IBM Security

Secure SD-WAN service offering from IBM Security

Ben Hendrick

Partner & Global Competency Leader
Consulting and Systems Integration
Infrastructure & Endpoint Security

December 12, 2017

IBM Security
IBM Security
SECURE
SD
WAN

Zero Trust Security is the guiding principle made possible by next generation architectures and technologies now available to clients

CURRENT STATE

Perimeter-Centric, Boundaries, and Trusted

FUTURE STATE

Private and Public Cloud, Virtualized, Boundary-less, Software Defined, and Zero Trust

Flat networks

Security infra sprawl

- Security is an enabler for the SDx infrastructure changes
- Enhanced security can be enabled by these SDx changes in the infrastructure

Secure end-to-end fabric

Simplified, agile management

IBM Security will help you in partnership with your infrastructure teams to:

Design and prove
- Build a business case
- Create a macro design

Integrate and test
- Develop a micro design
- Execute an implementation plan

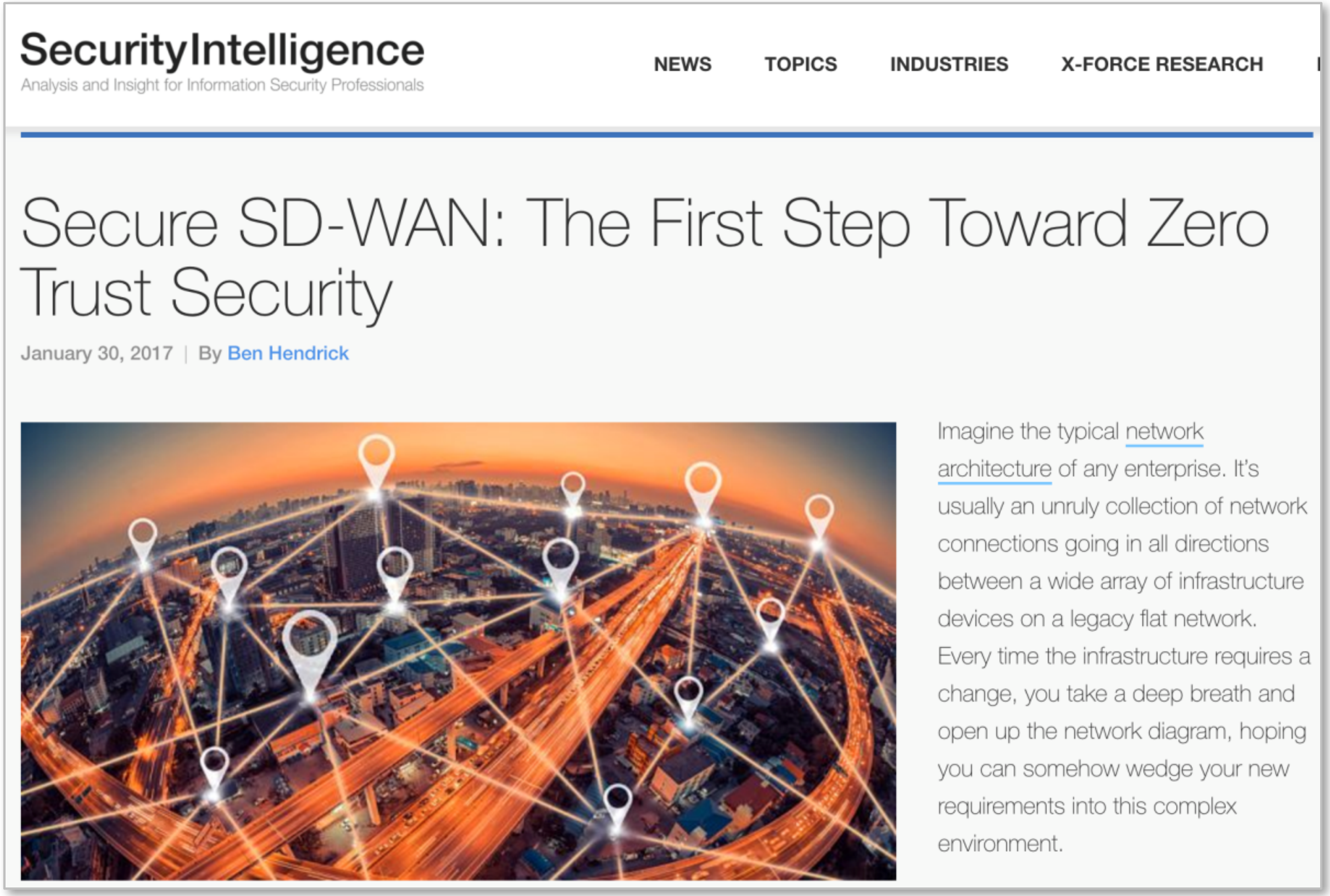
Manage and optimize
- Run a healthy security infrastructure
- Respond to changes

