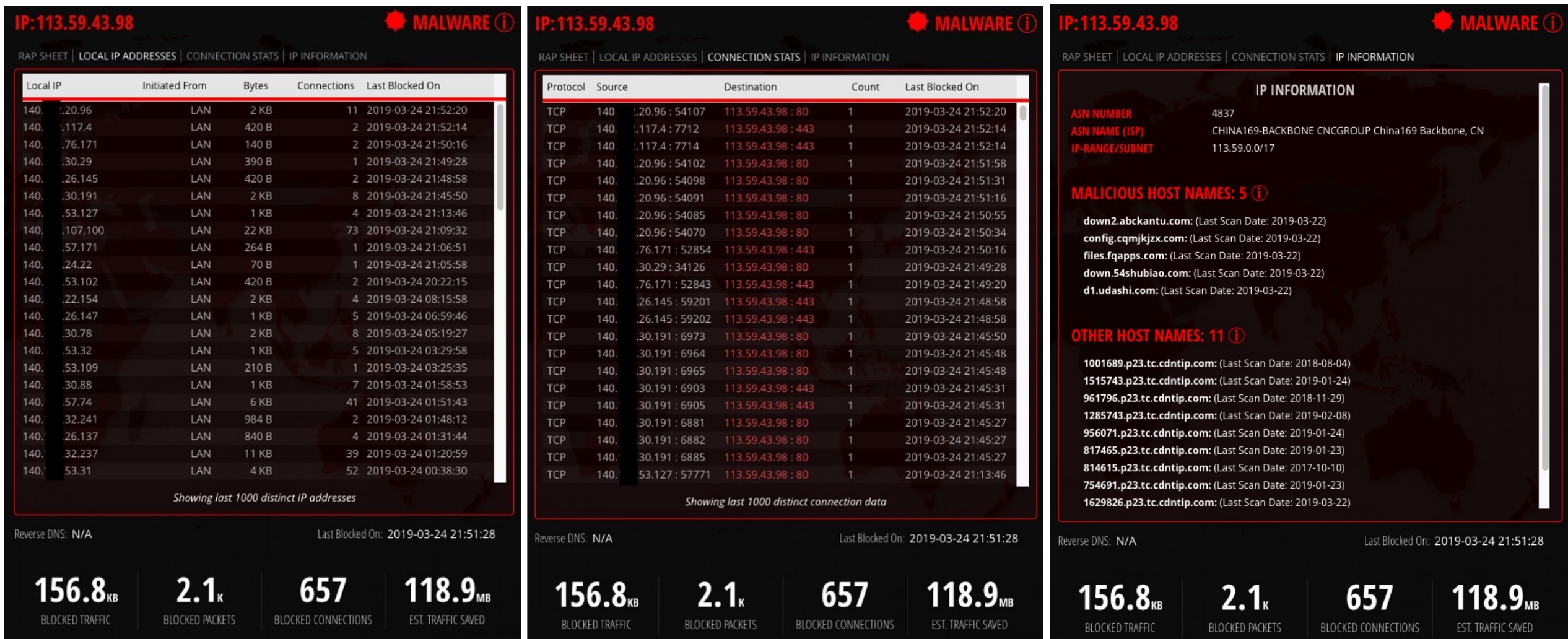
653
BLOCKED CONNECTIONS

118.2MB
EST. TRAFFIC SAVED

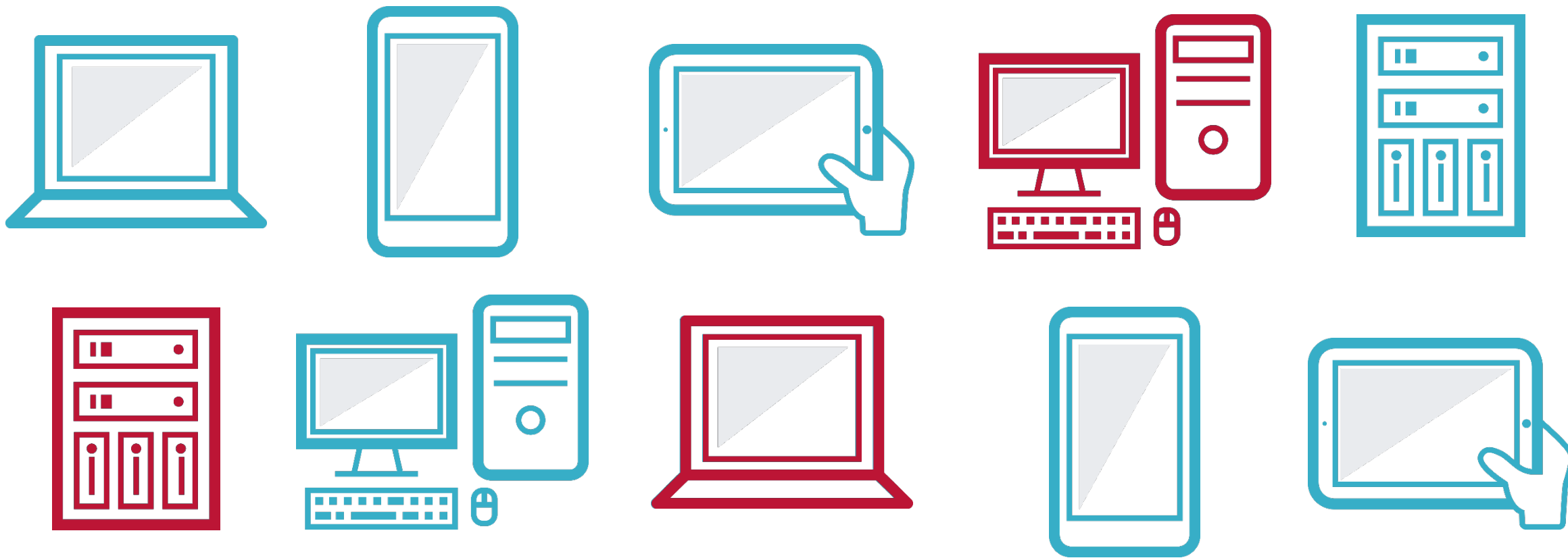
APT為IPS/Anti-Virus/NGFW
的最後一道防線?
Anti-Sandboxing => 如入無人之地

Anti-sandboxing behavior. Trying to detect the sandbox in order to evade it.
High Severity: Artifacts that are only found in Malware.

