CYBER SECURITY ICO

World's First Cyber Security Services ICO by the
World's Most Comprehensive Cyber Security Services Provider

SECURITY plus CLOUD

We are going to create the World's First Cyber Threat Intelligence De-centralised Database On Blockchain To Predict, Warn & Stop Future Cyber Attacks

SECURITY plus CLOUD

Cisco	IBM Security	Microsoft	paloalto NETWORKS
McAfee	SOPHOS Security made simple.	Symantec	TREND MICRO
splunk>	FireEye	Check Point SOFTWARE TECHNOLOGIES LTD	FORTINET
QUALYS Continuous Security	IMPERVA	gemalto security to be free	CYLANCE
RSA SECURITY	CYBERARK	DELL SecureWorks	vmware

VS SECURITY plus CLOUD

ABOUT OUR COMPANY

SecurityPlusCloud

MISSION, VISION, GROWTH

MISSION

Establish World's Largest Cyber Security Operations Centre (SOC) in all regions around the world to protect every organization, government, enterprise & children from current & future cyber security threats.

VISION

Reach amongst the Top 10 Cyber Security companies in the world capturing atleast 1% share of the Trillion $ market by 2021 & 8% by 2027.

GROWTH

Hypergrowth expansion across 22 cities over 6 continents with aggressive hunter sales approach in every economic hub producing viral customer growth.

SecurityPlusCloud CUSTOMERS

Established supply relationships with above clients of our parent company.

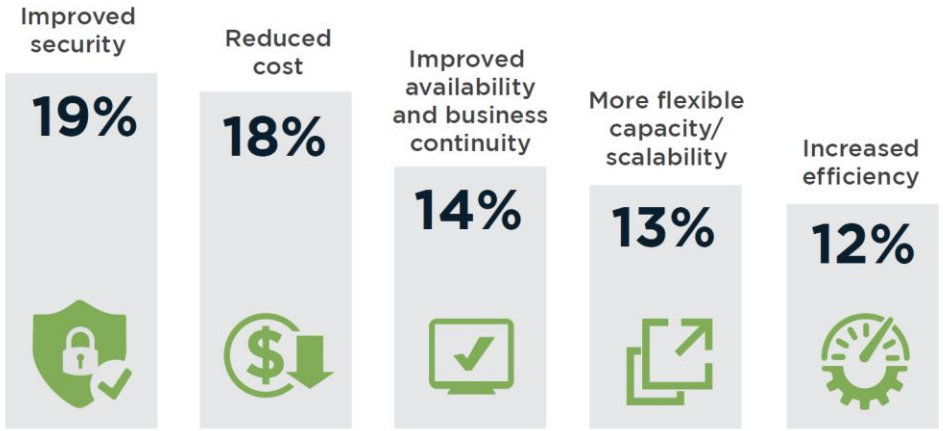
SecurityPlusCloud ADVANTAGE

SPC ADVANTAGE

The cost for businesses to invest in exorbitant security solutions & manpower becomes an expenditure of the past with our MSSP solution.

SpC's constant investment in elastic hardware and highly qualified cyber security team ensures enterprises & governments are always ahead of complex cyber security threats.

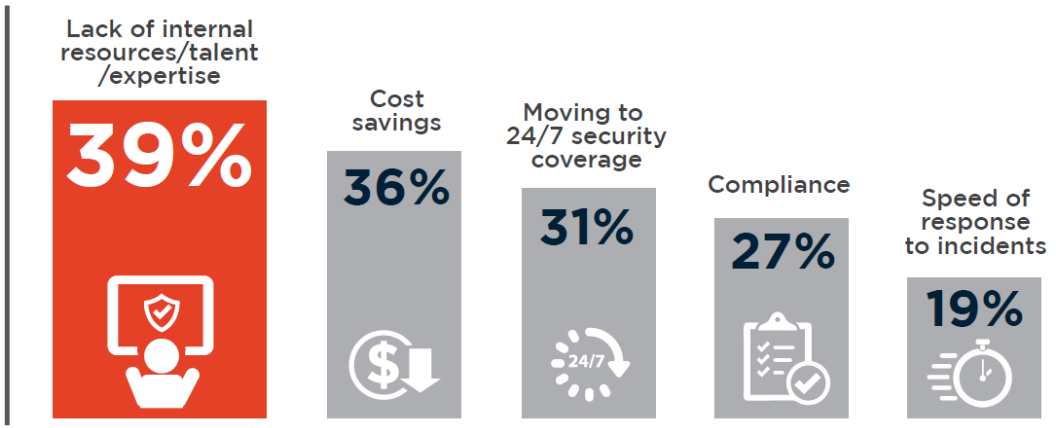
Our in-house expertise supports a network capable of growing dynamically, evolving to encompass new threat categories, with seamless and minimal intervention by organisations. Security hardware located in our network helps prevent sophisticated cyber attacks.



The two most frequently mentioned benefits organizations have realized from MSSP are improved security and reduced cost.

Improved availability, flexible capacity, scalability and increased efficiency round out the top 5 benefits.

The above research confirms that organizations gain the most benefits with a managed security services provider.



The predominant driver for **39%** of organizations to consider managed security services provider is lack of internal security resources, talent and expertise against increasingly sophisticated threats.

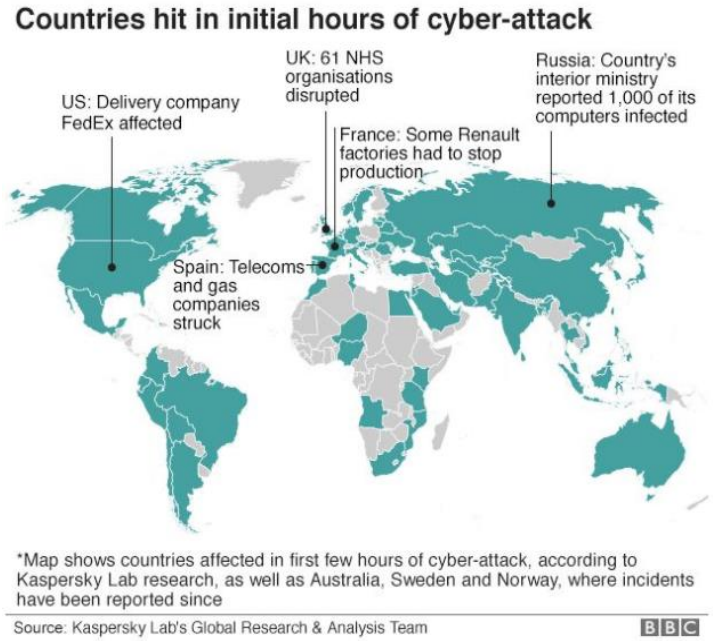
This is closely followed by a desire to reduce the cost of security (36%), moving to continuous 24/7 security coverage (31%), improving compliance (27%) and increasing the speed of response to incidents (19%).

CYBER SECURITY BREACHES (NEWS)

Cyber Security
WANNACRY

WannaCry is back! Virus hits Australian traffic cameras and shuts down a Honda plant in Japan

The WannaCry virus found a weakness in the Sayama plants operational systems running Windows 10



The global ransomware epidemic is just getting started

WannaCry should have been a major warning to the world about ransomware. Then the GoldenEye strain of Petya ransomware arrived. What's next?

BY ALFRED NG / JUNE 28, 2017 7:21 AM PDT

WannaCry ransomware attack at LG Electronics takes systems offline

'WannaCry' Malware Attack Could Just Be Getting Started: Experts

by ALEX JOHNSON

Cyber Security

PETYA RANSOMWARE

Petya cyberattack spreads to 65 countries

Brett Molina,Jon Swartz and Rachel Sandler, USA TODAY Published 10:43 a.m. ET June 28, 2017 | Updated 8:07 p.m. ET June 28, 2017

June 28 — 1 comment

FedEx's Dutch operations have been 'significantly affected' by the Petya virus

by Sean O'Kane | @sokane1

June 27 — 31 comments

A new ransomware attack is hitting airlines, banks and utilities across Europe

by Russell Brandom | @russellbrandom

Petya cyber attack: This is a wiper, not ransomware and much, much worse

Petya cyber attack that swept globally, and has infected enterprise networks across Europe is actually much worse than initially thought. Security researchers have now come to the conclusion that the Petya attack is not a ransomware, but a wiper instead.

Turns Out New Petya is Not a Ransomware, It's a Destructive Wiper Malware

Wednesday, June 28, 2017 Swati Khandelwal

JUN 27, 2017 @ 02:16 PM 60,908

Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry

West Virginia hospital replaces computers after Petya cyberattack

Princeton Community Hospital fell victim to the global NotPetya attack on Tuesday and plans to replace the corrupted network with a newly built system.

By Jessica Davis | June 30, 2017 | 02:43 PM

FedEx expects 'material' financial impact from Petya cyber attack

Published: July 17, 2017 9:11 a.m. ET

News

Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down

Like 12.3M

Wednesday, Sep

Daily Mail AUSTRALIA

Home | U.K. | U.S. | News | World News | Sport | TV&Showbiz | Femail | Health | Scienc

Breaking News | News | World News | Sydney | Melbourne | Brisbane | Malcolm Turnbull | Headlines | Wir

Cyber attack hits CHERNOBYL radiation system: 'Goldeneye' ransomware strikes across the globe, with US drug firm Merck, advertising giants WPP and Ukrainian power grid among victims

- New ransomware attack hit computers around the globe on Tuesday
- Ukraine is worst hit so far, with Chernobyl radiation monitoring system affected
- Country's deputy leader said all computers are down in 'unprecedented' attack
- Companies in UK, US, France, Norway, Denmark have also confirmed issues
- IT experts dubbed new virus GoldenEye and say it is similar to 'WannaCry'

By CHRIS PLEASANCE and SCOTT CAMPBELL FOR MAILONLINE
PUBLISHED: 00:02 +10:00, 28 June 2017 | UPDATED: 14:41 +10:00, 29 June 2017

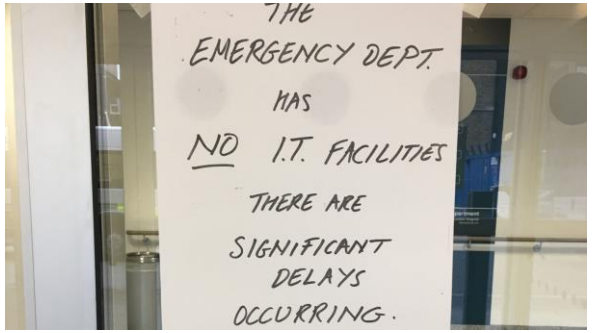
Cyber Security
NHS - UK

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Healt

Latest Headlines | News | World News | Arts | Headlines | France | Pictures | Most

As a cyber attack cripples the NHS and doctors are forced to use a pen and paper... Wouldn't life be better without the tyranny of computers, writes



East and North Hertfordshire NHS
NHS Trust

essionals | Member Area | Our Hospitals | About The Trust | Get Involved | News & Media

SEARCH

We're currently experiencing significant problems with our IT and telephone network