Security

Thought Leadership White Paper

Rein in “box sprawl” with an end-to-end Zero Trust approach to security

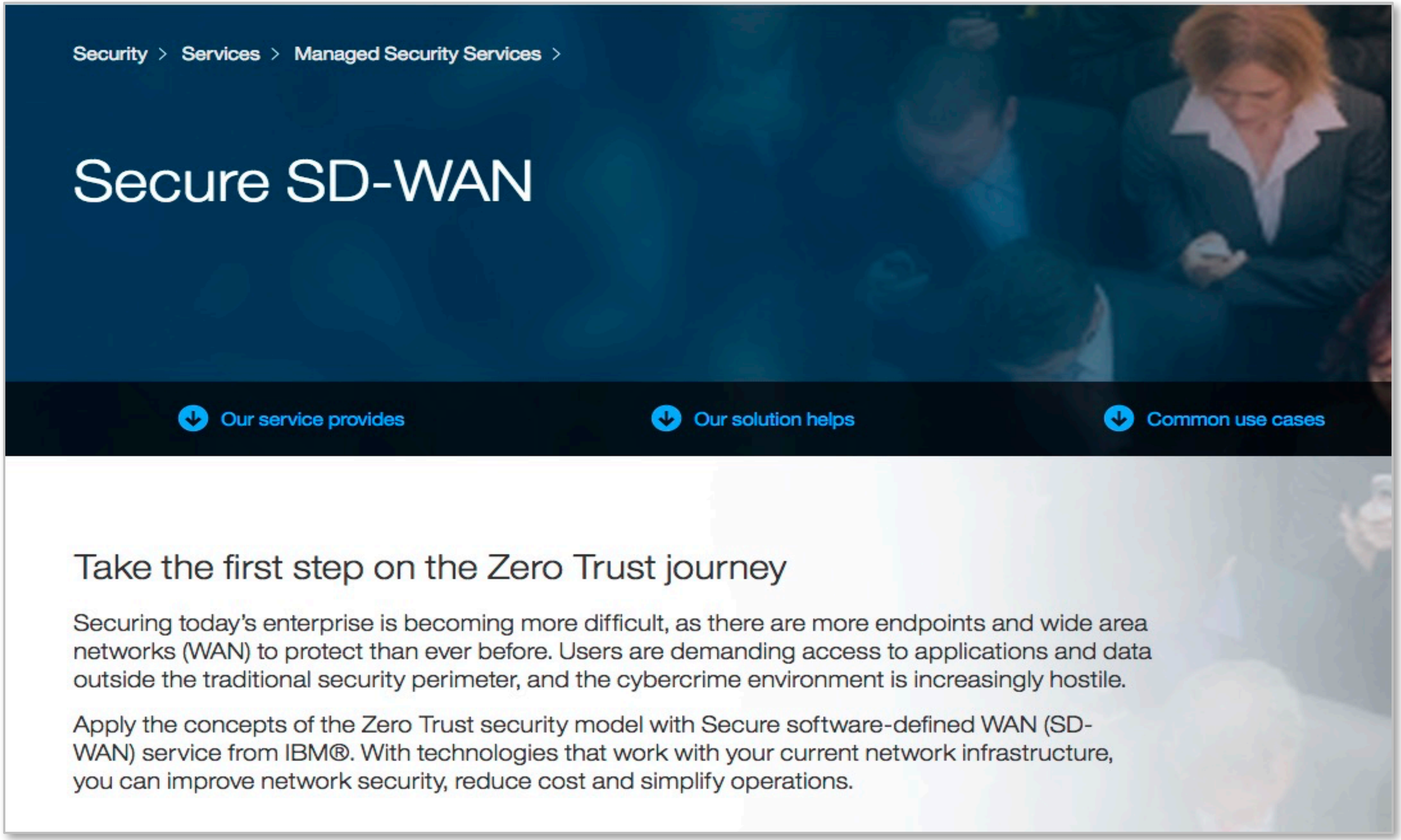
Deploy strong segmentation and encryption to ensure coherent data protection, enterprise-wide



Secure SD-WAN: The First Step Toward Zero Trust Security

January 30, 2017 | By Ben Hendrick

Imagine the typical network architecture of any enterprise. It's usually an unruly collection of network connections going in all directions between a wide array of infrastructure devices on a legacy flat network. Every time the infrastructure requires a change, you take a deep breath and open up the network diagram, hoping you can somehow wedge your new requirements into this complex environment.



Security > Services > Managed Security Services >

Secure SD-WAN

Take the first step on the Zero Trust journey

Securing today's enterprise is becoming more difficult, as there are more endpoints and wide area networks (WAN) to protect than ever before. Users are demanding access to applications and data outside the traditional security perimeter, and the cybercrime environment is increasingly hostile.

Apply the concepts of the Zero Trust security model with Secure software-defined WAN (SD-WAN) service from IBM®. With technologies that work with your current network infrastructure, you can improve network security, reduce cost and simplify operations.

Key links on the new Secure SD-WAN Solution

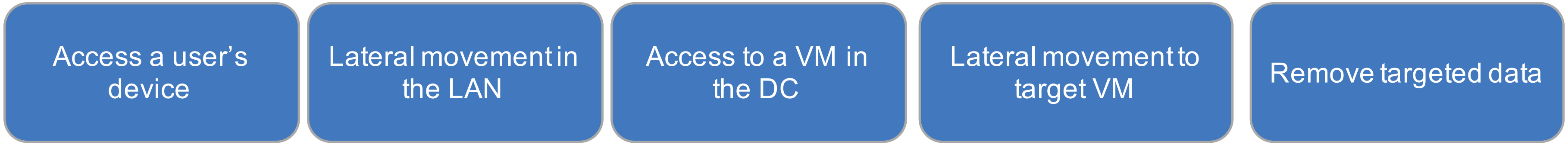
- http://www-03.ibm.com/security/services/managed-security-services/sd-wan/ (Main Public – IBM Portal for Secure SD-WAN)
- https://youtu.be/bUlAAHcM5j4 (John Wheeler – VP) Overview of Infrastructure and Endpoint Security video
- https://youtu.be/BrZWscc_Syk (Ben Hendrick – IES Partner) Overview of Zero Trust Security video
- https://securityintelligence.com/secure-sd-wan-the-first-step-toward-zero-trust-security/ (Ben Hendrick – Global IES Partner Blog)
- https://securityintelligence.com/events/zero-trust-security-for-the-infrastructure-and-endpoint/ (External Webinar)

Zero Trust Security : Effective Segmentation

- ***Breaking the Attack Kill-Chain at Multiple Points***
  - Segmentation using Zero Trust security models
  - Block all known threats
  - Identify and block all unknown threats

Zero Trust Security : no longer trust the user or devices

- Need to start to reduce the trust zone from everyone on the network toward a Zero Trust Architecture
  - Need to migrate from a static security policy based on what is known toward an architecture that focuses on blocking the known and discovering the unknown…to make it known
  - Security feedback loop
  - Need an architecture to deal with the threat of today, not the training of 2+ years ago
- Provide a path to move from what is a known defensive model (previous slide) toward a defensive architecture that is focused on defeating malware and hackers
- Create an architecture that is able to detect a hacker or malware through many different security techniques at every step of an “attack chain”—never stop detecting