全球資安情資分析防禦系統- Malware – Anti-Sandboxing

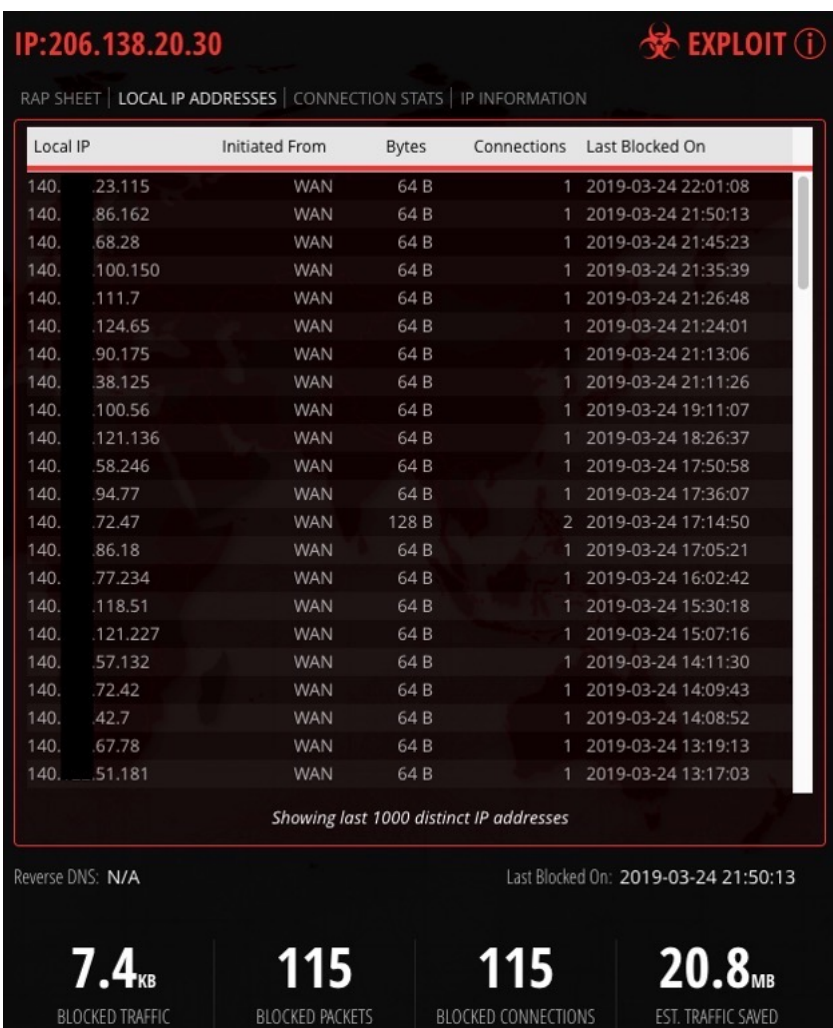