Which we're trying to resolve as soon as possible

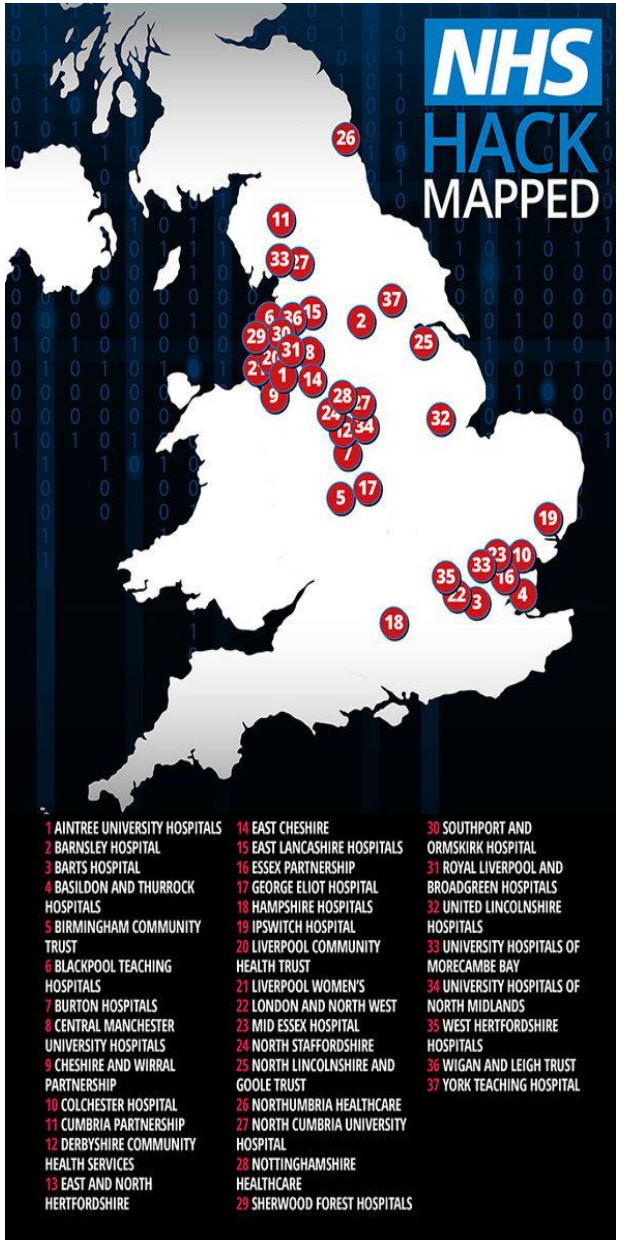
This means that people will have difficulty phoning us for the time being – please bear with us. Apologies for any inconvenience.

Peel GPs
@peelgps
Follow

All Greater Manchester networks down -we cannot access any patient info plz RT @NHSBuryCCG

RETWEETS 15

2:54 PM - 12 May 2017

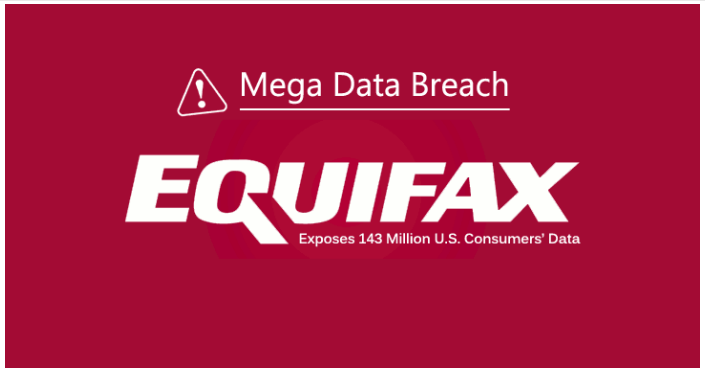


SECURITY plus CLOUD

WWW.SECURITYPLUSCLOUD.COM.AU

Cyber Security

EQUIFAX BREACH



The Equifax Hack--Bad for Them, Worse for Us

If all of our personal information is now widely available many of our current methods of authenticating identity, if not all of them, are suspect

By Paul Rosenzweig on September 12, 2017

How Bad Is the Equifax Hack?

It will take us a long time to figure that out.

By Josephine Wolff

Massive Equifax Hack Shows Cyber Risk to Deposits and Investments Today

Share 1 | Tweet 1 | Share 0 | Google + 0 | Email 0

-- Published: Wednesday, 13 September 2017 | Print | **Comment - New!**

By Jan Skoyles

- 44% of US population affected by Equifax hack
- Hackers took names, birthdays and addresses, Social Security and driver's license numbers
- Steve Mnuchin "concerned about the global financial system and keeping it safe,"
- Hacks is a reminder of the vulnerabilities created in a connected world
- Cyber security is a major threat to both banking and financial industry
- Investors should hold physical gold as insurance against hacking and cyber attacks

Equifax hack likely impacted all US adults, cybersecurity expert warns

By Brittany De Lea | Published September 11, 2017 | Personal Finance | FOXBusiness

Equifax data leak could involve 143 million consumers

by Ron Miller

Equifax stock tumbles 14% after credit score hack

by Katie Roof

Equifax shares tumble another 8% after hack

Posted yesterday by Katie Roof (@Katie_Roof)

Equifax turned its hack into a public relations catastrophe

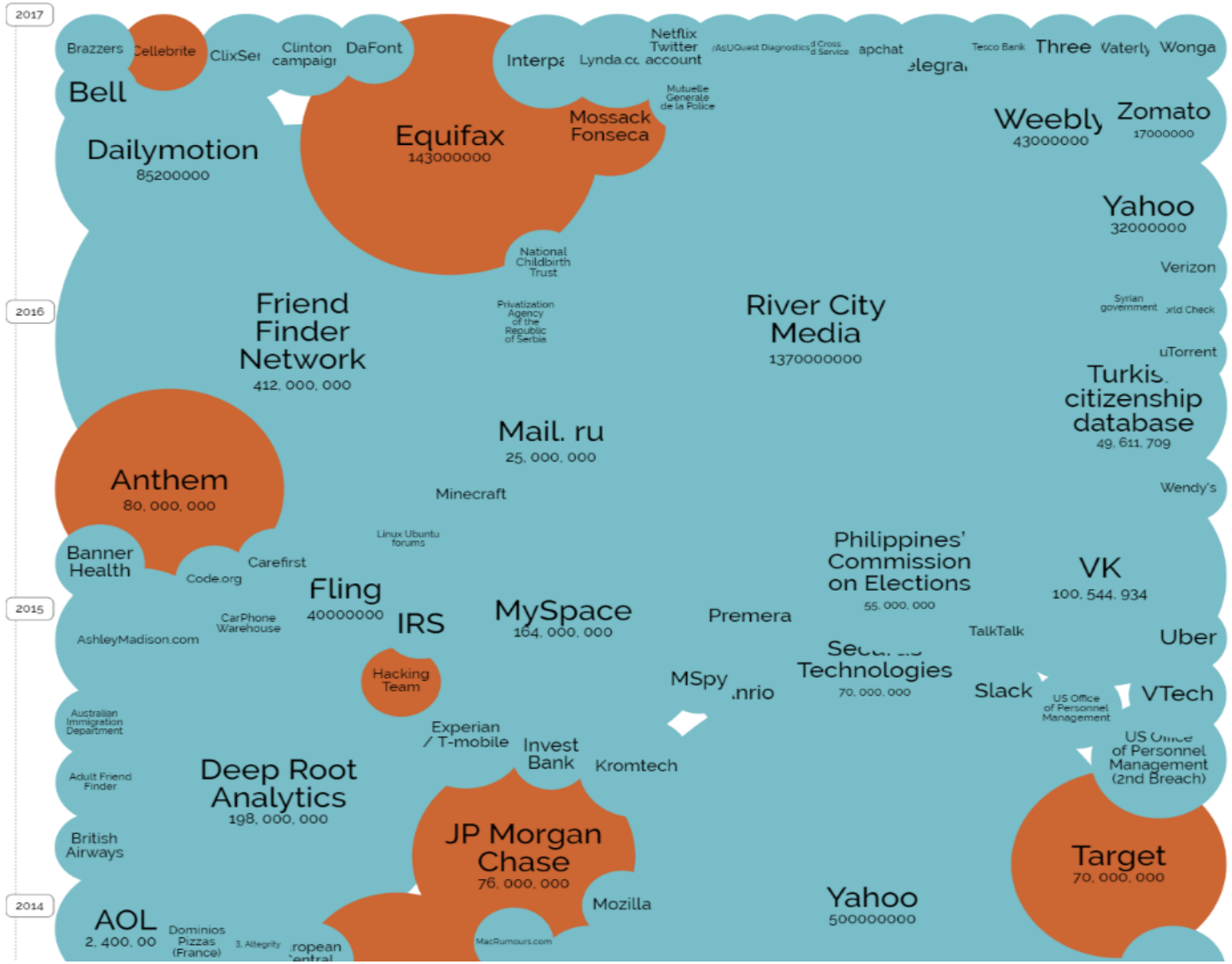
by Danielle Wiener-Bronner @dwbronner

September 13, 2017: 8:47 AM ET

Recommend 182

WORLD's BIGGEST DATA BREACHES - SEP 2017

Cyber Security
DATA BREACHES



SECURITY plus CLOUD

WWW.SECURITYPLUSCLOUD.COM.AU

Cyber Security FAMOUS HACKS

Hackers selling 117 million LinkedIn passwords

by Jose Pagliery @Jose_Pagliery

May 19, 2016: 10:59 AM ET

MAY 16, 2017 @ 10:00 AM 21,838

Data Protection Mishap Leaves 55M Philippine Voters at Risk

Posted on: April 6, 2016 at 8:09 pm Posted in: Bad Sites, Targeted Attacks Author: Trend Micro

Hackers break into Telegram, revealing 15 million users' phone numbers

REUTERS AUGUST 2, 2016 10:15 AM

DocuSign Confirms Hack And The Stolen Data Could Put You At Risk

March 15, 2017

Hackers Steal Payment Card Data From Over 1,150 InterContinental Hotels

Wednesday, April 19, 2017 Swati Khandelwal

Dun & Bradstreet database breached, 33.6M files vulnerable

HBO CYBERATTACK IS "SEVEN TIMES WORSE" THAN THE SONY HACK

BY CLAIRE SHAFFER ON 8/2/17 AT 11:17 AM

Sony says massive hack cost the company $15 million

THE ASSOCIATED PRESS / Feb 04, 2015

The company is forecasting a loss of 170 billion yen ($1.4 billion) for the fiscal year.