Access a user’s device

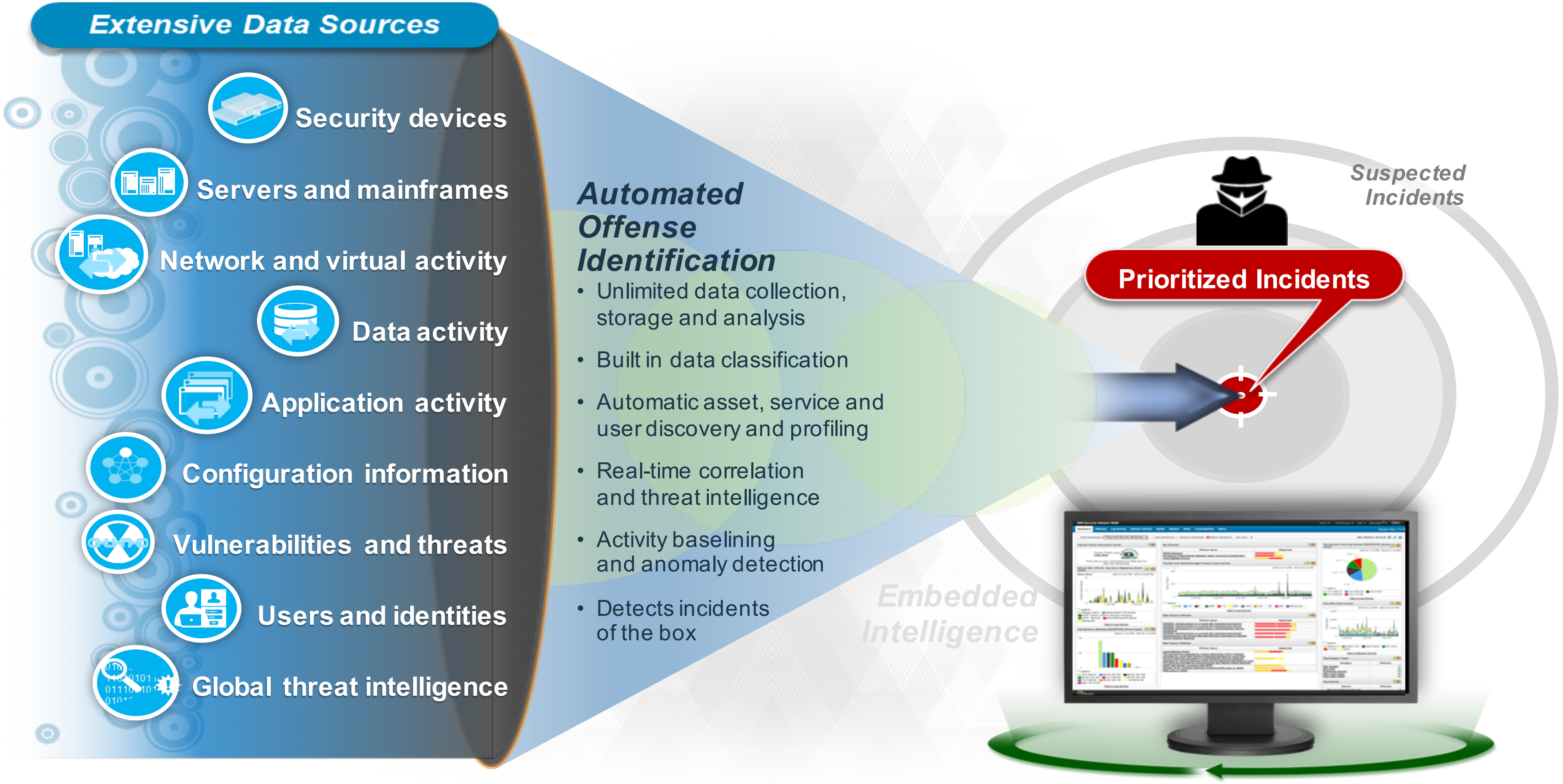
Lateral movement in the LAN

Access to a VM in the DC

Lateral movement to target VM

Remove targeted data

QRadar embedded intelligence offers automated offense identification



Extensive Data Sources

- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence

Automated Offense Identification

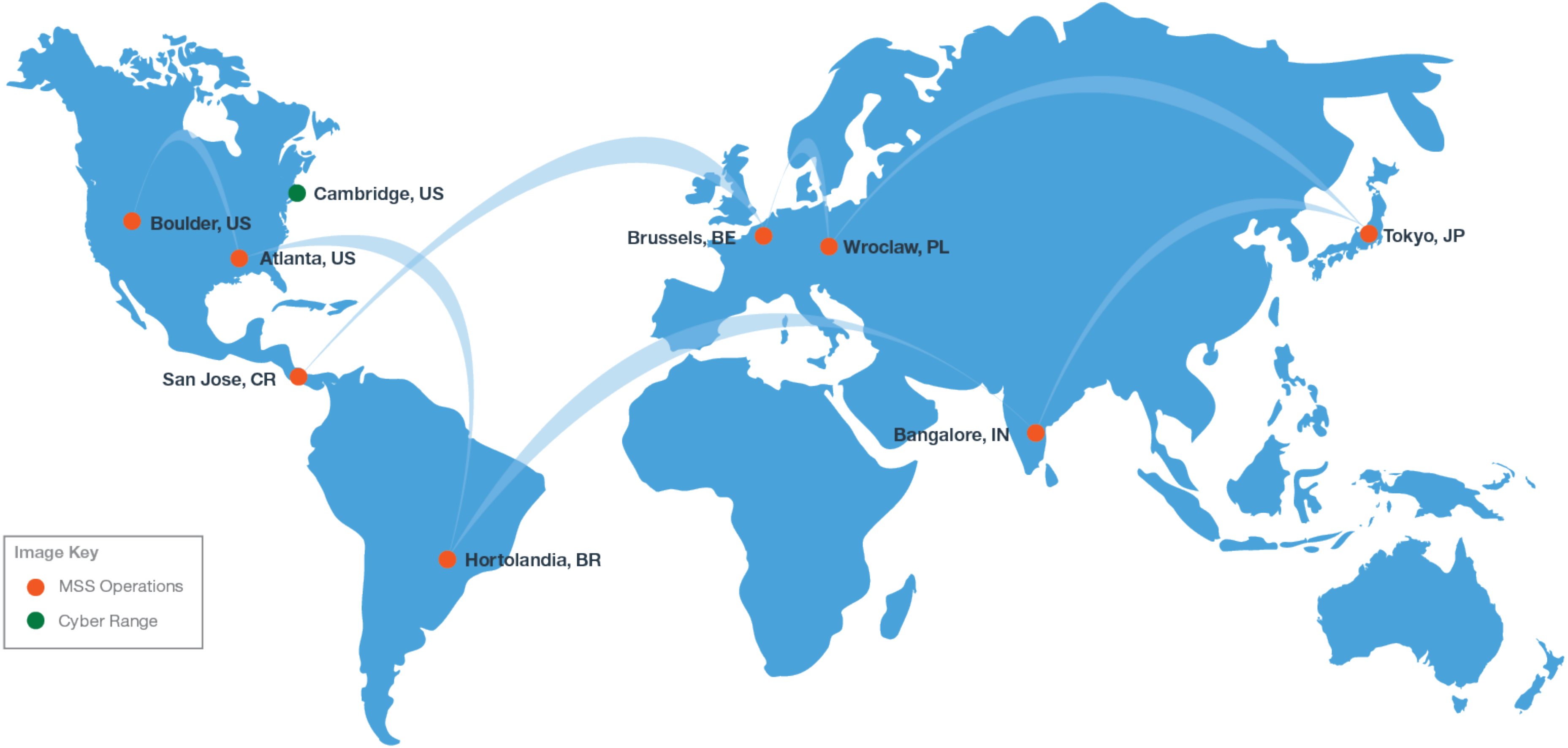
- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

