We Protect Your World

Steve King

September 15, 2016

Presentation for: MISA

SecureWorks®

Intelligence-driven information security solutions:

- Over 2,000 employees
- 4,100 clients across 61 countries
- Recognized as an industry leader
- Counter Threat Unit™ research team: 70+ dedicated security researchers
  - Focused on emerging threat trends
  - Rapid countermeasure development
- Applied intelligence across solutions

Powered by the Counter Threat Platform

16+ Years of threat intelligence data	**Up to 150B** Events processed daily	**2B+** Threat Indicators
700 Incident Response engagements last year	**1,500+** Consulting engagements performed annually	**300+** Expert security consultants

FIRST · INFRAGARD · CREST · CESG Certified Service Cyber Incident Response · CPNI · DEPARTMENT OF JUSTICE · U.S. DEPARTMENT OF HOMELAND SECURITY · DEPARTMENT OF DEFENSE · THE CYBER WARFARE FORUM INITIATIVE · NCFTA · INTERNET SECURITY ALLIANCE · IDF The Institute of Digital Forensics · Microsoft Active Protections Program

Organizations are struggling to keep up against cyber threats

Cyber attacks are growing in complexity...

66%
3rd Party Discovery

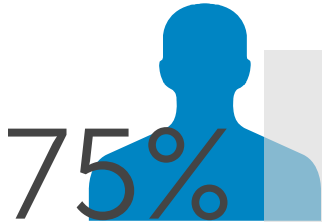
33%
2 Years to Discover

50%
Bypass existing controls & "Living off the Land"

$3.7M
Average total cost of a breach involving records

Source: Ponemon Institute's 2014 State of Endpoint Risk Report
Source: Dell SecureWorks

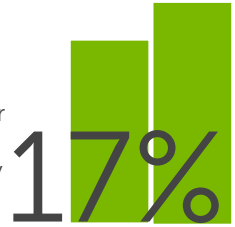
...security professionals are limited in number...



75%

Percentage of security professionals who "have been approached by a hiring organization or headhunter about IT job opportunities in the past year."

Premium paid to senior and middle-level managers with security in their titles.



17%

Source: ComputerWorld IT Salary Survey 2015

...lack of true "intelligence" minimizes ability to see the big picture.

Your data on the underground market

Sutton's Law in Cyberspace: Your business is where the money is.

RAT

Angler
$100

$15

Price of a Visa credit card with Track I and II data available on the dark web.

$30

Price of an American Express premium credit card with Track I and II data.

$40

Price for banking credentials for a U.S.-based account with a $1,000 balance.

$90

Price for a new identity - a driver's license, social security number and matching utility bill.

Breaches are a global, systemic problem

By Industry

Cost per stolen record (U.S.)

By Country

U.S.	$6.5M	↑ 11%
Germany	$4.8M	↑ 3.1%
Canada	$4.4M	-
France	$4.3M	↑ 3.5%
Arabian	$3.8M	↑ 21%
U.K.	$3.7M	↑ 1%
Japan	$2.6M	↑ 13.5%
Australia	$2.6M	↑ <1%
India	$1.4M	↑ 6.5%

Average Total Org Cost, % change over prior year

Source: Ponemon 2015 Cost of Data Breach Study - Global Analysis

Cyber Security has become a top priority at the executive level

Financial Performance

How will a breach affect our current and future financial performance?

Cost to Resolve

What's our plan and how much will it cost to resolve a breach?

Intellectual Property

How do we ensure our intellectual property is adequately protected?

Reputation

What's the impact to our reputation and brand among customers, partners and employees?

Legal Liability

What is the organization's legal liability to customers, employees, partners, and regulatory entities?