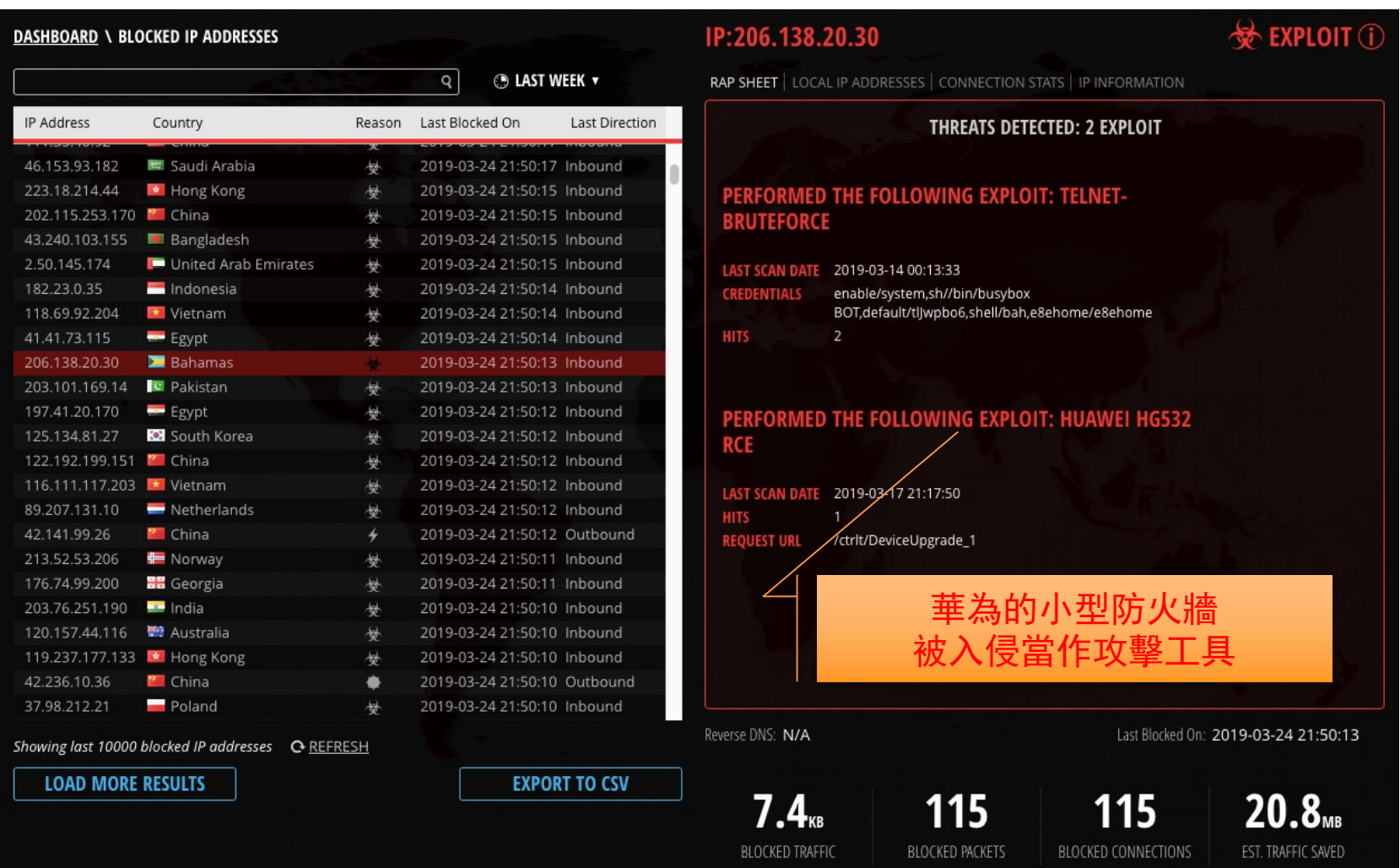