Suspected Incidents

Prioritized Incidents

Embedded Intelligence

IBM Security has global reach with IBM X-Force Command Centers



IBM Security

Secure SD-WAN with Security Hub Technical Review

Ron Howell

Executive Consultant & Senior Architect
Consulting and Systems Integration
Infrastructure & Endpoint Security

December 12 , 2017

IBM

Five questions from your Board

1. Is our program ready to stop the threats of today and tomorrow?

2. We have a lot of tools, but are they providing deep protection?

3. How protected are we as the business adopts Cloud and IoT?

4. How can security reduce friction for employees and customers?

5. How resilient are we in the face of a breach?

Five keys to secure your enterprise that we will address today

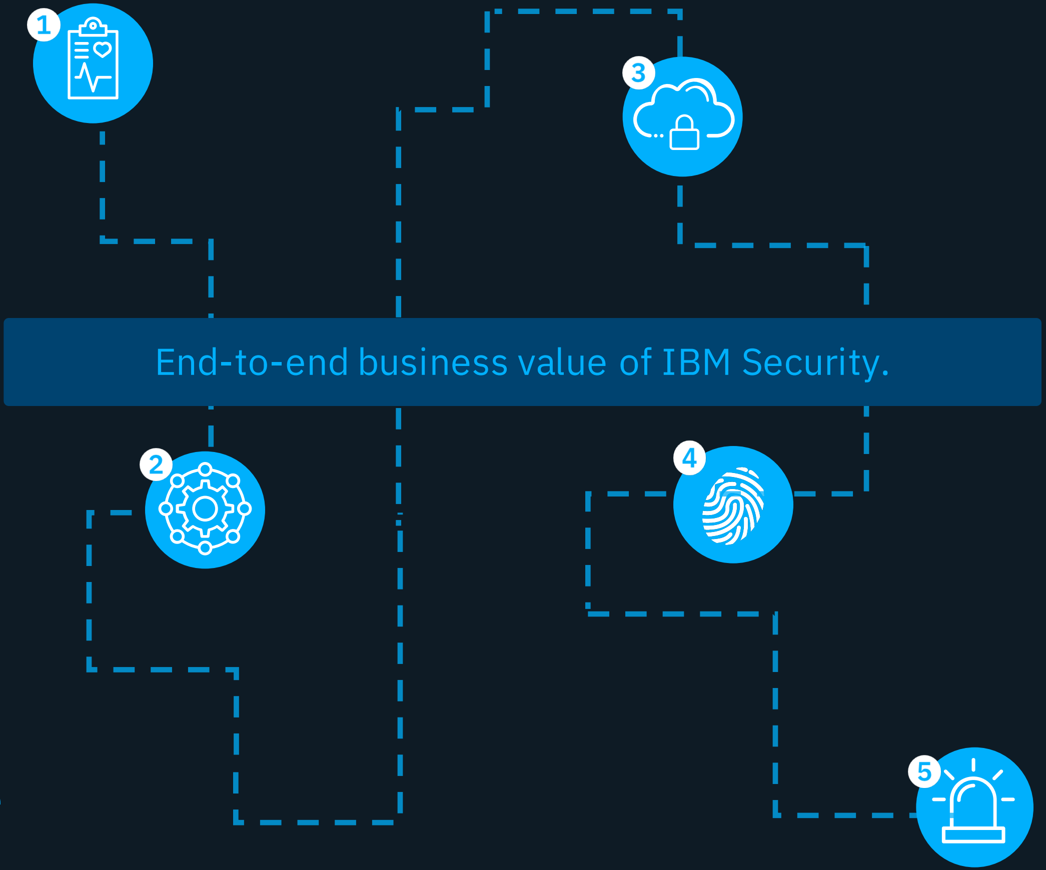
1 **Assessment and Hygiene**
10 Essential Practices™ program and 24x7 experts to plan, design and operate security

2 **Integrated Defenses**
IBM Security Immune System, powered by AI and Watson, detects threats across the business and takes action to protect users, data, applications and infrastructure

3 **Multi-Cloud Security**
We pick up where cloud providers leave off with visibility, identity and data protection purpose-built for clouds

4 **Enable Digital Transformation**
We've combined behavioral analytics from Trusteer with Identity and MaaS360 to deliver delightful and secure user experiences