Opportunity Cost

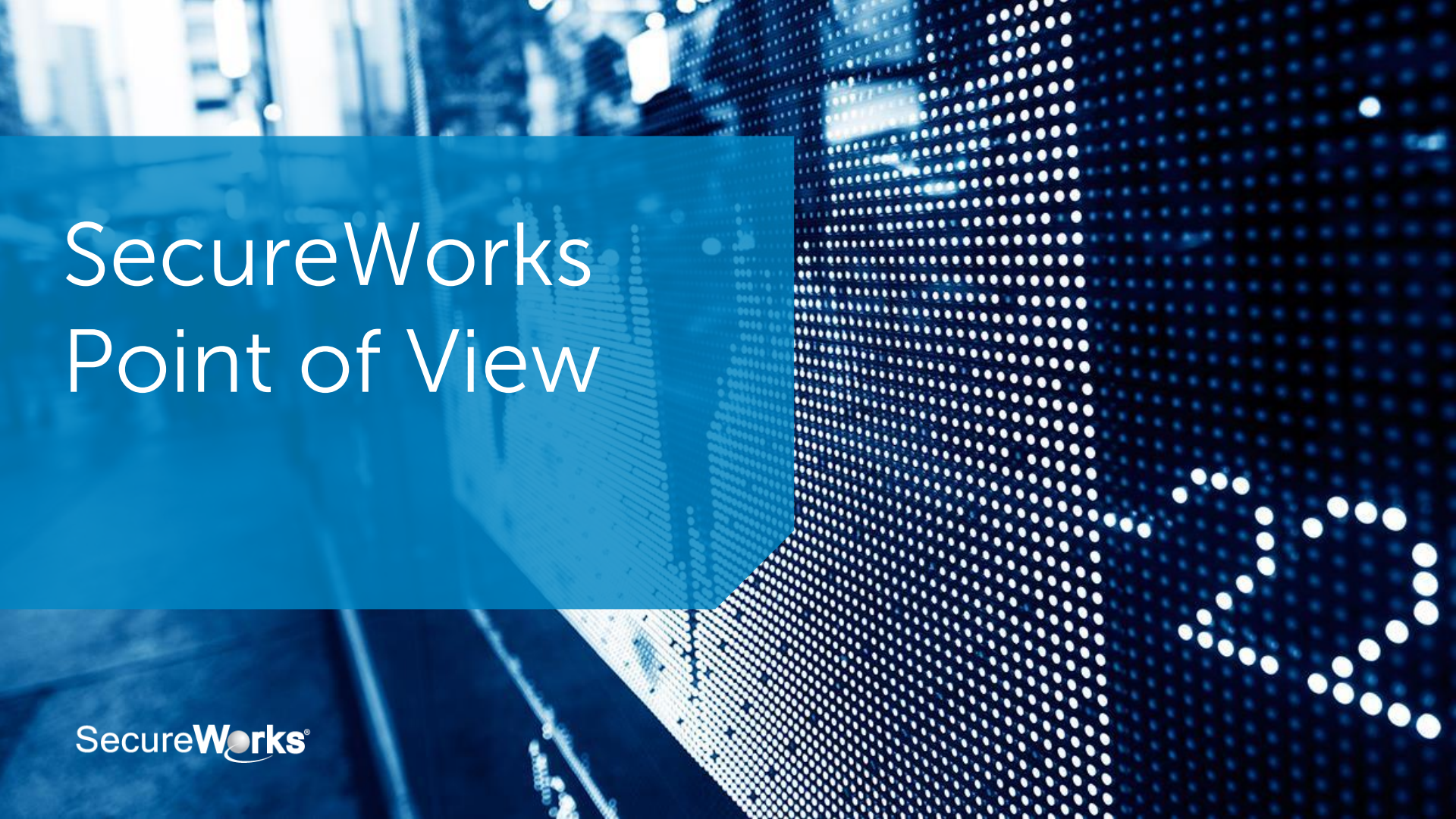
How will a major breach affect our existing plans?

Risk Management

Do we really understand the level of risk we're exposed to, and what are we doing to address it?

Security Program

What program metrics exist today? How quickly would we know if our risk profile suddenly changed?