The entire Turkish citizenship database has allegedly been leaked online

Lianna Brinded

Apr. 4, 2016, 10:58 AM 22,311

Indian hacker group leaks data of 1.7 million Snapchat users after CEO's 'poor country' comments: Report

Target's Data Breach Gets Worse: 70 Million Customers Had Info Stolen, Including Names, Emails And Phones

Posted Jan 10, 2014 by Sarah Perez (@sarahintampa)

Yahoo Says 1 Billion User Accounts Were Hacked

By VINDU GOEL and NICOLE PERLROTH DEC. 14, 2016

Bluetooth BlueBorne Attack

Critical BlueBorne Vulnerability Infects More Than 5 Billion Bluetooth

1.5 million Verizon Enterprise customers hacked: Report

Anita Balakrishnan | @MsABalakrishnan

Published 4:22 PM ET Thu, 24 March 2016 | Updated 5:28 PM ET Thu, 24 March 2016

Nearly 800,000 Brazzers Porn Site Accounts Exposed in Forum Hack

JOSEPH COX Sep 5 2016, 8:00pm

Dropbox hack leads to leaking of 68m user passwords on the internet

Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked

Ashley Madison offers to pay $11.2 million to hacking victims

Panama Papers leak was a hack, firm's founder says

BY KATIE BO WILLIAMS - 04/06/16 07:02 AM EDT

INVESTMENT BANKING | LEGAL/REGULATORY

JPMorgan Chase Hacking Affects 76 Million Households

BY JESSICA SILVER-GREENBERG, MATTHEW GOLDSTEIN AND NICOLE PERLROTH OCTOBER 2, 2014 12:50 PM

British Airways frequent-flyer accounts hacked

Airline says no personal information viewed or stolen and it has frozen affected accounts while it resolves issue

French police hit by security breach as data put online

27 June 2016 | Europe

Share

CYBER SECURITY PROBLEMS

Cyber Security
CRITICAL INFRASTRUCTURE

THREATS TO CRITICAL INFRASTRUCTURE

Critical infrastructure systems are vulnerable to today's motivated cyberterrorists, fraudsters and well-funded agents of espionage.
All control systems belonging to critical infrastructure are either vulnerable or already under attack from outside sources.

Cyber Security VULNERABILITIES

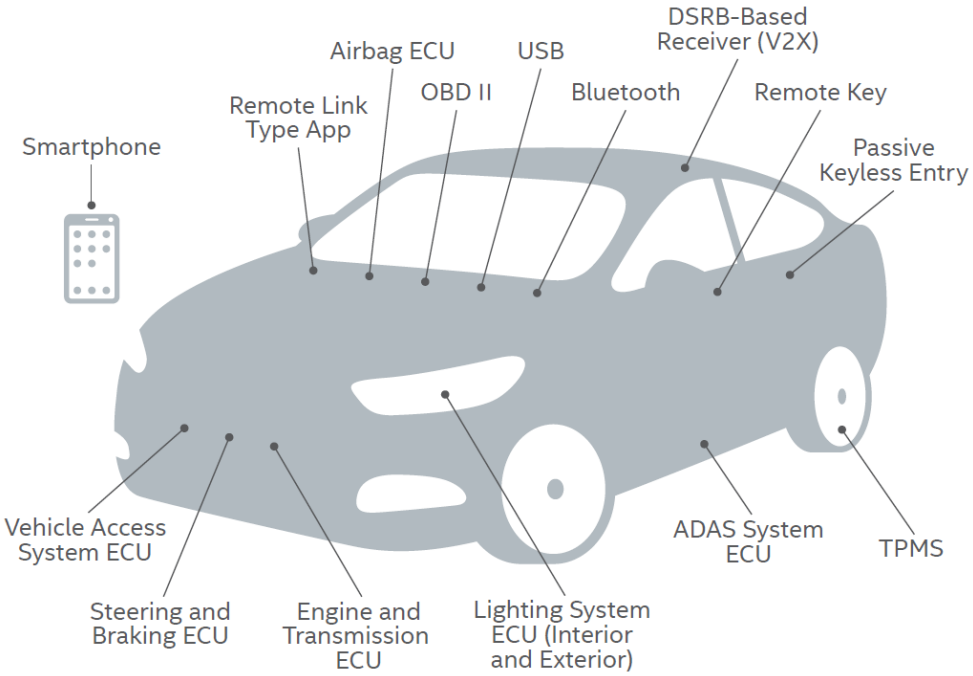
Smartwatches – Who is accessing your smartwatch, **You or 3rd Party ?**
Hint: Top devices are vulnerable to a cyberattack.

- Operating system kernel
- Networking software/WiFi
- User interface
- Memory
- Local files and storage system
- Access control/security software

Cloud Applications –Are you sure no one can access them except **You ?**
Hint: Read the news on Cloud Applications which are regularly hacked !

- Cloud virtual machine and control apps
- Web app
- Memory
- Local files and storage system
- Access control/security software

Cars – Who can access your over internet besides **YOU ?**
Hint: Connected cars are hackable !

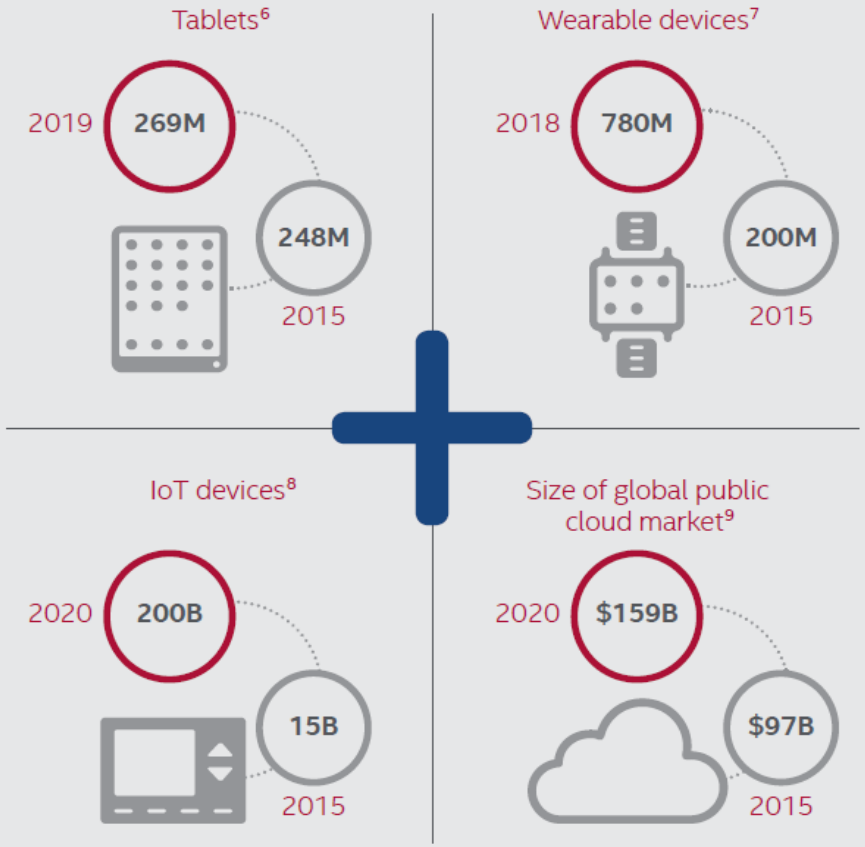


Cyber Security PROBLEMS

Gartner Says:

- 8.4 Billion Connected Things Will Be in Use in 2017
- 11.1 Billion Connected Things Will Be in Use in 2018
- 20.4 Billion Connected Things Will Be in Use in 2020

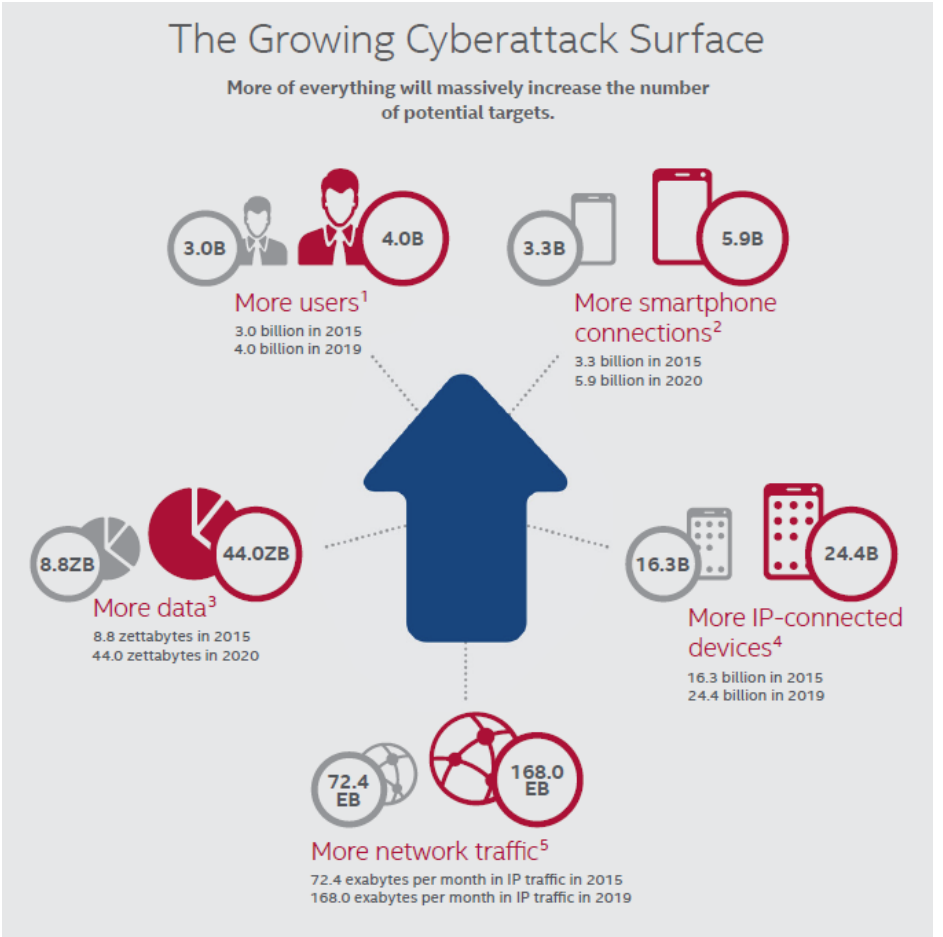
And all these connected Things need SECURITY



World is experiencing Exponential Growth in:

- Users, data & Network Traffic
- Smart Phones & Encrypted Connections
- Internet of Things (IoTs) & IP Connected Devices