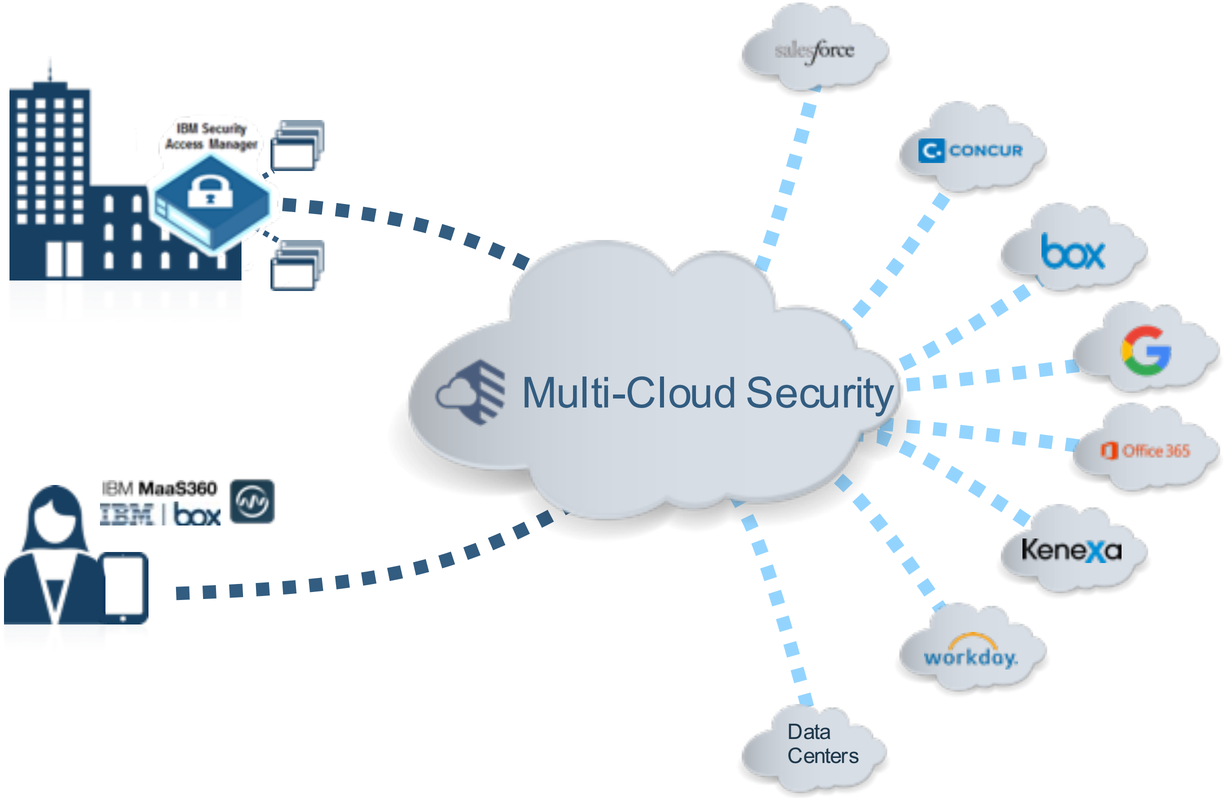
5 **Visibility & Incident Response**
You can't secure what you can't see



Accelerate your digital transformation with Multi-Cloud Security

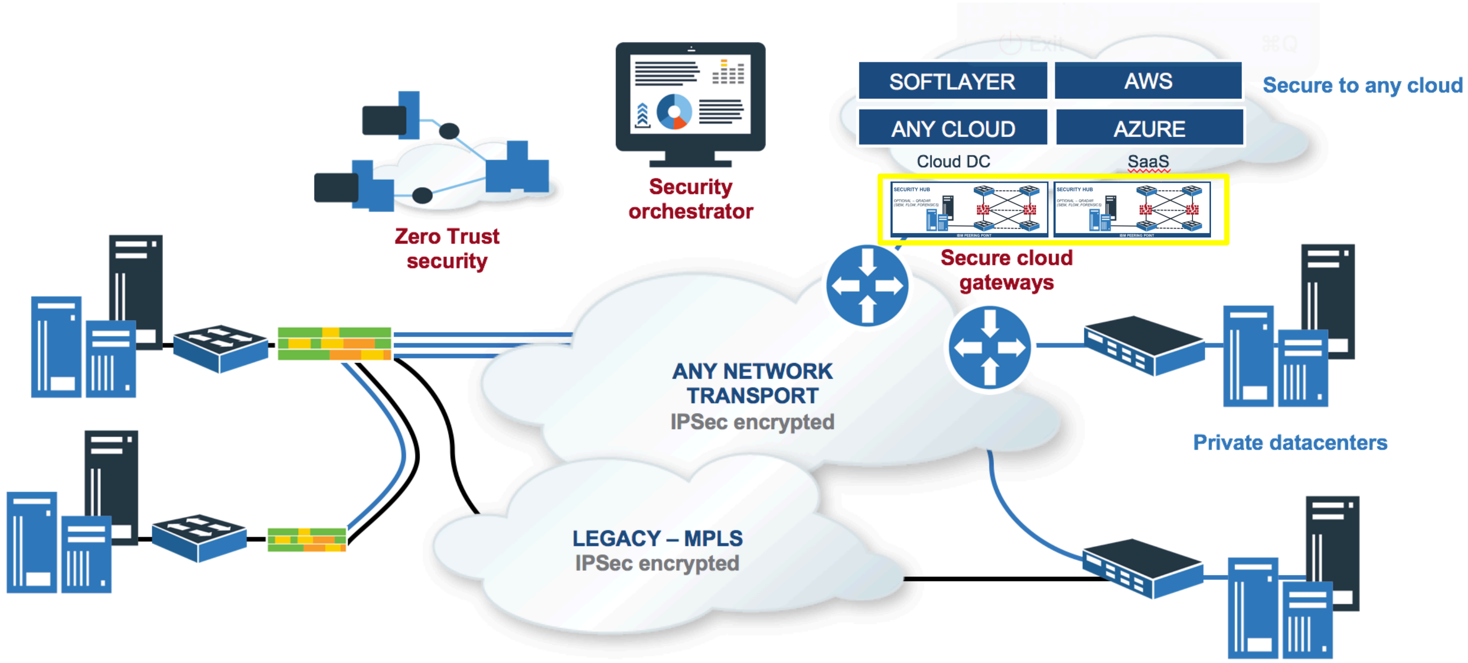
Software Defined Secure Network Services that extend security from any location to any Cloud or Data Center

Multi-Cloud Secure Network Protection that include your Mobile Users and IoT Devices from anywhere they are at any time