SecureWorks
Point of View
SecureWorks

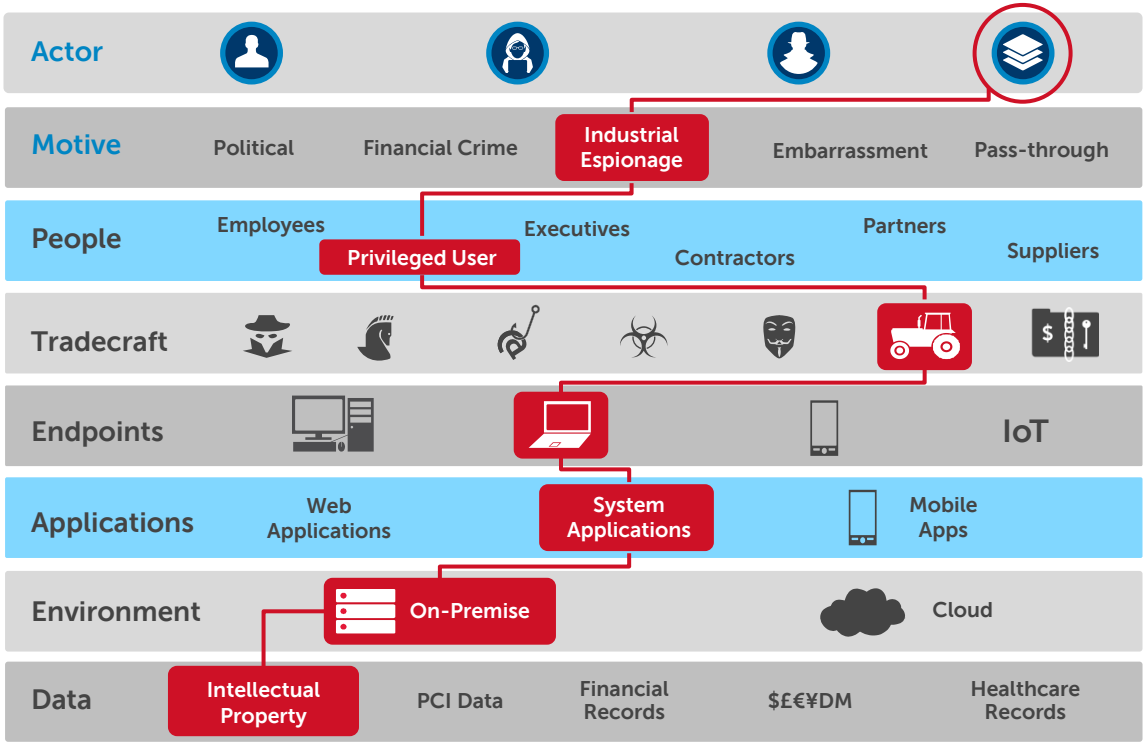
The many forms the threat can take

The Situation

A nation-state sponsored adversary acquired legitimate credentials as a result of a phishing email.

The adversary:

- Didn't use malware.
- Used admin tools within the target environment to expand access – known as "living off the land"
- Successfully exfiltrated intellectual property



Evolution of security operations

	TODAY	TOMORROW
Investment	IT expense without ROI	Optimized investments **delivering increased protection** and compliance
Visibility	Limited and disconnected visibility	**Integrated visibility** with control across your hybrid environment
Intelligence	Security data without intelligence	Actionable intelligence that **reduces time-to-detect** and **time-to-respond**
Protection	Security technologies without protection	**Future-proof protection** that meets the needs of today and tomorrow
Skills	Limited availability of skills and expertise	On-demand access to expertise and tools for **faster speed-to-protection**
Strategy	Uneven security posture based on resources	**Enabled business outcomes**: Secure — Anywhere, anytime

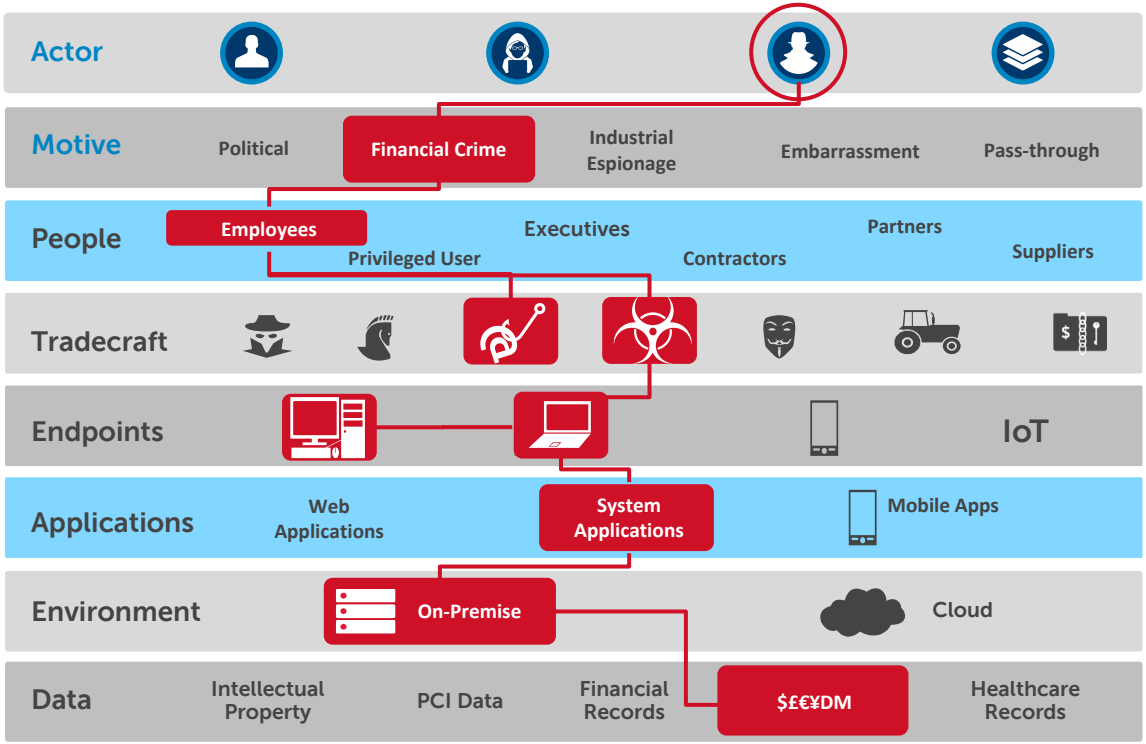
The many forms the threat can take: Ransomware

How the Situation Unfolded

Unknown cybercriminals managed to introduce ransomware into a hospital's environment via a phishing email. The ransomware soon spread affecting numerous systems with sensitive patient and other data. The breach has resulted in a major disruption to hospital operations with a lockdown in usage of digital assets.

