IBM **i2 for a safer planet**

IBM Security

Know your enemy

Find the bad guys with proactive cyber threat intelligence and threat hunting

IBM Security Thought Leadership White Paper

Evolve from reactive to proactive cyber defense

In today's security landscape, where organizations face multiple, ever-evolving[1] security threats every year and millions of dollars in damage from each threat that succeeds,[2] fortifying the enterprise against cyber attacks is a near-universal practice. And in most cases—about 80 percent, according to security experts[3]—those fortifications work. But what about the other 20 percent? Why aren't those threats stopped? And what can be done to prevent them?

Security is hard. But increasingly, organizations facing cyber threats are discovering the truth of the old adage: *The best defense is a strong offense.* So, to existing defenses, they are adding aggressive capabilities known as "cyber threat hunting" to detect, disrupt and defeat advanced threats before they do damage.

IBM® i2® Enterprise Insight Analysis is a next-generation intelligence analysis solution that provides cyber threat hunting using advanced analytics and human-led analysis. These capabilities allow the analyst translate huge amounts of structured and unstructured information into intelligence, uncover hidden connections in threat actions and actors, and help turn data into decisions in near-real time.

By leveraging proactive cyber threat intelligence analysis along with advanced analytics, you can better understand your enemy and their tactics, techniques and procedures (TTPs). Armed with this insight, you can better defend your network against advanced attacks.

[1] "2018 Verizon Data Breach Investigations Report," *Verizon,* April 2018.

[2] "2017 Cost of Data Breach Study: Global Overview," *Ponemon Institute,* June 2017.

[3] Bob Stasio, "Understanding Cyber Threat Hunting," *IBM,* March 21, 2017.

Uncover advanced threats

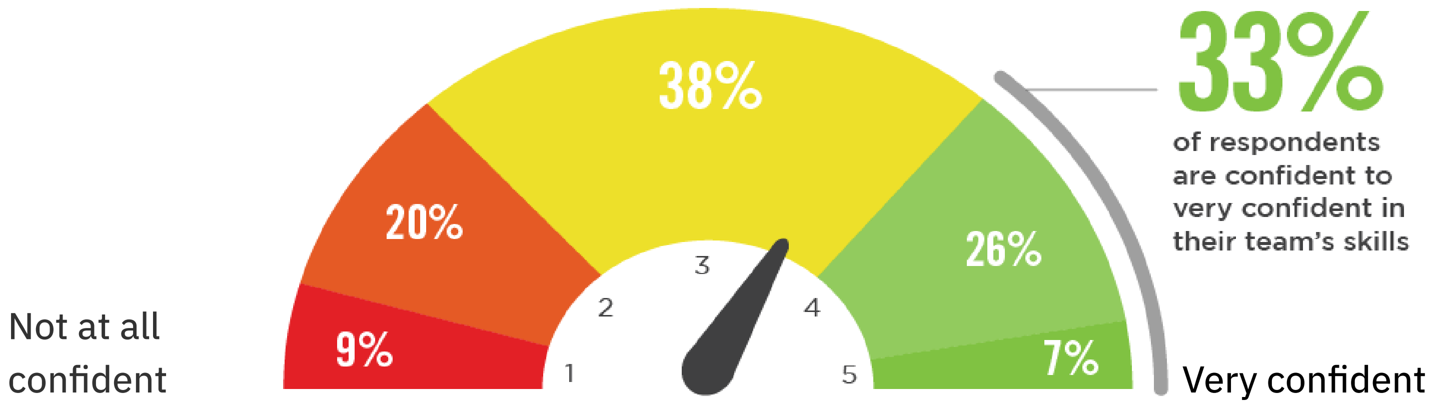
Enterprise security operations centers (SOCs) are overworked and understaffed. The volumes of security data they must analyze is overwhelming. And while many of their reactive, incident-driven defenses work, sophisticated cybercriminals typically know where those protections reside in their organizations—and possess the skills and tools to get around them. Then, when advanced persistent threats (APTs) do penetrate the enterprise, they remain in the infrastructure for months, slowly doing their dirty work. Though a relatively small percentage of total attacks, these undetected and unknown threats can, over time, be the most damaging.