IBM MULTI-CLOUD SECURITY SERVICES

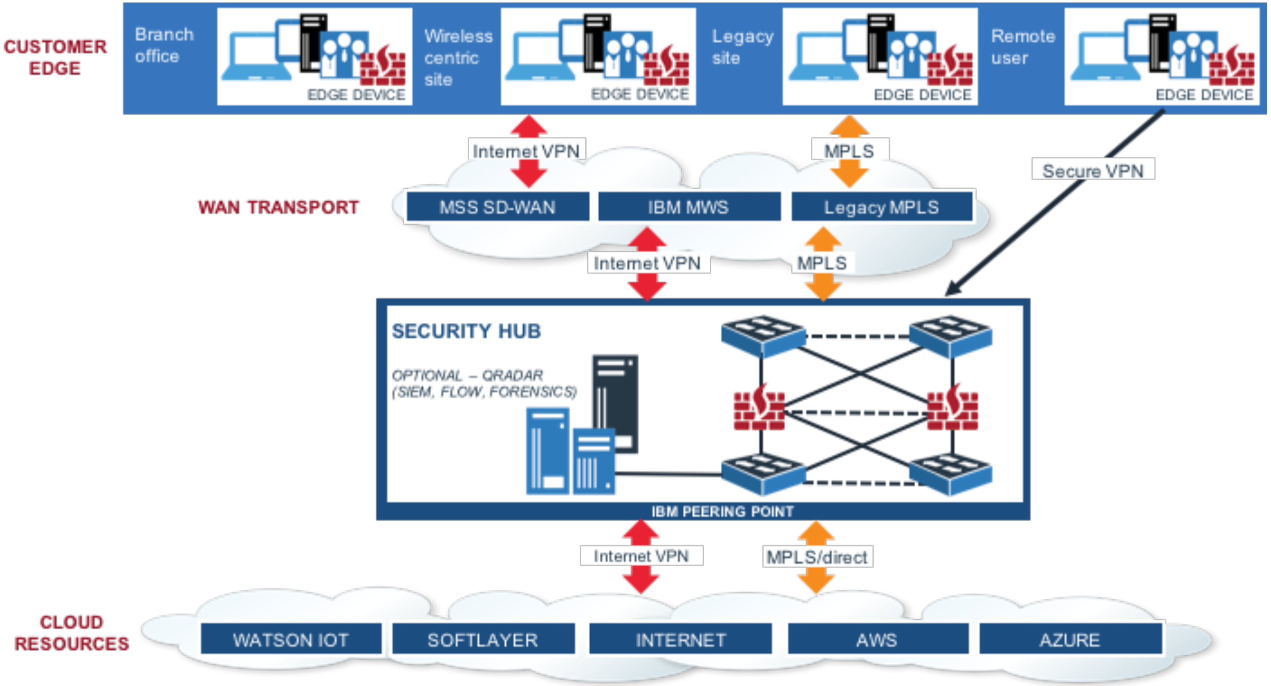
Security SD-WAN : Secure Connectivity over Any Network



- Branch office firewall
- IPSec between branch offices
- Secure Transport Overlay over any type of WAN
- Scalable Cloud VPN for secure connectivity to any destination

- Extensible Network Segmentation to Enterprise datacenter and Cloud
- Integrated Application Firewall for Branch security
- Virtual Services Edge Platform for adding 3rd party Secure VNFs

Security Hub Multi-Cloud Security Protection



Security Features:

- Next Gen firewall
- IPS
- Anti-spam
- URL Filtering
- Malware / AV detection
- Command & control traffic detection
- Geo IP blocking
- SSL VPN
- IPSec
- Dynamic routing (eBGP, iBGP, OSPF)
- QoS
- User FW with machine identification
- SSL forward proxy
- Mobile Security

- Resiliency, high-level of redundancy
- High performance, highly scalable and high throughput

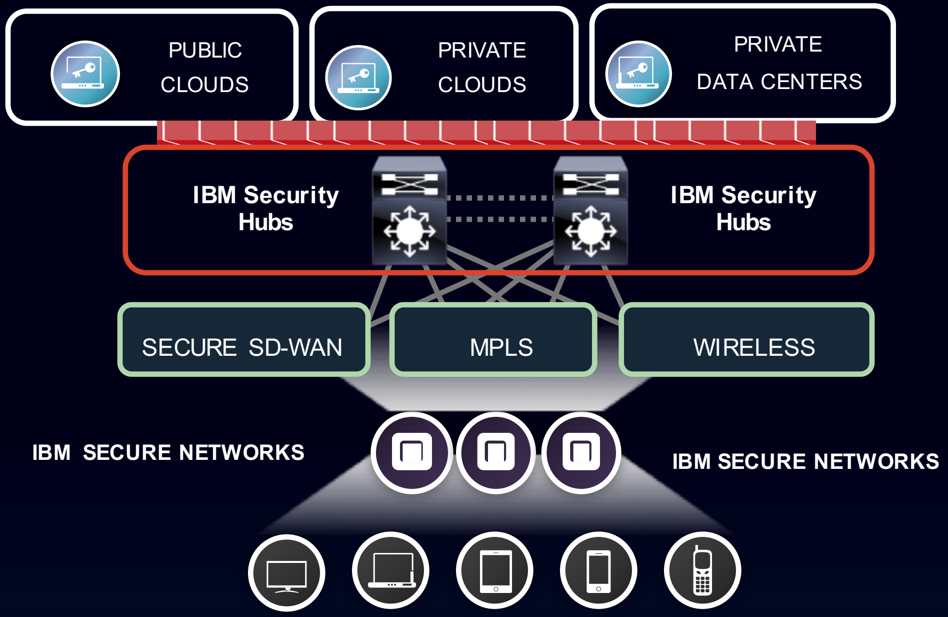
IBM Secure Networking Services

Zero Trust Security

- Secure Application Access to Simplify the Network and Enable Virtualized Cloud & Data Center Services
- Strong Security for Mobile users
- Secure Multi-Cloud Application Protection

Software Defined Security Benefits

- Programmable Security
- End to End Segmentation
- Agile Security Services



Any Person , Anywhere , Any Department , Any Device

IBM Security Hubs

- High Feature Security Services
- Maximized Network Availability with Any Network Transport.
- Secure and resilient high availability Network with Strong Encrypted Zero Trust Security

Integrated Security

- Network and Security Integrated together
- Proactive Analytics
- IoT Security

STRONG SECURITY FOR ALL LOCATIONS:
Firewall, IDS, IAP, DDoS, Malware-AV, DNS Firewall, Ransomware, Anti-Spam, URL Filtering, SSL VPN, IPSec, User FW Machine ID