內部非常多IP皆是連線至此具有高風險的Malware來源
且連線除了藉由80 Port, 還有443的加密連線



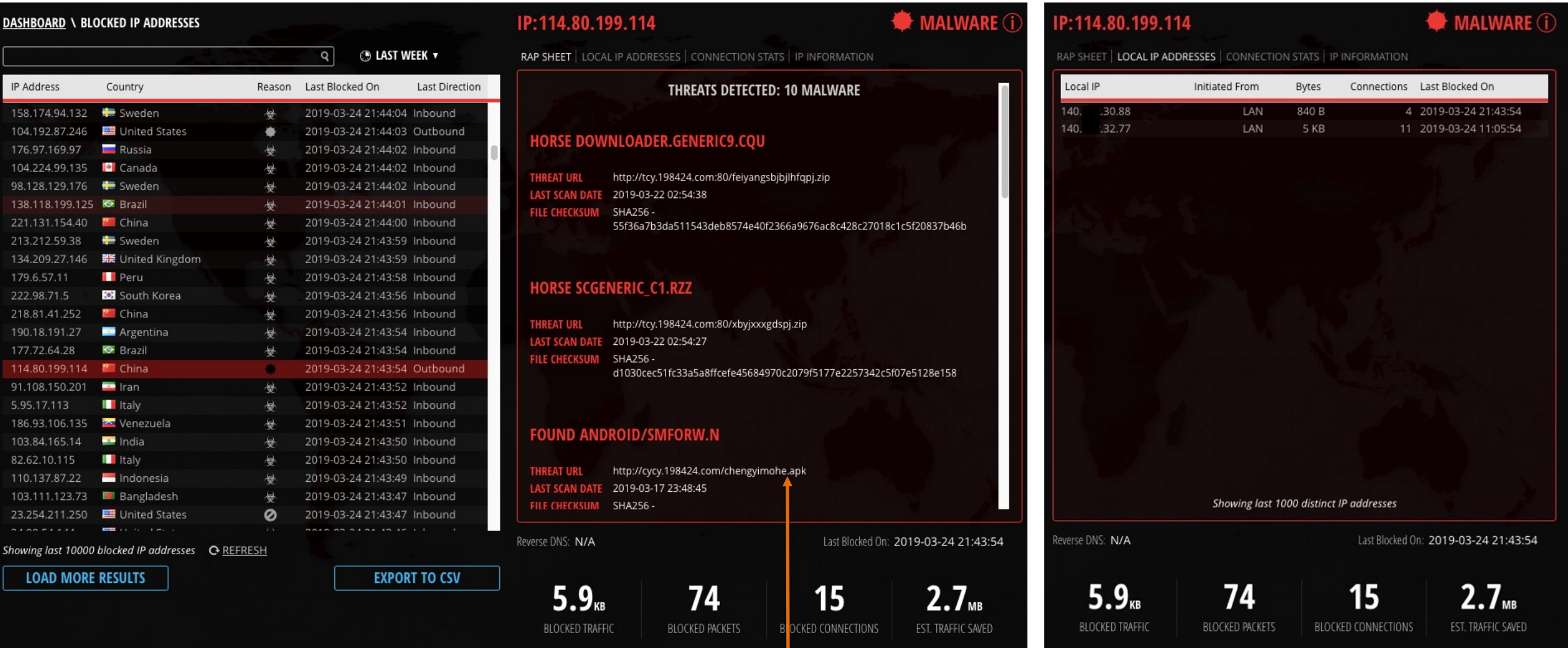
筆電, 伺服器, 網路設備, 無線AP, 個人終端裝置, IOT, OT...
使用FW/IPS/APT/Antivirus保護??
眾多設備是無法接受這些資安設備的保護的