In the face of these challenges, policy-based defenses that simply recognize known threats based on previous experience are no longer enough. Threat intelligence analysts need tools that can help them gain insight into the criminals they are fighting—thereby identifying the weaknesses in enterprise defenses and understanding the evolving tools, techniques, tactics and practices of their attackers. But if they are to win the battle, analysts ultimately need to move beyond reactive response and outwit their attackers. In order to achieve this, analysts need a new, proactive approach to security that enables them to identify threat actors and their purpose, intentions, infrastructure and weaknesses.

Whether the risk is to national security and public safety that can occur when threats strike defense and law enforcement organizations, or the interruptions to workflow, loss of intellectual property, theft of customer data, and damage to reputation and bottom line that can occur when threats strike businesses. Stopping cyber threats now requires situational awareness and contextual insights that prevention alone cannot provide.

View the IBM infographic for a quick overview describing the basics of cyber threat hunting.

▶ How confident are you in your SOC's ability to uncover advanced threats?



33% of respondents are confident to very confident in their team's skills

IBM i2 cyber threat hunting merges data from multiple sources to help counter threats.

Cyber threat hunting enriches existing security measures to expose abnormal and dangerous behavior among seemingly normal activities. It employs digital analytics to unearth unidentified details describing an attacker's behavior that an analyst would never spot in the mountains of databases, emails, social media, the Internet of Things and open sources that generate data. And it utilizes human-led analysis that may be based on a simple hunch a researcher feels but that never would appear in a computer's findings. Cyber threat hunting then merges data from these various sources to counter and mitigate threats.

Increase speed and accuracy of detection

In recent years, APTs have not only become more frequent and dangerous, they've also become easier for attackers to purchase, build and deploy. Kits for creating threats are readily available for purchase on the dark web. Malware no longer requires coding skills to customize for the attacker—or the target. An individual with an inexpensive laptop can pose a significant threat to even the largest enterprise.

Meanwhile, the SOC team at the enterprise often doesn't have enough experienced threat intelligence staff. It is deluged with too much data to understand—and too many point solutions that attempt to provide security with insufficient integration. The SOC may be able to protect against the threats it knows about, but seldom can protect against those that are undetected and unknown.

Unless, and until, it engages in proactive cyber threat hunting.

Threat hunting's combination of computer-driven analytics and human-led analysis provides actionable insights to protect data and neutralize cyber threats. And it works. A recent survey by the SANS Institute found that 91 percent of organizations experienced increases in both the speed and accuracy of their responses when they used threat hunting. An equal number said threat hunting reduced their overall exposure to threats.[1]

By blending intelligence analysis, information security and forensic science to examine data sources ranging from network traffic and system logs to human-generated information, threat hunting provides a faster, more comprehensive and more effective way to process extremely large amounts of data—helping close the gap between the capabilities of defenders and attackers.

Read the IBM blog to learn the key concepts behind cyber threat hunting.

What are the main benefits of using a threat hunting platform for security analysis?

64%
Improving detection of advanced threats

63%
Reducing investigation time

59%
Saving time from manually correlating events

More importantly, the near-real-time capabilities of cyber threat hunting help close another gap—the one between the time of compromise and the time to detection. With an average "dwell time" in systems of 197 days before detection,[2] many attackers conduct "low and slow" campaigns that do serious damage before they are discovered.

Beyond helping discover that an attack has taken place, cyber threat hunting also proactively gathers information to determine who is attacking and how the attack is being conducted. These insights become key parts of the organization's strategy, practices and tactics for preventing future attacks.

[1] Rob Lee and Robert M. Lee, "The Hunter Strikes Back, The SANS 2017 Threat-Hunting Survey," *SANS Institute,* April 2017.

[2] "2018 Cost of a Data Breach Study: Global Overview," *Ponemon Institute,* July 2018.