And all the above poses a security NIGHTMARE

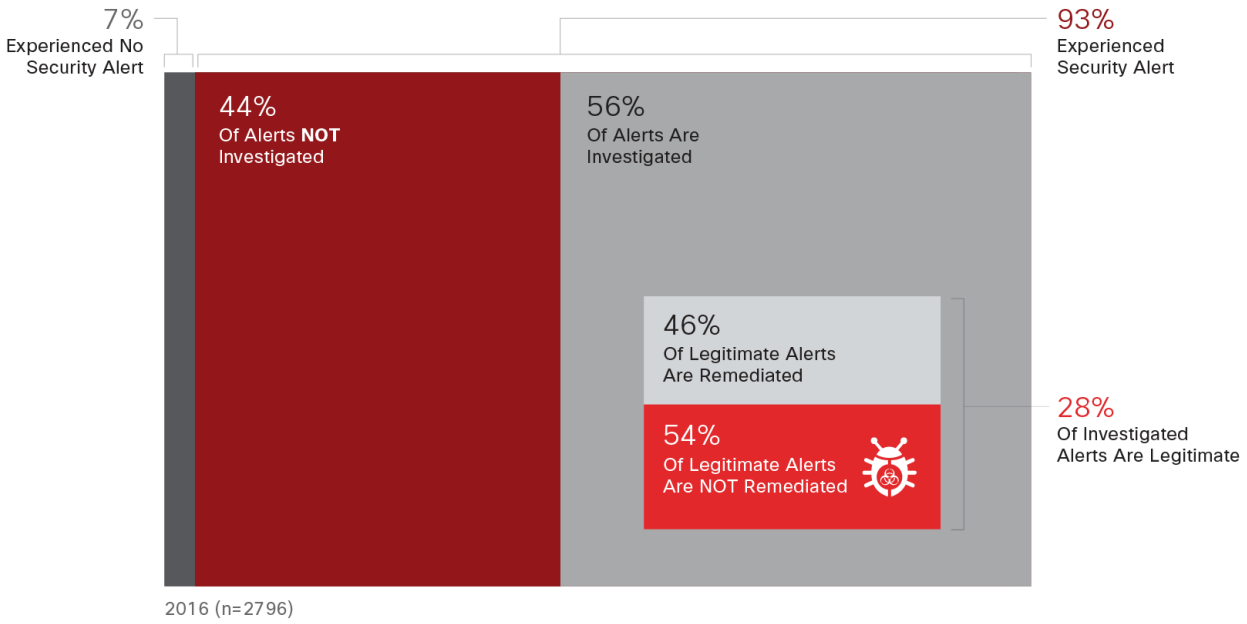


Cyber Security REALITIES

Biggest **sources** of concern for security professionals related to cyber attacks

Mobile Devices	Data in Public Cloud	Cloud Infrastructure	User Behavior (For Example, Clicking Malicious Links in Email or Websites)
58%	57%	57%	57%

Percentage of security alerts that are **NOT** **investigated or remediated**



Thousands of alerts are encountered daily but **fewer than half** are remediated

Healthcare Organizations Encounter Thousands of Daily Security Alerts

50% Investigated Alerts

31% Legitimate Threats

48% Remediated

ORGANIZATIONAL CYBER SECURITY DILEMMA

Cyber Security OBSTACLES

#1 Lack of skilled personnel — **45%**

#2 Lack of budget — **45%**

#3 Low security awareness among employees — **40%**

#4 Lack of collaboration between departments — **32%**

- 31% Lack of management support/awareness
- 29% Poor integration/ interoperability between security solutions
- 24% Too much data to analyze
- 18% Lack of contextual information from security tools
- 18% Inability to justify additional investment
- 9% Lack of effective solutions available in the market

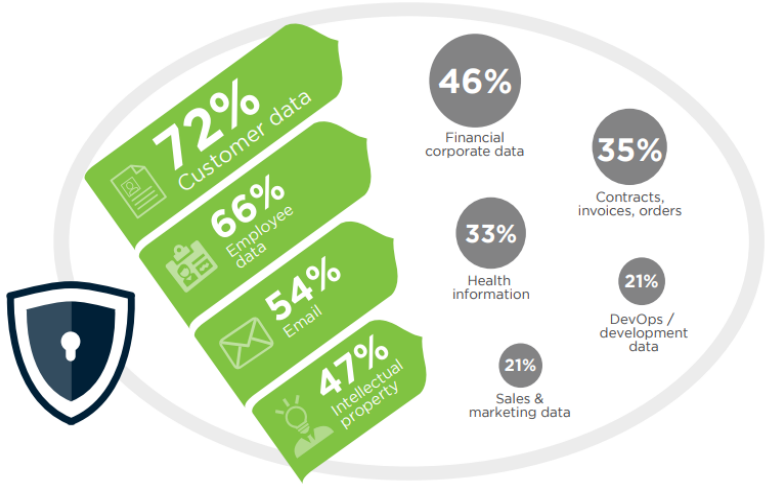
35% report ransomware in the cloud, particularly within the following popular SaaS applications: Dropbox, Office 365 and Google Apps.

- 70% Dropbox
- 29% Office 365
- 12% Google Apps
- 6% box
- 3% salesforce

70% Detection of advanced threats (hidden, unknown, and emerging)

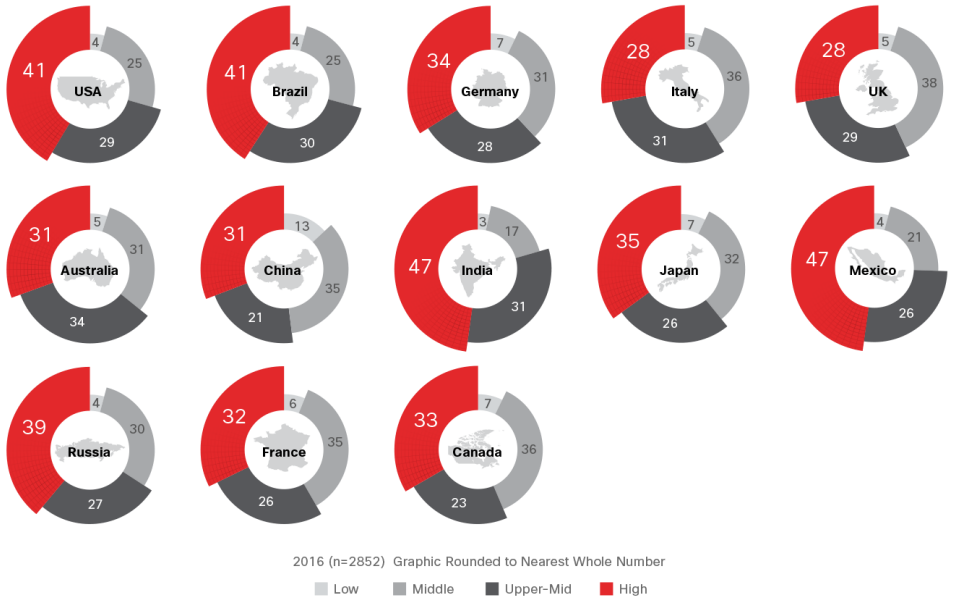
59% The lack of expert security staff to assist with threat mitigation

- 49% Detection of rogue insiders/ insider attacks
- 49% Slow response time to find or detect advanced threats
- 47% Too much time wasted on false positive alerts
- 45% Lack of confidence in automation tools catching all threats
- 32% Lack of proper reporting tools

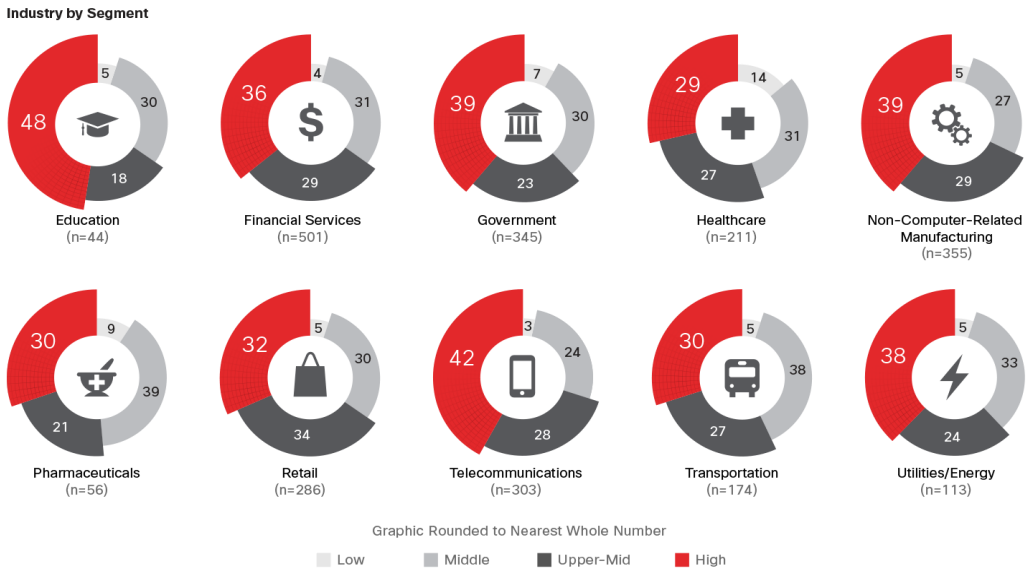


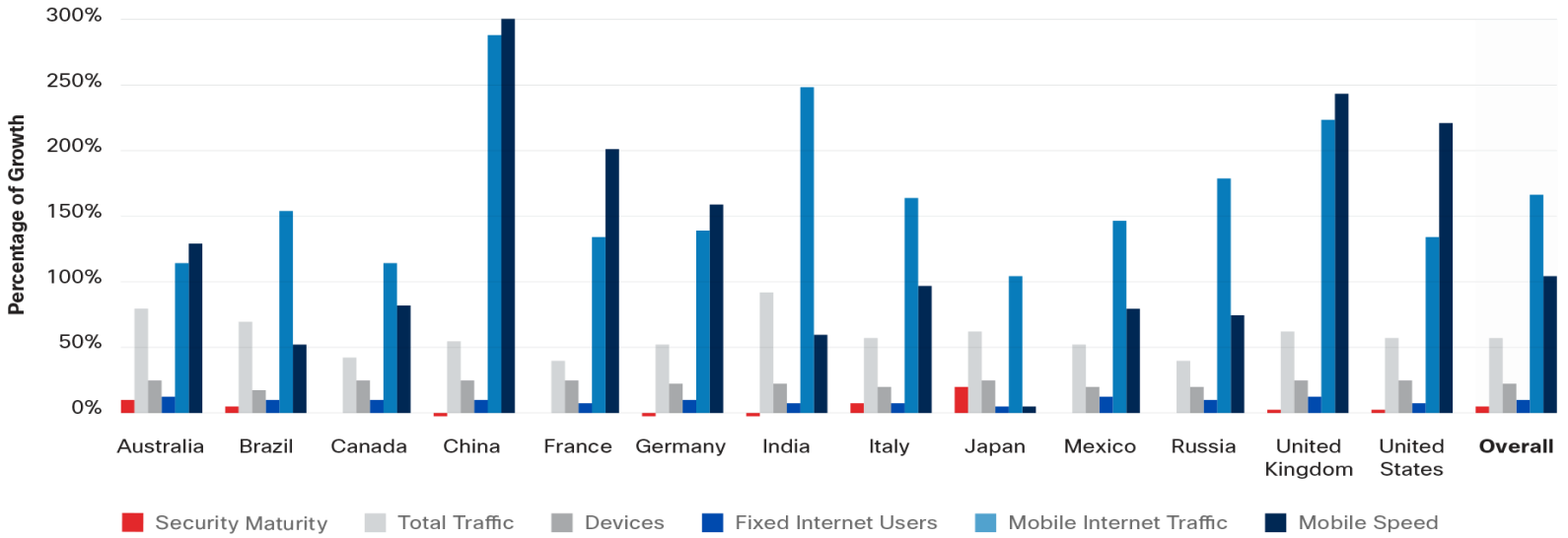
Cyber Security MATURITY

Security maturity by **Country**



Security maturity by **Industry Verticals**





Security Maturity & Growth Rates

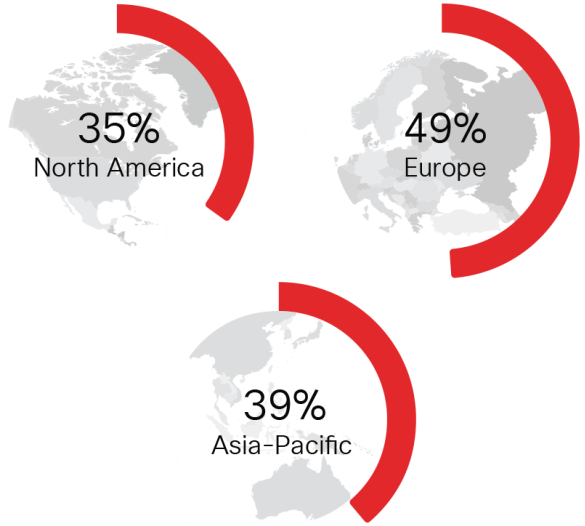
Hint: Observe the Security **Maturity & Capability** bar in red color !