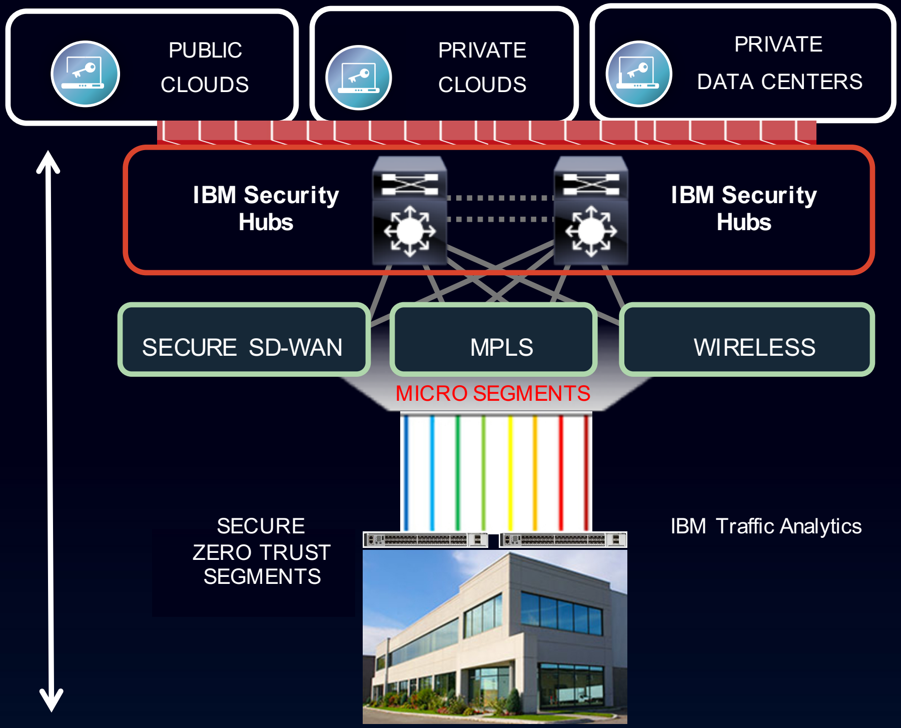
IBM Secure Network Segmentation

Zero Trust Security

- Secure Application Access to Simplify the Network and Enable Virtualized Cloud & Data Center Services
- Strong Security for Mobile users
- Secure Multi-Cloud Application Protection

Software Defined Security Benefits

- Programmable Security
- End to End Segmentation
- Agile Security Services



IBM Security Hubs

- High Feature Security Services
- Maximized Network Availability with Any Network Transport.
- Secure and resilient high availability Network with Strong Encrypted Zero Trust Security

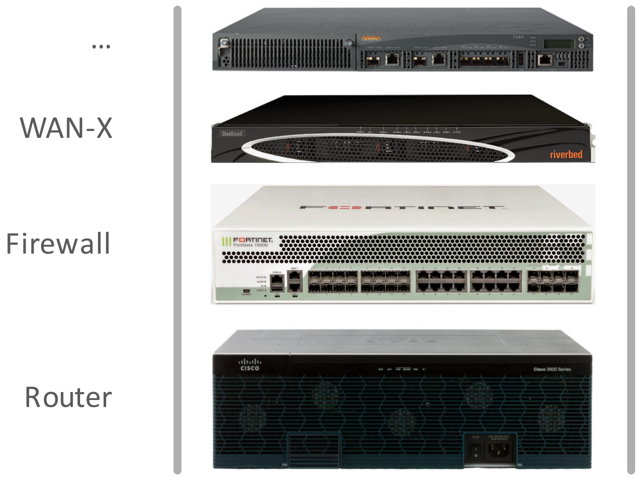
Integrated Security

- Network and Security Integrated together
- Proactive Analytics
- IoT Security

STRONG SECURITY FOR ALL LOCATIONS:
Firewall, IDS, IAP, DDoS, Malware-AV, DNS Firewall, Ransomware, Anti-Spam, URL Filtering, SSL VPN, IPSec, User FW Machine ID