Accelerate cyber threat hunting with advanced analytics and intelligence analysis

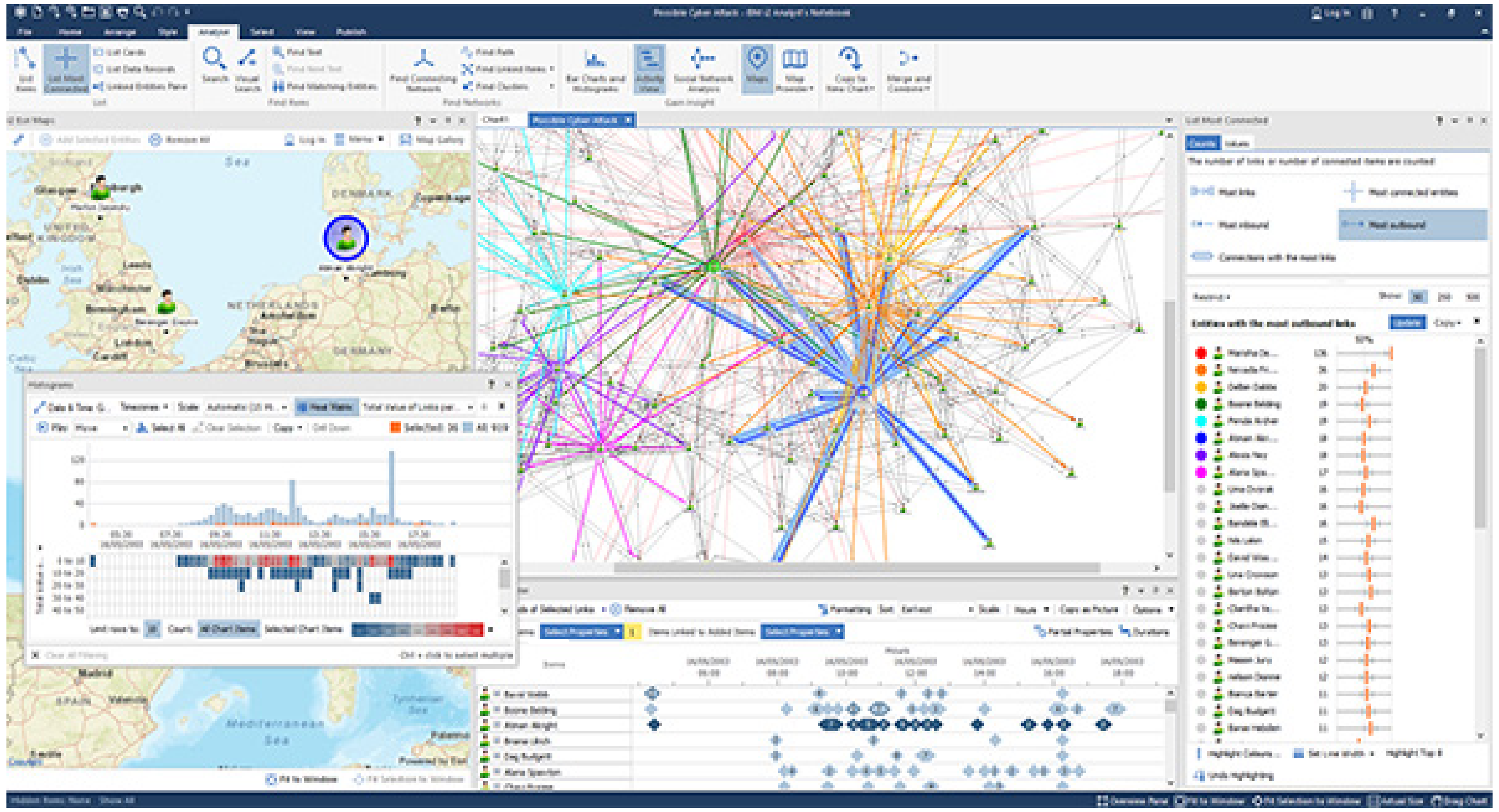
IBM i2 Enterprise Insight Analysis provides cyber threat hunting capabilities that go far beyond policy-based solutions by combining advanced analytics with a human-versus-human approach. Designed to detect, disrupt and defeat advanced threats by correlating and analyzing disparate data, the solution can make the difference in understanding and anticipating when and where cyber threats will occur—so they can be stopped before they cause damage.