SECURITY plus CLOUD

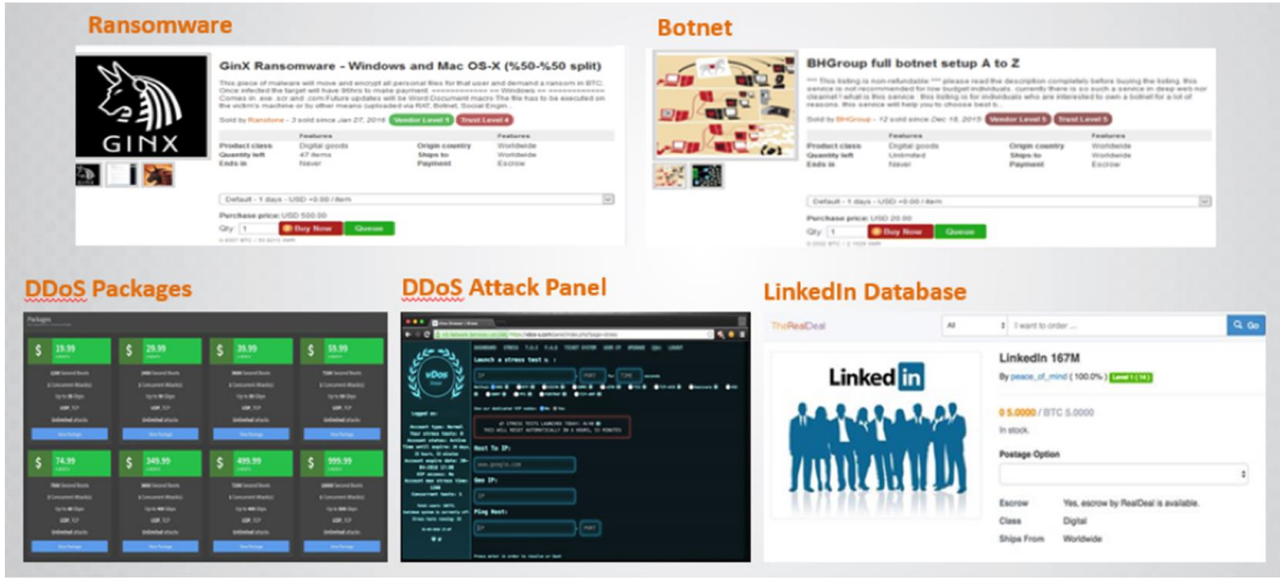
WWW.SECURITYPLUSCLOUD.COM.AU

Cyber Security RANSOMWARE

Distribution of ransomware attacks by region in **2016** alone.



Examples of Cyber Attack **Automated Tools, Packages & Ransomware As A Service.**



Percentage of organizations that dealt with **consequences** of data breaches.

54%
dealt with public scrutiny due to data breaches

32%
lost revenue due to attacks in the past year

25%
lost customers or business opportunities due to attacks

Organizational **functions** affected by a public breach.

VERIZON DATA BREACH INVESTIGATIONS REPORT

Cyber Security
CRIME SNAPSHOT

For the **TENTH time**, Verizon brings together the collective experience of **65 Organizations** to give you the full picture on cybercrime.

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

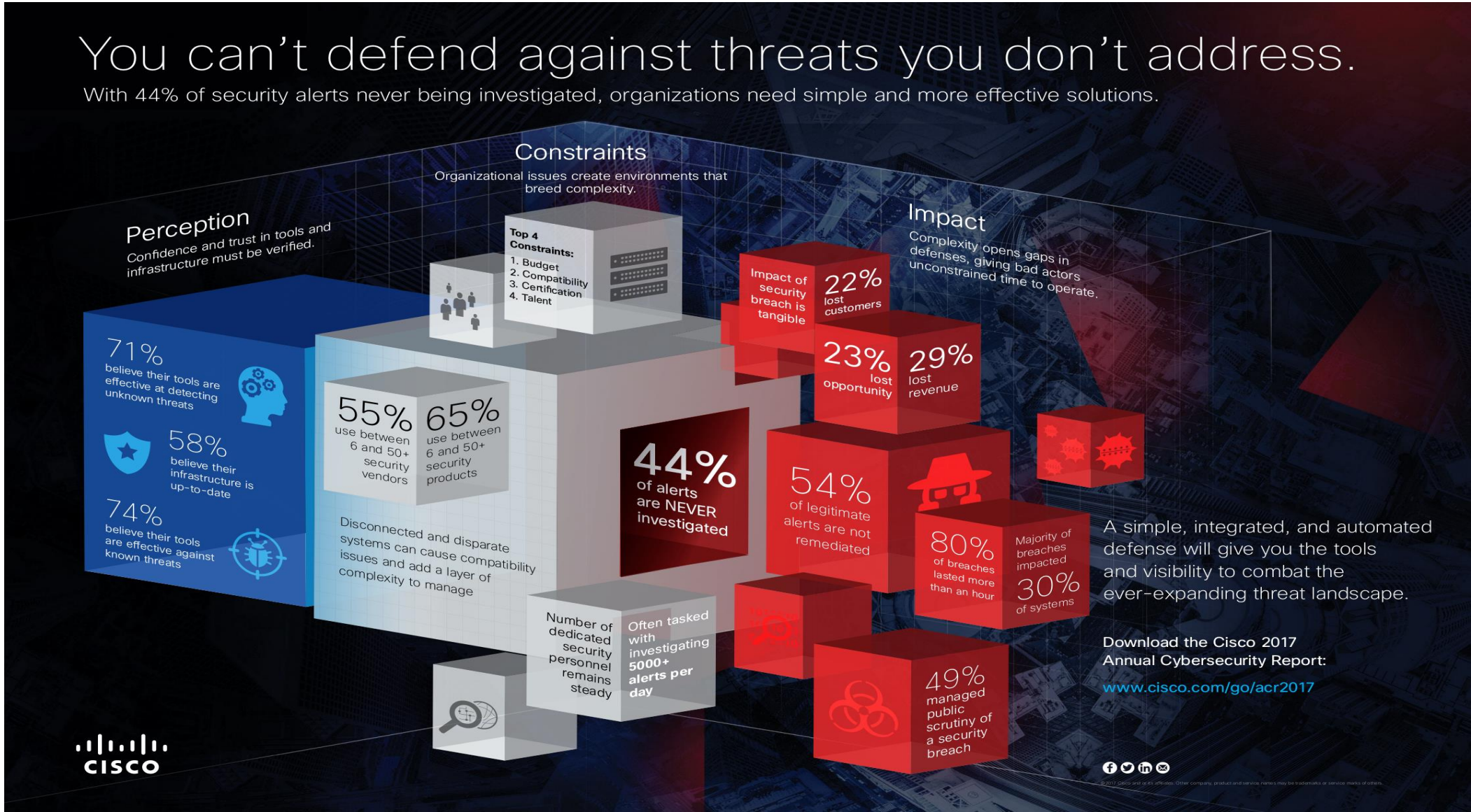
73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

CISCO'S 2017 ANNUAL SECURITY REPORT

Cyber Security SUMMARY



SOLUTIONS BY SPC

100+ CYBER SECURITY SOLUTIONS BY SPC

MANAGED ENDPOINT SECURITY

- Endpoint Protection
- Endpoint Device Control
- Endpoint Data Loss Prevention
- Endpoint Privilege Escalation
- Endpoint Encryption
- Endpoint Malware Sandboxing
- Endpoint Vulnerability Assessment
- Endpoint Machine Learning
- Endpoint Detection and Response
- Database Security Solutions
- User and Entity Behavior Analytics
- Mobile Device Management
- Ransomware Protection
- Container & Docker Security

MANAGED NETWORK SECURITY

- Network Firewall
- Network Intrusion Prevention Systems
- Network Web Gateway Security
- Network Data Loss Prevention
- Network Malware Sandboxing
- Network DDOS Protection
- Network Monitoring Solutions
- Network Vulnerability Assessment
- Network Web Application Firewall
- Network Behavior Anomaly Detection

MANAGED CLOUD SECURITY

- Cloud DDOS Protection
- Cloud Shadow IT Security Solutions
- Cloud Vulnerability Assessment
- Cloud Data Encryption
- Cloud Secure Access Control
- Cloud Access Security Brokers
- Amazon Web Services Security
- Google Apps for Business Security
- Microsoft Office 365 Security
- Microsoft Azure Security

CYBER SECURITY BY AUSTRALIAN SIGNALS DIRECTORATE

- Top 4 Cyber Intrusion Mitigation Strategy by ASD
- Essential Eight by ASD
- Top 35 Mitigation Strategies by ASD
- Information Security Manual by ASD
- Cloud Computing Security Considerations by ASD
- Cyber Security for Contractors by ASD

HACKING

- Red Teaming Penetration Testing
- Blue Teaming Penetration Testing
- Air Gap Systems Penetration Testing
- External Penetration Testing
- Internal Penetration Testing
- Web Application Penetration Testing

GOVERNANCE RISK COMPLIANCE

- ISO 27001
- Security Auditing
- PCI DSS Compliance
- APRA 234 Assessment
- Cyber Risk Quantification
- COBIT 5 Information Security
- COBIT 5 for Risk
- NIST Cybersecurity Framework
- Cyber Security Insurance Consulting
- General Data Protection Regulation (GDPR)
- Cybersecurity Capability Maturity Model C2M2

COUNTER CYBER TERRORISM

- Engineering Cyber Counter Terrorism Centre
- Secure Communications Solutions
- Cyber Intelligence & CCT for Enterprise
- Cyber Intelligence & CCT for Government
- Cyber Intelligence & CCT for Financial Markets
- Cyber Intelligence & CCT for Critical Infrastructure
- Cyber Warfare Room Establishment & Support
- Digital Human Intelligence Development

CYBER SECURITY TRAINING

- Incident Handling and Response
- Security Operations Centre Management
- Enterprise Threat Vulnerability Assessment
- Understanding Hacker Tools Techniques Exploits
- Cloud Security Fundamentals
- Security Information Event Management In Depth
- Cyber Threat Intelligence

SCADA SECURITY

- SCADA Application Whitelisting
- SCADA Configuration and Patch Management
- SCADA Attack Surface Management
- SCADA Defendable Environment Management
- SCADA Managed Authentication
- SCADA Secure Remote Access
- SCADA Monitoring and Response Management
- SCADA Penetration Testing
- SCADA SANS 20 Critical Security Controls
- SCADA NIST 800-82 r2
- SCADA ANSI ISA 62443
- SCADA Cybersecurity Capability Maturity Model C2M2
- SCADA Belden 1-2-3 ICS Security
- SCADA SOC Security Operations Centre

MANAGED SECURITY OPERATIONS CENTRE (SOC)

- SOC In A Box
- Cyber Security Audits for SOC
- Cyber Security Health Checks for SOC
- Cyber Security Advisory Services for SOC
- Managed Security Information Event Management
- Managed Incident Response Security Monitoring
- Managed Threat Hunting Detection Response
- Managed SOC Secure Communications
- Virtual SOC
- Co-Managed SOC
- Dedicated SOC
- Cloud SOC
- Command SOC
- Build, Operate, Manage or Transfer (BOM/T) SOC

EVERY INDUSTRY COVERED BY SPC

Cyber Security Solutions For All

INDUSTRIES

AIRLINES
DEFENCE
EDUCATION
FINANCE & INSURANCE
MEDIA
MINING
REAL ESTATE
HOSPITALITY
TRANSPORT
MANUFACTURERS
HEALTHCARE
RETAIL & WHOLESALE
FOOD & AGRICULTURE
GOVERNMENT
HIGH NET WORTH
TELECOMMUNICATION
UTILITIES & ENERGY
LEGAL

COMPREHENSIVE TECHNICAL SUPPORT LEVELS

SecurityPlusCloud Cyber Security SUPPORT

Cost of premium support levels vary from $250K to $1M Annually for the most critical & dedicated cyber security operations.