The adversary:

- Introduced ransomware that potentially rendered sensitive data unusable.
- Demanded a ransom in Bitcoin currency



Security Operations and Intelligence

- Cyber Security Operations Consulting
- Global Threat Intelligence
- Enterprise Brand Surveillance
- Borderless Threat Monitoring
- Counter Threat Unit™ Support
- Advanced Malware Analysis

Security, Risk and Compliance Solutions

- Security Advisory
- Critical Security Controls Assessment (CSC 20)
- Information Security Program Assessment
- Information Security Policy Development
- Security Design and Architecture

Compliance Solutions

PCI, HIPAA, GLBA/FFIEC FISMA, EI3PA

- Managed Security Solutions
- Compliance Consulting and Audit
- Managed Vulnerability Scanning
- PCI Forensic Investigation (PFI)

Security Testing

Network Testing

- Vulnerability Assessment
- Penetration Test
- Advanced Penetration Test
- Wireless Security Testing
- Social Engineering
- Phishing: Click and Log
- Phishing: Endpoint Attack
- Vishing

Real-world Testing

- Onsite Red Team Testing
- Remote Red Team Testing

Network and Endpoint Solutions

Security Monitoring

- Managed Firewall Managed NG Firewall
- Managed IPS/IDS
- Manage iSensor/ Enterprise iSensor
- Managed Web Application Firewall (WAF)
- Firewall Audit and Optimization

Advanced Malware Protection

- MAMP
- AMPD

Endpoint Security

- AETD
- Monitored Server Monitoring

Data and Application Solutions

Vulnerability Management

- Managed Vulnerability Scanning
- Managed Web Application Scanning
- Managed VMS – PCI Scanning
- Managed VMS – Web App Scanning
- Vulnerability Threat Prioritization
- Managed Policy Compliance
- Vulnerability Assessment
- Mobile Application Security Assessment
- Web Application Security Assessment
- API Assessment

Incident Response and Management

Proactive Services

- Compromise Screening Assessment
- Incident Management Risk Assessment
- Response Workshops and Exercises
- Response Plan Review/ Development
- Targeted Threat Hunting (TTH)
- Incident Management Retainer

Reactive Services

- Incident Response Remote/Onsite
- Digital Forensics and Malware Analysis
- PCI Forensic Investigation (PFI)
- Targeted Threat Response (TTR)

Cloud and IoT Solutions

Security Advisory

- Security Design and Architecture
- Cloud Strategy Dev. and Assessment
- Cloud Vendor Assessment
- Cloud Strategy Assessment
- Security Framework Assessment
- Vulnerability Management

Security Testing

- Penetration Testing
- Red Team Testing
- API Assessments
- Incident Response for AWS

Security Consulting | Managed Services | Incident Response and Management | Threat Intelligence

Our Point of View: Security for your world when you need it

Act as a trusted security partner to all levels of the organization

CISO
IT Security Directors

CIO
IT Directors

C-Suite Leaders
Board of Directors

Safeguard your environment against emerging threats

Provide visibility and detection of threats for an expanding perimeter

Data Center

Cloud

Endpoint

Mobile and IoT

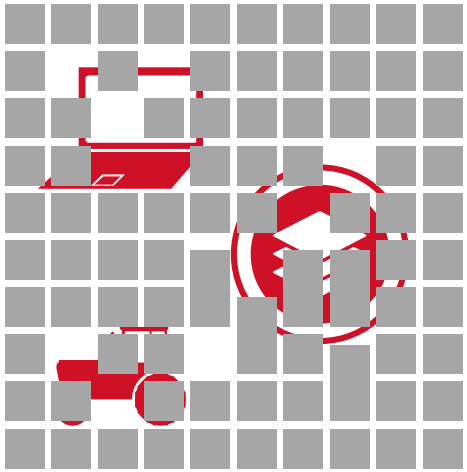
Leverage global visibility, scale and analysis to drive cognitive insights across our solution portfolios.

Provide end-to-end security solutions to create business value

Minimize Business Risk and Enable Business Priorities

“Early Warning” actionable intelligence is critical

...lack of actionable “intelligence” reduces ability to see the big picture.