全球資安情資分析防禦系統- 不受限任何裝置的情資判斷



<https://paper.seebug.org/490/>

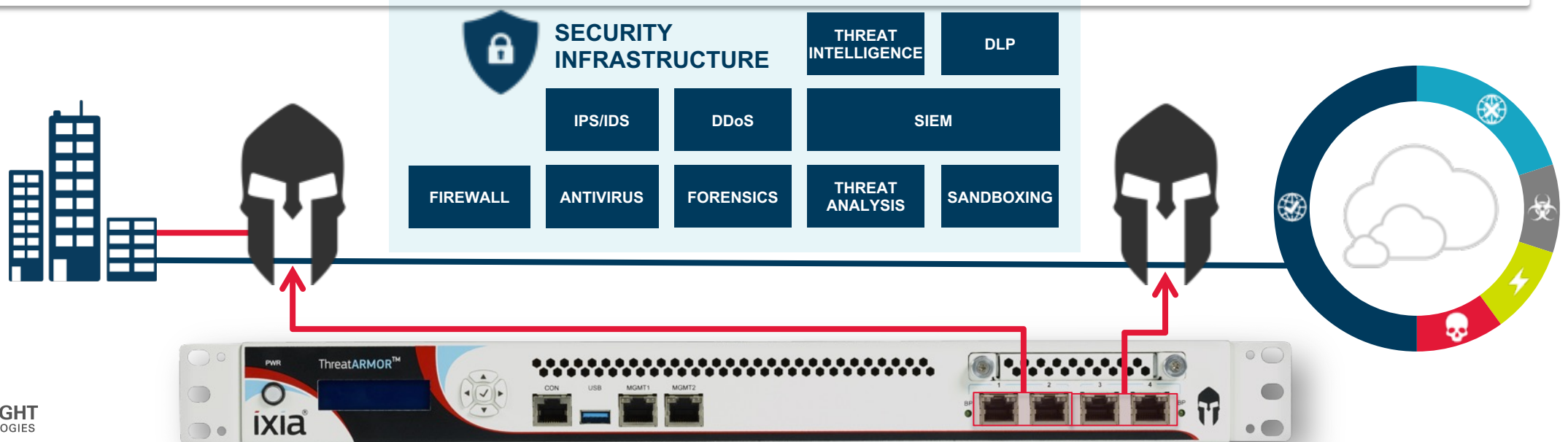
全球資安情資分析防禦系統- 不受限任何裝置的情資判斷

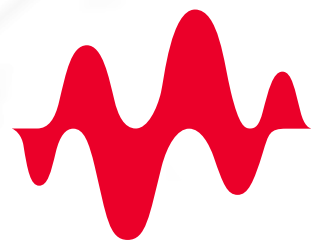


高風險的APK檔案
無需埋入安全Client至Mobile Device
直接藉由情資系統分析阻擋

全球資安情資分析防禦系統- ThreatARMOR™ 特點及優勢

1. 消除各種資安威脅的流量而縮小客戶端的攻擊面, 可減輕後端資安設備負擔(NGFW/IPS/DDOS/WAF/APT/SIEM.....等)
2. 提供全球最完整的IP及DNS威脅資料庫, 並以內建的獨有高速處理晶片協助客戶端直接在local比對, 避免網路延遲
3. 提供Exploit, Botnet, phishing, hijacked, Malware, Anti-Multiple與非法IP (未註冊IP)全面性的防禦, 並且在開啟所有功能之後, 仍然可以維持line rate speed高速處理效能!
4. 無需解開HTTPS/SSH/RDP/VPN或其他加密連線即可判斷資安威脅!
5. 100%無誤判, 再也無須擔心到底是阻擋了駭客還是客戶!
6. 業界最快每五分鐘更新資料庫, 縮短資安威脅防護時差
7. 內建Bypass機制, 即使設備發生故障, 電源無法接續, 仍可保持原有線路暢通





KEYSIGHT
TECHNOLOGIES