BLACK Level
Ultimate support level offers Titanium + dedicated team at customer site, SOC visits & incubation.

TITANIUM Level
Premium support level offers Diamond + dedicated Cyber Security Analyst at customer site.

DIAMOND Level
Premium support level offers Platinum + access to Executive Management & RSA Conferences.

PLATINUM Level
Premium support level offers dedicated remote Cyber Security Analyst & immediate answer.

GOLD Level
Standard support service part of every solution under SpC.

For more information, click here

Advanced Cyber Threat Intelligence - Force ACTI-F

ADVANCED CYBER THREAT INTELLIGENCE - FORCE

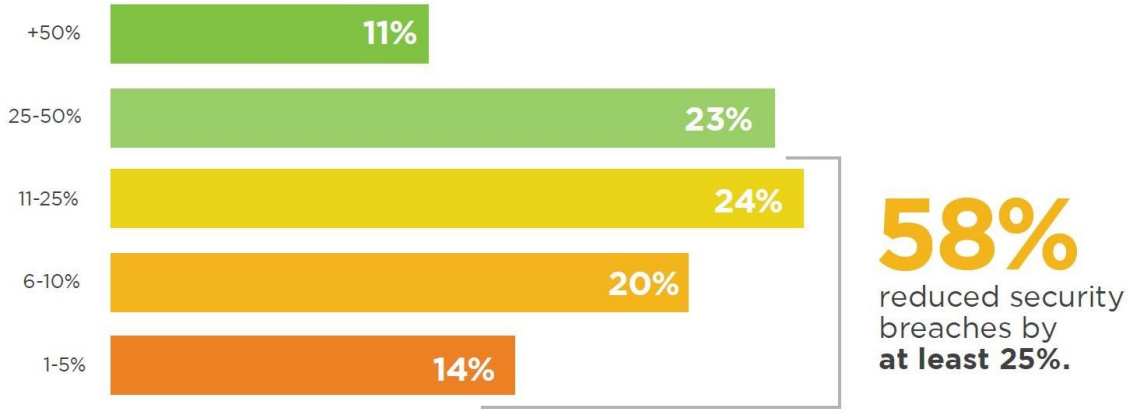
One of the biggest security challenges is the prevention of an impending attack instead of recovery. **ACTI-F** plans to achieve just that.

ACTI-F (*Advanced Cyber Threat Intelligence – Force*) redefines cyber threat intelligence where a single security vendor largely relies on data provided by their software & hardware, SecurityPlusCloud's ACTI-F **passively gathers threat intelligence from log output of virtually all security vendors**' solutions deployed at customer sites.

This data does not just give a holistic view of worldwide threats in **real time** but SecurityPlusCloud will use this data to **develop global cyber threat intelligence system** that will be **leased out to**:

- **Current & Future Cyber Security Vendors**
- **Governments**
- **Enterprises & more**

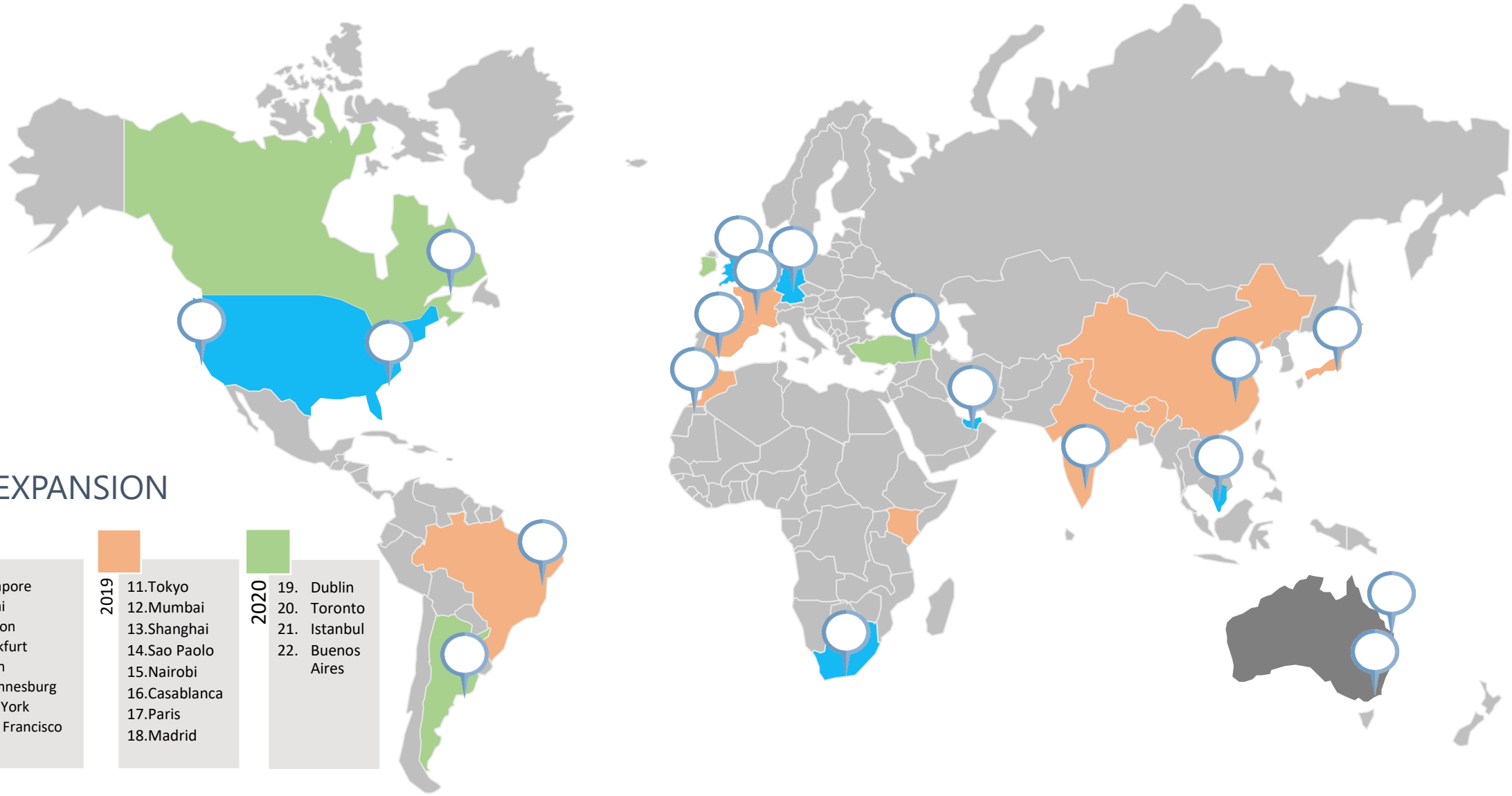
to achieve one sole purpose of finally being not one but **thousand steps** ahead of attackers.



A majority of organizations (58%) estimate they reduced the number of security breaches by atleast 25% by using threat intelligence solutions.

Thirty-four percent reduced breaches by more than 25%.

CREATE SOCs IN 22 CITIES ACROSS 6 CONTINENTS



YEAR BY YEAR EXPANSION

2017
1. Sydney
2. Gold Coast

2018
3. Singapore
4. Dubai
5. London
6. Frankfurt
7. Berlin
8. Johannesburg
9. New York
10. San Francisco

2019
11. Tokyo
12. Mumbai
13. Shanghai
14. Sao Paolo
15. Nairobi
16. Casablanca
17. Paris
18. Madrid

2020
19. Dublin
20. Toronto
21. Istanbul
22. Buenos Aires

TRILLION DOLLAR MARKET

CYBER SECURITY - A TRILLION DOLLAR MARKET

Cyber Security
A TRILLION $ MARKET

$1Trillion: Cybersecurity Global Spend 2017-2021

Published on June 19, 2016

Digital Warfare Just Created a Trillion Dollar Market

OilPrice.com News Commentary

Cyber security set to become $1 trillion market

7th February 2017

ANALYSIS

Cybersecurity spending outlook: $1 trillion from 2017 to 2021

Cybercrime growth is making it difficult for researchers and IT analyst firms to accurately forecast cybersecurity spending.

Smart Money Heading To The $1 Trillion Cybersecurity Sector

Gartner: Worldwide information security spending to hit $93B in 2018; exceed $1 trillion over next five years.

BY GRAHAM.GATES@TECHEXECONLINE.COM · AUGUST 24, 2017

Tech Billionaires Positioning Themselves for $1 Trillion Cybersecurity Boom

By AccessWire, July 10, 2017, 09:00:00 AM EDT

Cybersecurity Ventures projects $1 trillion will be spent globally on cybersecurity from 2017 to 2021.