Security event information can tell you:

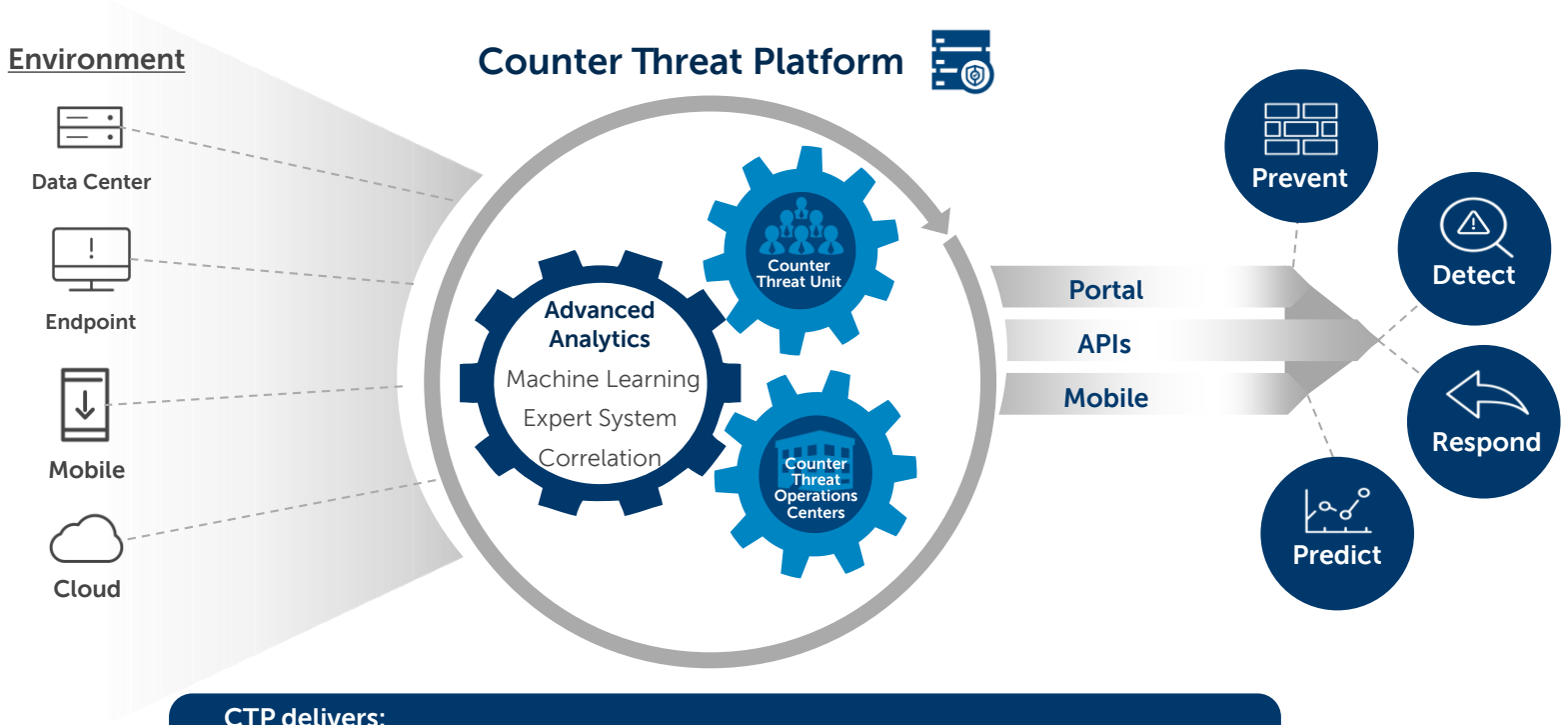
- **How?** How did the adversary get in and where did they spread to?
- **What?** What malware did they use and what does it do?
- **When?** When did this happen and what’s gone on since then?

Intelligence helps you go beyond to answer:

- **Who?** Who may be behind it and what else should we look for?
- **Why?** Why were we targeted? What is the actor’s end game?

Accurate diagnosis and remediation

Counter Threat Platform – Visibility, Scale, Intelligence



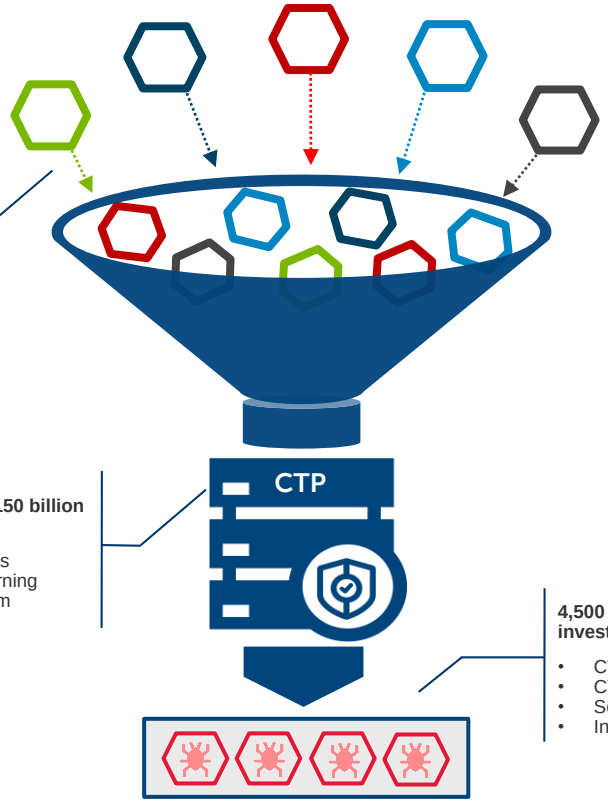
CTP delivers:

- Global Threat Intelligence
- 16+ years of attack & threat actor group
- 2B+ threat indicators
- Applied intelligence based on industry/business

Counter Threat Platform (CTP) – Visibility, Scale, Intelligence

Top Logging Activity:

- Malware, IDPS, Endpoint,
- Web Proxy, AV, DNS, FW, VPN
- Outlook Web Access
- Admin protocols, App Whitelisting
- Authentication



CTP processes 150 billion events per day:

- Data Sciences
- Machine Learning
- Expert System
- Correlation

4,500 potential threats to investigated by:

- CTOC Analyst
- CTU Researcher
- Security Consultant
- Incident Responders

We help you:

- **99.999%** of threats automatically handled by Counter Threat Platform
- **Expert monitoring** & event management
- Average **40+% cost savings** over traditional solutions
- Detect emerging threats **53+days ahead** of traditional solutions
- Coordinated defenses using **1,000s** of data and **intelligence sources**
- **Enable Security** – Anytime, Anywhere, Anyway you need it

CTP Scale:

- **Filter Groups** = 397
- **Filter Rules** = 47,600
- **MPLE Rules** = 62,948

About the Counter Threat Unit™ (CTU) research team

We actively monitor the cyber threat landscape, perform in-depth analysis of emerging threats and zero-day vulnerabilities, and apply protections to client environments worldwide, every day.

Top Research Talent

70+ Top security researchers

2B+ Threat Indicators

100+ Threat Groups actively monitored from 30+ countries

100+ APT-response engagements

Expertise

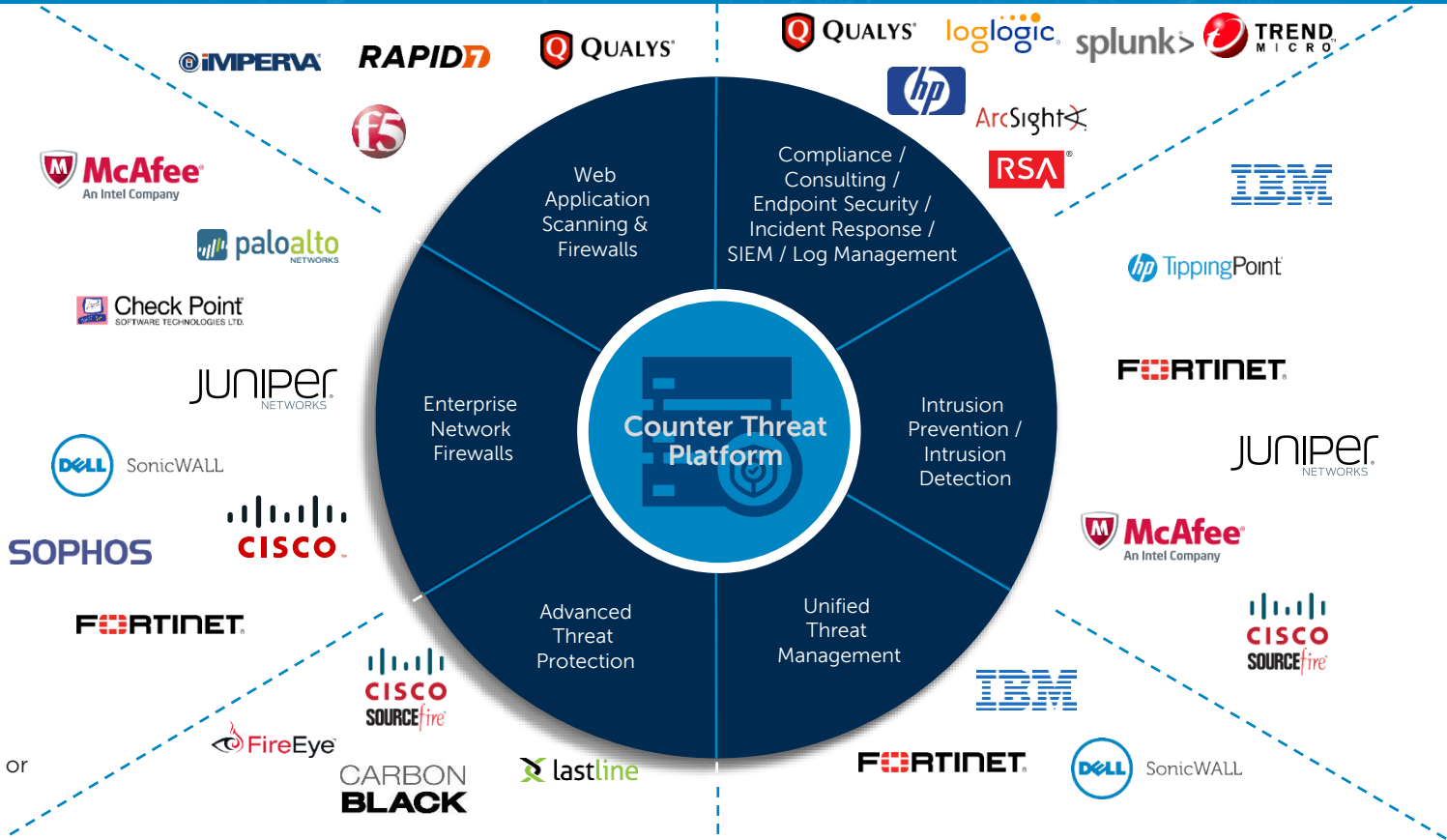
- Countermeasure Development
- Advisory and Support
- Knowledge Sharing
- Malware Analysis
- Security Innovation
- Specialized Threat Research
- Vulnerability Analysis and Management