Network Function Virtualization & vCPE

Traditional Network Appliance Approach

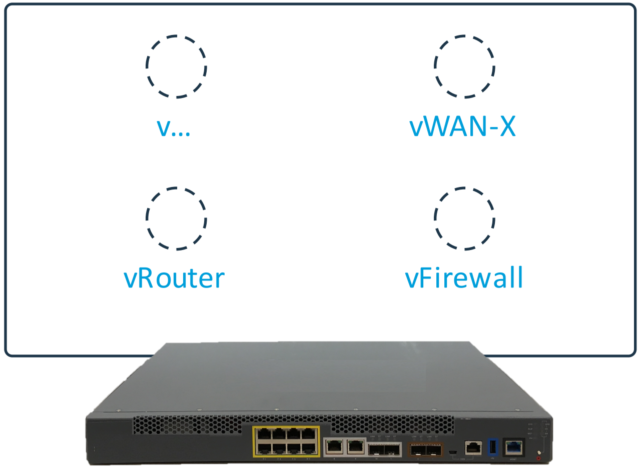


Specialized, proprietary hardware

Physical install per appliance per site

Complex network management

Network Function Virtualization Approach

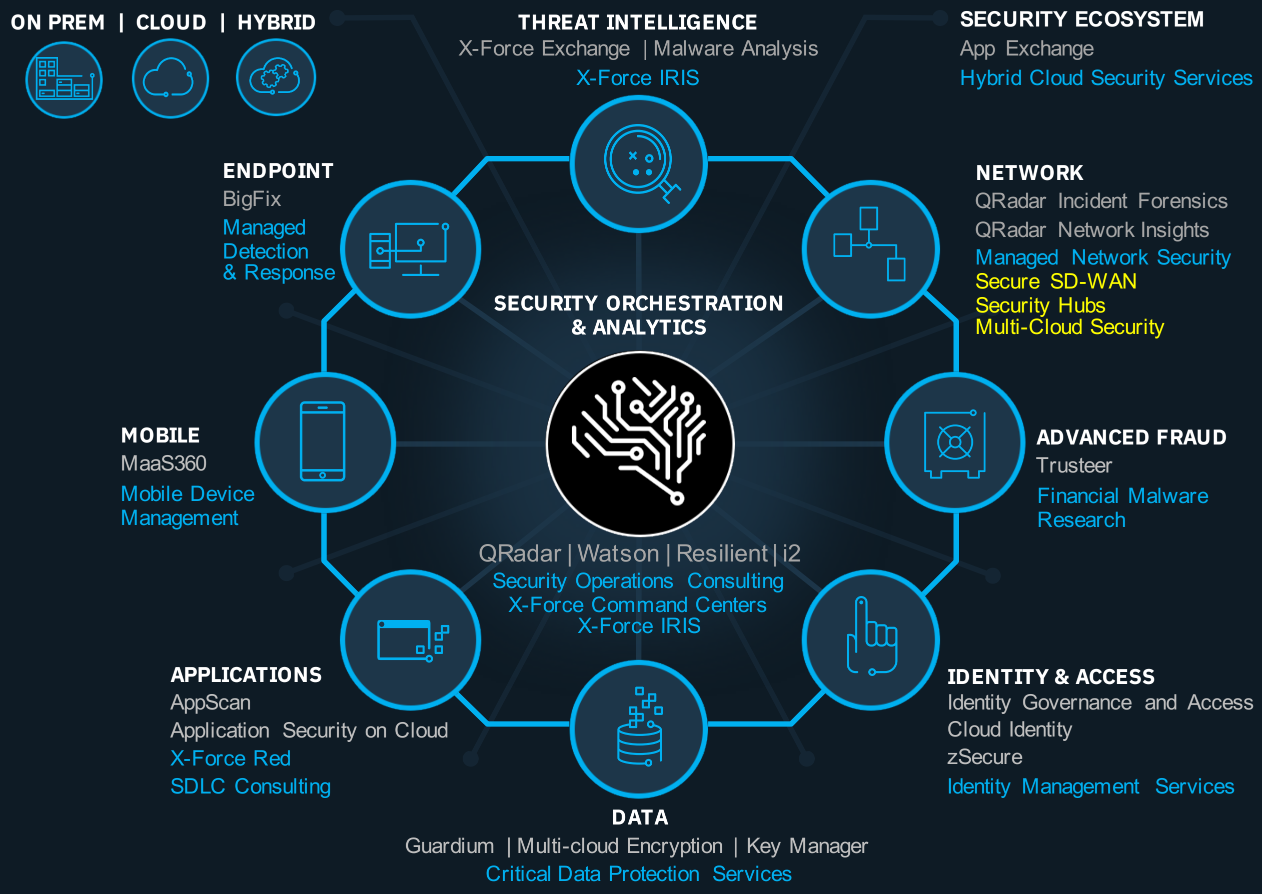


Standard x86 hardware platform

Multiple functions on a single device

Less complexity, improved TCO

IBM Security Immune System



ON PREM | CLOUD | HYBRID

THREAT INTELLIGENCE
X-Force Exchange | Malware Analysis
X-Force IRIS

SECURITY ECOSYSTEM
App Exchange
Hybrid Cloud Security Services

ENDPOINT
BigFix
Managed Detection & Response

NETWORK
QRadar Incident Forensics
QRadar Network Insights
Managed Network Security
Secure SD-WAN
Security Hubs
Multi-Cloud Security

SECURITY ORCHESTRATION & ANALYTICS
QRadar | Watson | Resilient | i2
Security Operations Consulting
X-Force Command Centers
X-Force IRIS

MOBILE
MaaS360
Mobile Device Management

ADVANCED FRAUD
Trusteer
Financial Malware Research

APPLICATIONS
AppScan
Application Security on Cloud
X-Force Red
SDLC Consulting

IDENTITY & ACCESS
Identity Governance and Access
Cloud Identity
zSecure
Identity Management Services

DATA
Guardium | Multi-cloud Encryption | Key Manager
Critical Data Protection Services

Products
Services

Achieving Results : Securely Connect Users and Protect Data

Cloud Security

Mobile Security

Zero Trust Security

Internet of Things Security

Secure SD-WAN enabled protection for all of your assets

What differentiates IBM Security

Global industry expertise

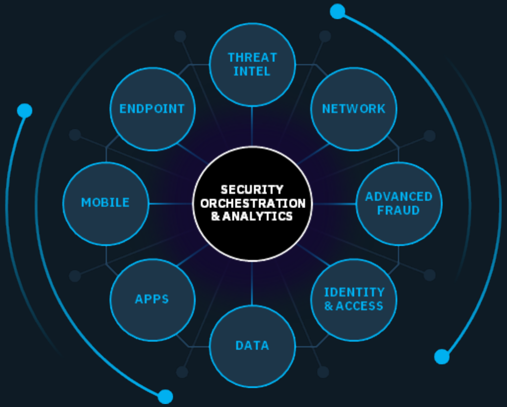
Thousands of engagements driving security transformation

Built 90+ client SOCs and manage over 35B+ events daily in our own

An integrated security system

100+ vendors adopting our open immune system platform

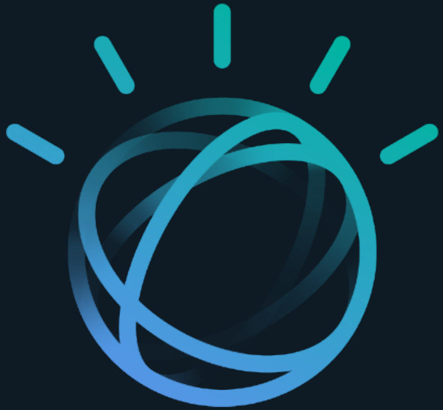
20 strategic acquisitions and leading offerings in 10+ market segments



Leading AI and analytics

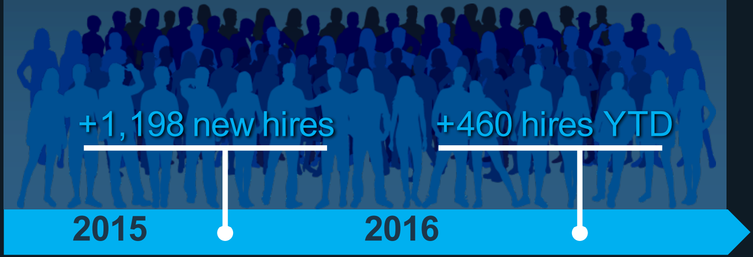
#1 Security Analytics platform, new AI across the portfolio

Successfully trained Watson in the language of Cyber Security



IBM Security today

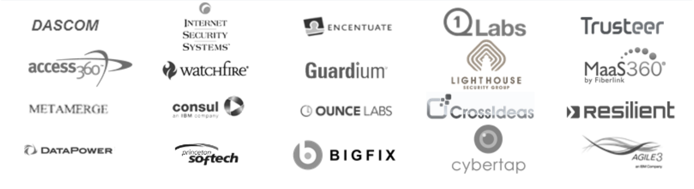
8,000+ security experts, researchers and developers across 133 countries



17,500+ customers

20 acquisitions

2012	2013	2014	2015	2016	2017
Q1 Labs	Trusteer MaaS360	Lighthouse CrossIdeas		Resilient	Agile3



Market Position and Share

Market Position*	Company	'16 Revenue Growth	2016 Share
#1	Cisco	13%	3%
#2	IBM	13%	3%
#3	Symantec	10%	2%
#4	Checkpoint	7%	2%
#5	Palo Alto	36%	2%
#6	Dell / EMC	-1%	1%

Source: GMV 1H17 Spring Plan Market @ Plan Rate (In $B)

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®