RESEARCHANDMARKETS
THE WORLD'S LARGEST MARKET RESEARCH STORE

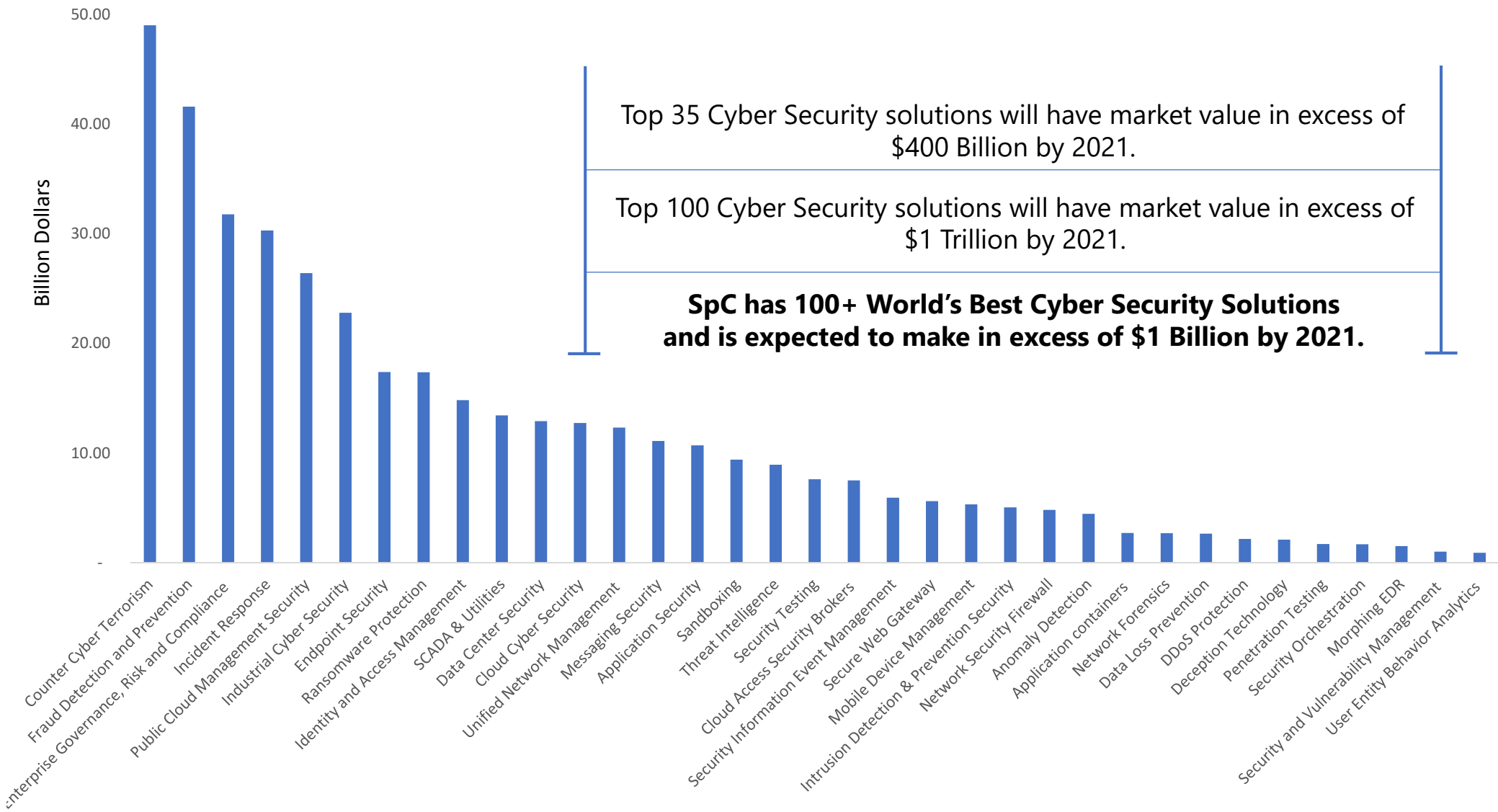
Global $1 Trillion Cybersecurity (Products & Services) Market Outlook and Forecasts 2017 - 2022

Global Cybersecurity Market Outlook and Forecasts 2017 - 2022: Cumulative Enterprise and Governments Spending will Reach Nearly $1 Trillion - Research and Markets

MARKET VALUE BY CYBER SECURITY SOLUTIONS

Cyber Security Solutions

MARKET VALUE



WORLD'S BEST CYBER SECURITY TEAM

FOUNDERS OF SECURITYPLUSCLOUD

World Class Cyber Security Team

FOUNDERS

HARRY Asghar.
CEO & Co-Founder

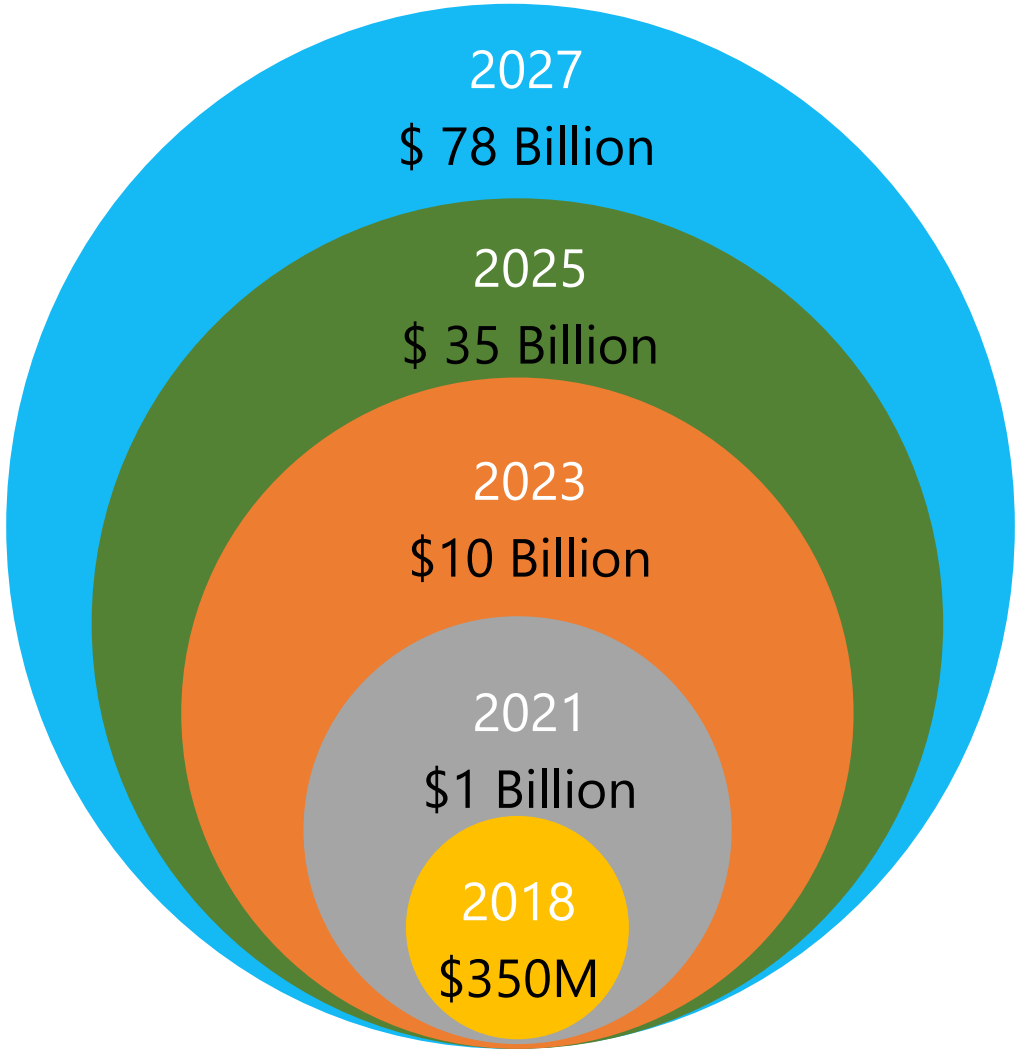
FRANK Kahn.
CTO & Co-Founder

10 YEAR HYPER GROWTH STRATEGY & ROADMAP OF SPC

SecurityPlusCloud GROWTH STRATEGY

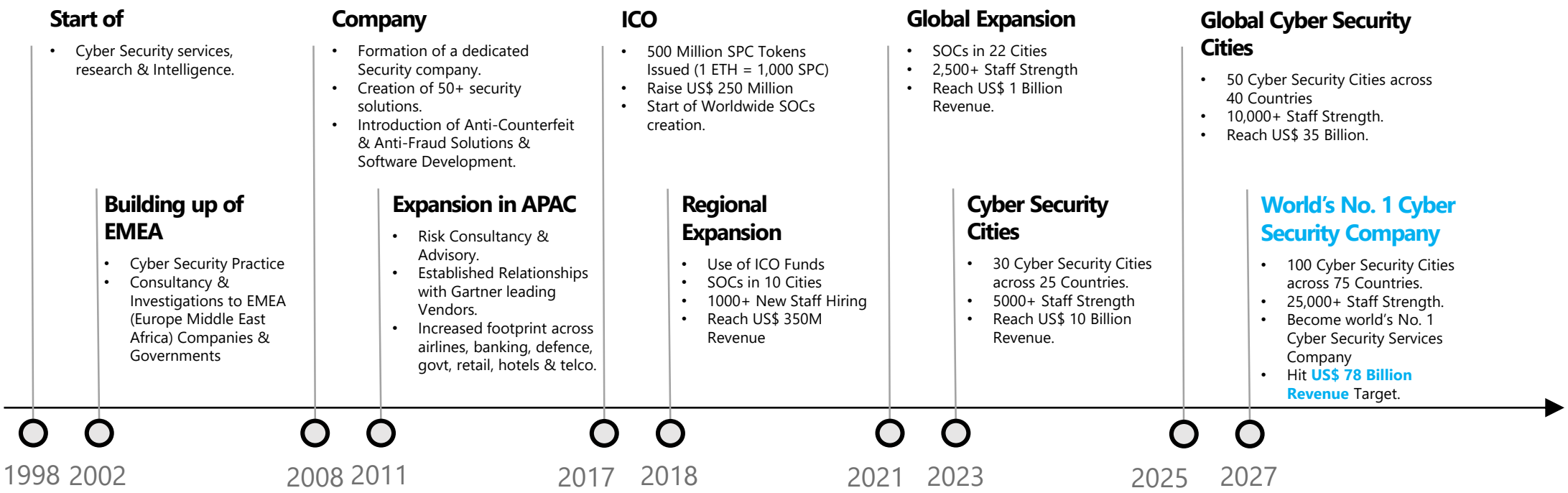
10 Year Hyper Growth Strategy & Roadmap

Year 2018 Growth 150 % **Revenue $350 Million**	**Regional Cyber Security Expansion**	• 10 Cities to have Cyber Security Operation Centers (SOCs) • 1,000+ Hiring of Cyber Security Experts & Security Sales Staff
Year 2021 Growth 70 % **Revenue $1 Billion**	**Global Cyber Security Expansion**	• 22 Cities to have Cyber Security Operation Centers (SOCs) • 2,500+ Hiring of Cyber Security Experts & Security Sales Staff
Year 2023 Growth 200 % **Revenue $10 Billion**	**Worldwide Cyber Security Cities**	• 30 Cyber Security Cities established across 25 countries • 5,000+ Hiring of Cyber Security Experts & Security Sales Staff
Year 2025 Growth 80 % **Revenue $35 Billion**	**Global Cyber Security Cities & SOC Expansion**	• 50 Cyber Security Cities established across 40 countries • 10,000+ Hiring of Cyber Security Experts & Security Sales Staff
Year 2027 Growth 25 % **Revenue $78 Billion**	**World's No. 1 Cyber Security Company**	• 100 Cyber Security Cities established across 75 countries • 25,000+ Hiring of Cyber Security Experts & Security Sales Staff



ROADMAP TO 2027

SecurityPlusCloud ROADMAP



ICO FUNDRAISER

SecurityPlusCloud
ICO FUNDRAISER

SecurityPlusCloud - SPC

Will launch world's first cyber security services ICO Pre-sale on 1st November 2017. It will recommend a token allocation based on contributions in Ethers and bitcoins (subject to legal terms & conditions) and these SPC tokens can be used as a payment method for SPC's cyber security services & can be traded on exchanges.