Applied Intelligence

Intelligence formulated by the CTU is applied across SecureWorks' operations.

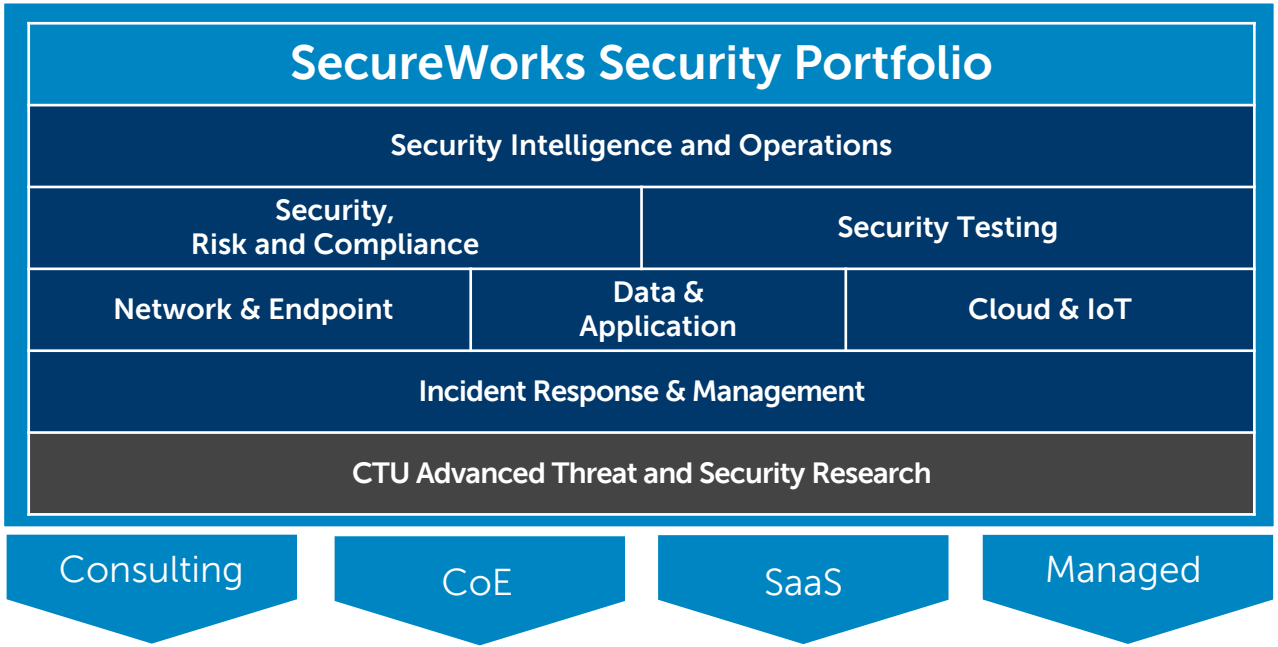
SecureWorks unifies enterprise security for our clients

We span the security ecosystem to preserve your investments

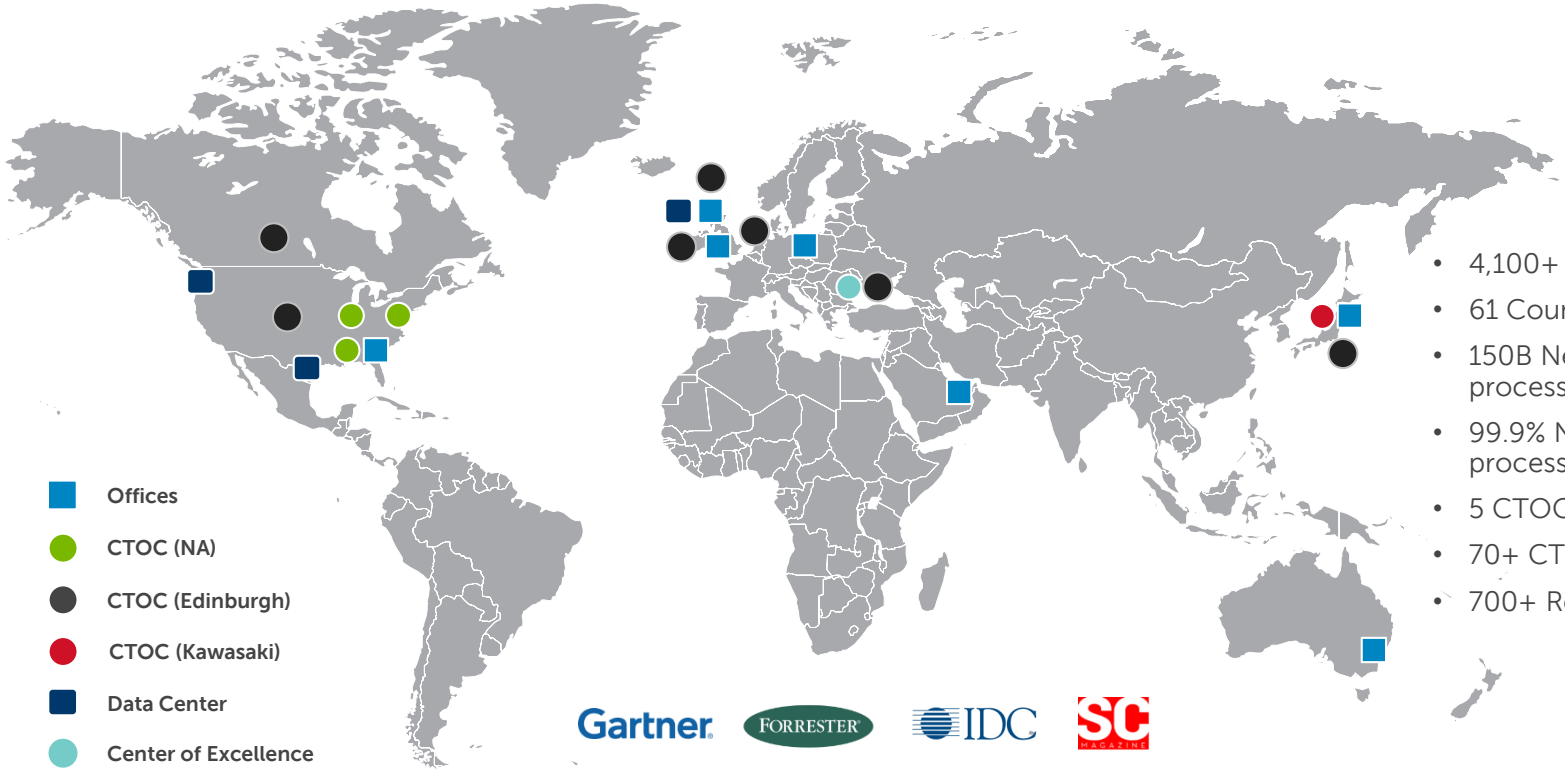


Additional device or vendor support may be available.

SecureWorks Security Framework



Why SecureWorks



- 4,100+ Clients
- 61 Countries
- 150B Network Events processed daily
- 99.9% Network events processed automatically
- 5 CTOCS
- 70+ CTU Researchers
- 700+ Response engagements

Gartner FORRESTER IDC SC MAGAZINE

What our clients say:

Trusted Advisor
"Dell SecureWorks is a strategic MSSP partner for my company and I would recommend their services to others."

— Client: Global Industrial Development Industry

Intelligence
"SecureWorks consistently provides the fastest and most informative alerts on events and activity on our perimeter."

— Financial Industry

Value and Breadth of Portfolio
"The value of the services we have contracted for are invaluable. Your portfolio of services Is robust...."

— Trade Association

Service Excellence
"Our experience in the implementation of the Dell SecureWorks SIEM and IDS/IPS Managed Solutions went flawlessly; the continued support and monitoring provided has been exceptional and [I] feel the solutions implemented are providing substantial value for our organization."

— Healthcare Network Provider

Trusted Partner
"The solution is constantly protecting the bank's network from all sorts of attacks ensuring no disruption to service."

— Financial Industry

Trusted Partner
"[The consultant] provided us the essential guidance for improving our security posture as we look to mature our company's information security."

- Healthcare Provider

SecureWorks®

Next Steps

- Contact your Dell SecureWorks sales representative for a consultation on:
  - Assessing your organization's risk
  - Building a road map to become a leader in security

- Download Your Complimentary Copy of the: 2016 State of Cyber Security Report

SecureWorks

For more information, visit **www.secureworks.com**

Or, contact your Security Specialist

Thank You