ICO Pre-Sale Launch on 1st November 2017

Accepting Ethers & Bitcoins

www.securitypluscloud.com.au/tokensale

US & Canadian customers are not allowed to participate in SPC ICO.

SecurityPlusCloud

SPC TOKENS UTILISATION

Three Main Benefits of **SPC** Tokens

SecurityPlusCloud
SPC TOKENS UTILISATION

SPC tokens as a payment method for Cyber Security Solution

Post successful completion of ICO Main sale, SPC Tokens can also be used as a payment method to purchase SecurityPlusCloud's 100+ Cyber Security Solutions.

SPC
TOKENS

- MANAGED ENDPOINT SECURITY
- MANAGED NETWORK SECURITY
- GOVERNANCE RISK COMPLIANCE
- COUNTER CYBER TERRORISM
- MANAGED CLOUD SECURITY
- CYBER SECURITY BY AUSTRALIAN SIGNALS DIRECTORATE
- CYBER SECURITY TRAINING
- SCADA SECURITY
- HACKING
- MANAGED SECURITY OPERATIONS CENTRE (SOC)

SecurityPlusCloud ICO PRE-SALE BONUS

PRE-SALE DETAILS

SPC pre-sale begins on 1st November 2017 and will run for 12 days or until all assigned tokens are sold out.

Bonus Percentage: 50%

Maximum for sale pre-ICO	50,000,000 SPC
Pre-ICO price in ETH	1 ETH = 1,000 SPC*
Pre-ICO price in Bitcoin	1 Bitcoin = 20,000 SPC*
Minimum ETH transaction amount	0.1 ETH
Pre-ICO sale period	12 Days starting 1st November 2017
Coin distribution	Contract will distribute coins/tokens instantly to your Ethereum wallet upon for Bitcoins or Ethers.
Bonus Rate	**50%**

* SPC Token distribution rate has been increased for Main Sale in lieu of substantial increase in ETH & BTC US$ values.

SecurityPlusCloud

ICO MAIN SALE

MAIN ICO SALE DETAILS & BONUS PERCENTAGE

SPC main sale begins on 22nd November 2017 and will run for 45 days or until all assigned tokens are sold out. Our ICO structure will perform an immediate exchange of SPCs from your contributed Ethers & Bitcoins.

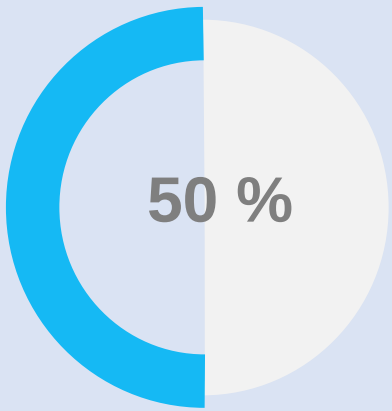
	Main ICO Sale Lot 1	Main ICO Sale Lot 2	Main ICO Sale Lot 3
Maximum for sale main ICO	100,000,000 SPC	75,000,000 SPC	25,000,000 SPC
Pre-ICO price in ETH	1 ETH = 1,000 SPC*		
Pre-ICO price in Bitcoin	1 Bitcoin = 20,000 SPC*		
Minimum transaction amount	0.1 ETH		
Main ICO sale period	45 Days starting 22nd November 2017.		
Coin distribution	Contract will distribute coins/tokens to your Ethereum wallet upon receiving Bitcoins or Ethers.		
Bonus Rate	**30%**	**10%**	**0%**

* SPC Token distribution rate has been increased for Main Sale in lieu of substantial increase in ETH & BTC US$ values.

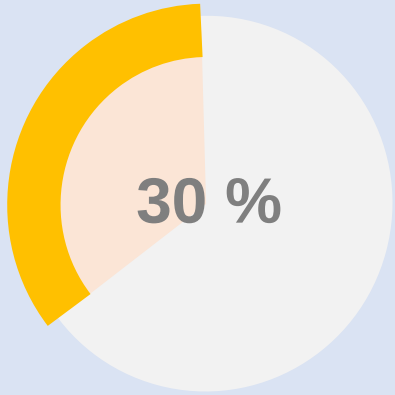
SecurityPlusCloud

ICO BONUS PERCENTAGE

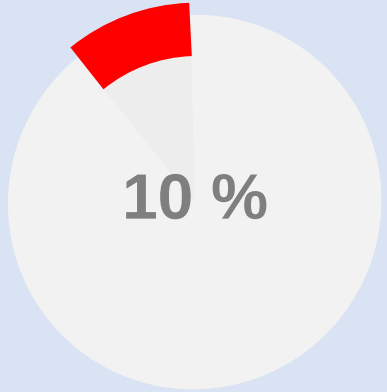
PRE-SALE & MAIN ICO SALE BONUS RATES



Pre-Sale Bonus %



Lot 1 Main Sale Bonus %

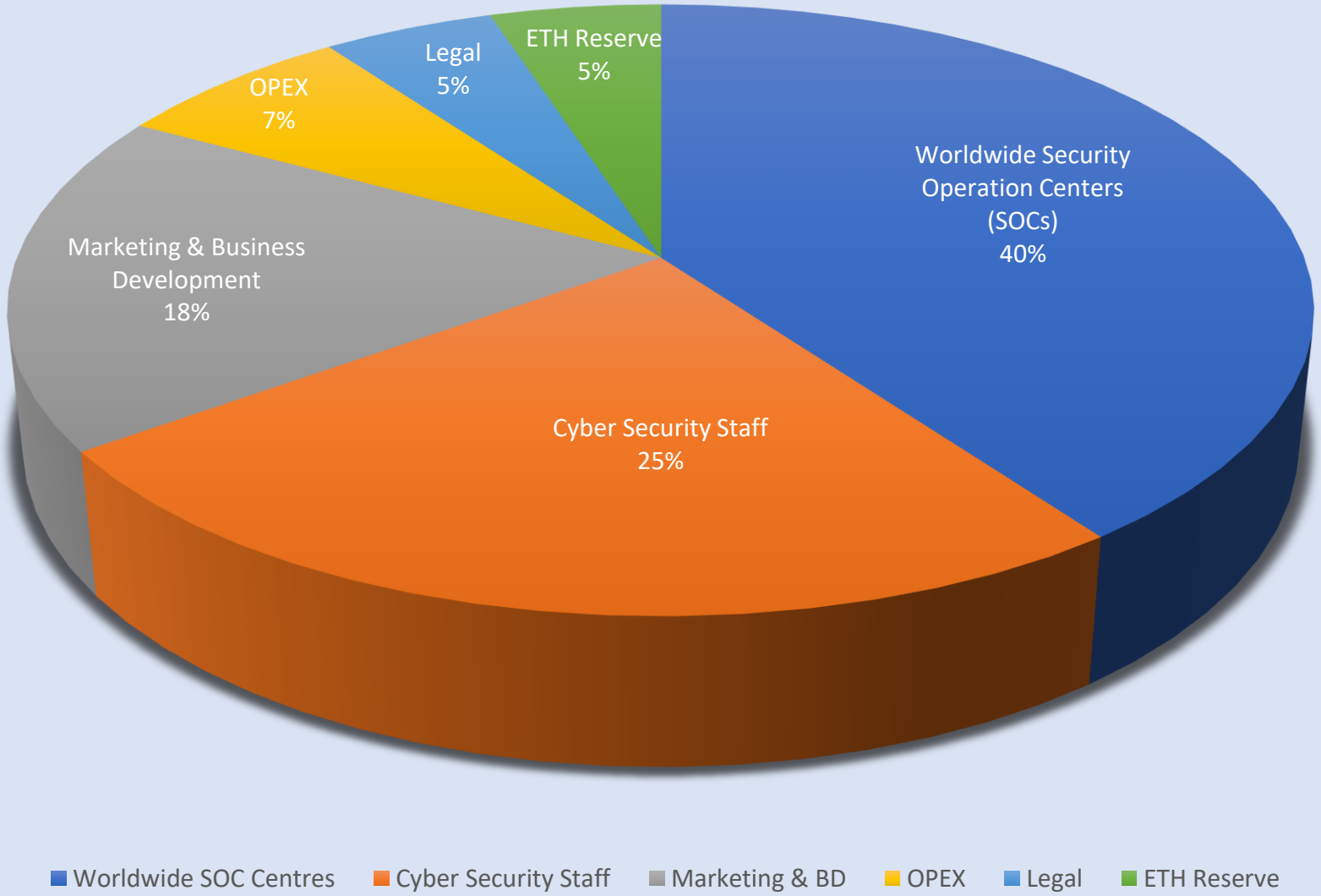


Lot 2 Main Sale Bonus %

Lot 3 Main Sale Bonus %

SecurityPlusCloud
SPEND SPECTRUM

WHERE DO WE SPEND



SecurityPlusCloud

ICO IS GENUINE

SPC ICO IS GENUINE

- ✓ Founders With 20+ Years of International Cyber Security Experience.
- ✓ Real & Existing Customer relationships with leading brands & government agencies.
- ✓ 100+ real solutions – More than any technology & cyber security vendor in the **World**.
- ✓ 10 Years solid growth strategy across 100 cities, 75 countries and revenue forecasted at $78 Billion.
- ✓ Cyber Attacks are a bigger threat to humanity than nuclear weapons (*Warren Buffett).*
- ✓ Cyber Security is a necessity, not a 'good to have'.
- ✓ **Not a science fiction like most other ICOs.**

Smart investors are now capitalizing on the fight against the growing wave of cyber crime.

In 2004, the global cybersecurity market was valued at $3.5 billion. By 2015, that figure had risen to $78 billion, and it's projected to soar to $120 billion or even as high as $175 billion by the end of 2017.

That’s a 5,000% rise in just 13 Years.

SECURITY plus CLOUD

info@securitypluscloud.com.au

www.securitypluscloud.com.au

TERMS & CONDITIONS

SecurityPlusCloud ICO
TERMS & CONDITIONS

ICO TERMS & CONDITIONS

Participating in SecurityPlusCloud is subject to below terms & conditions. Any form of participation means that you have read, understood and agreed to terms & conditions. If there are any questions, objections or feedback, please get in touch with us on info@securitypluscloud.com.au

SecurityPlusCloud Pty Ltd. Is registered in Marshall Islands.

Click below to open page containing Terms & Conditions document.

https://www.securitypluscloud.com.au/ico-tnc.pdf

US & Canadian customers are not allowed to participate in SPC ICO.

Whitepaper
REFERENCES & CREDITS

REFERENCES & CREDITS

Name	Source
Cybersecurity Ventures (Cybersecurity Market Report)	www.cybersecurityventures.com
Gartner	www.gartner.com
Cisco	www.cisco.com
Verizon	www.verizonenterprise.com
McAfee	www.mcafee.com
Crowd Search Partners	www.crowdresearchpartners.com
MarketandMarkets	www.marketsandmarkets.com
Cision PR Newswire	www.prnewswire.com
Symantec	www.symantec.com
Warren Buffet	Warren Buffet