Using machine learning and visual, temporal and geospatial analysis, IBM i2 Enterprise Insight Analysis enables analysts to discover connections between potentially matching items imported from disparate data sources. It then finds and merges matching entities, including seemingly unrelated relationships and patterns.

By analyzing large volumes of structured and unstructured data—including business information such as personnel data that is not normally considered to be security-focused, or physical data that is not typically analyzed as part of cybersecurity measures—IBM i2 Enterprise Insight Analysis enables analysts to triangulate their search for the situational awareness that is critical to securing organizations today.

For example, the discovery of a large download of intellectual property over a weekend may indicate either an external or internal threat. But if physical information, such as a badge swipe, is added to the cyber discovery, the SOC can pinpoint the download as an internal bad actor.

Merging security product data, open-source intelligence and dark web data helps analysts visualize the connection between network activity and behavior. Utilizing social media data, human resource data, expense data, inexplicable travel data, and data about an insider's known associates—among other information—can help analysts solve the particularly thorny problem of separating threats by actual insiders from threats posed by external attackers disguising themselves as insiders with legitimate, but stolen, credentials.



Watch the video to learn how IBM i2 protects against "whaling attacks" on key executives.

How does IBM i2 Enterprise Insight Analysis work?

IBM i2 Enterprise Insight Analysis is a software-deployed solution—integrated with security consulting capabilities provided by IBM and IBM business partners. Deployment and consultation, in fact, go hand-in-hand from the very beginning, with IBM helping the organization understand what data it needs to collect and analyze for the types of threats it is facing and the issues it is trying to solve.

Analysts can use IBM i2 Enterprise Insight Analysis integrated analysis capabilities to transform data into decisions in near-real time by uncovering hidden connections with visual displays and turning overwhelming and disparate data into actionable intelligence. This layered approach addresses a wide range of data sources, from network logs to social media, in order to determine who is attacking the organization as well as the threat's locations, targets and associates.

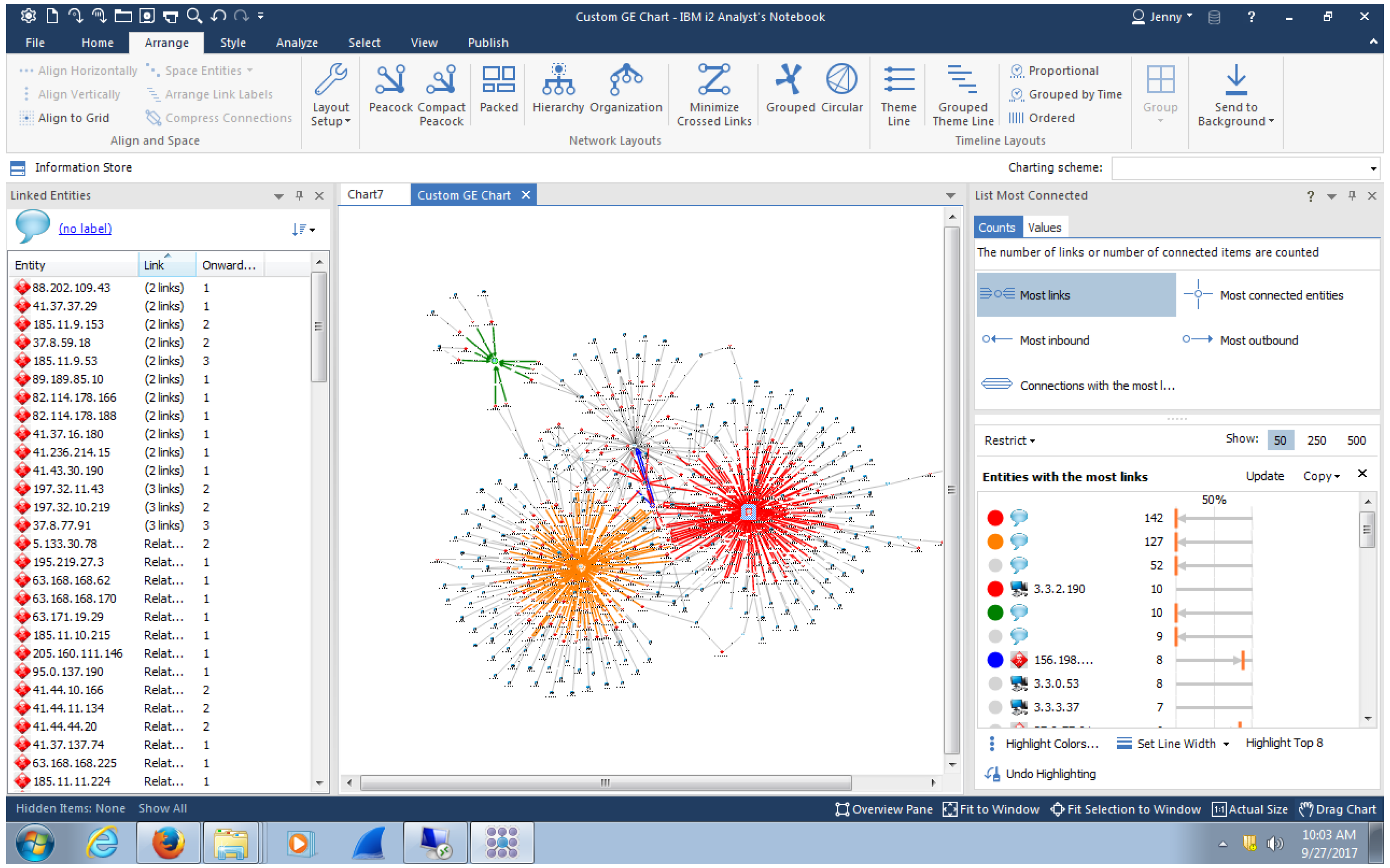
IBM i2 Enterprise Insight Analysis enables organizations to find threats faster, reduce dwell time and reduce the costs and impacts of attacks by enabling analysts to:

- Quickly identify threats, threat actors and hidden connections using multi-dimensional visual analysis and advanced analytics
- Visualize cyber incidents by analyzing large, disparate silos of data with unprecedented speed
- Extend capabilities to process data that is not only about cybersecurity, such as data generated by human resources or physical data, with comprehensive analysis, in near-real time
- Analyze structured and unstructured data including dark web and open-source intelligence (OSINT) data
- Deploy capabilities out of the box with an open and extensible architecture,

Watch the video to learn how IBM i2 helps protect against insider threats.

IBM i2 has a library of PPS connectors for third party data sources

Supported by IBM in-house subject matter experts and the IBM ecosystem for design, install, support and training, IBM i2 Enterprise Insight Analysis is an ideal solution for large organizations facing complex security challenges.



Entity	Link	Onward...
88.202.109.43	(2 links)	1
41.37.37.29	(2 links)	1
185.11.9.153	(2 links)	2
37.8.59.18	(2 links)	2
185.11.9.53	(2 links)	3
89.189.85.10	(2 links)	1
82.114.178.166	(2 links)	1
82.114.178.188	(2 links)	1
41.37.16.180	(2 links)	1
41.236.214.15	(2 links)	1
41.43.30.190	(2 links)	1
197.32.11.43	(3 links)	2
197.32.10.219	(3 links)	2
37.8.77.91	(3 links)	3
5.133.30.78	Relat...	2
195.219.27.3	Relat...	1
63.168.168.62	Relat...	1
63.168.168.170	Relat...	1
63.171.19.29	Relat...	1
185.11.10.215	Relat...	1
205.160.111.146	Relat...	1
95.0.137.190	Relat...	1
41.44.10.166	Relat...	2
41.44.11.134	Relat...	2
41.44.44.20	Relat...	2
41.37.137.74	Relat...	1
63.168.168.225	Relat...	1
185.11.11.224	Relat...	1

The number of links or number of connected items are counted

Most links | Most connected entities | Most inbound | Most outbound | Connections with the most l...

Restrict | Show: 50 250 500

Entities with the most links | Update | Copy

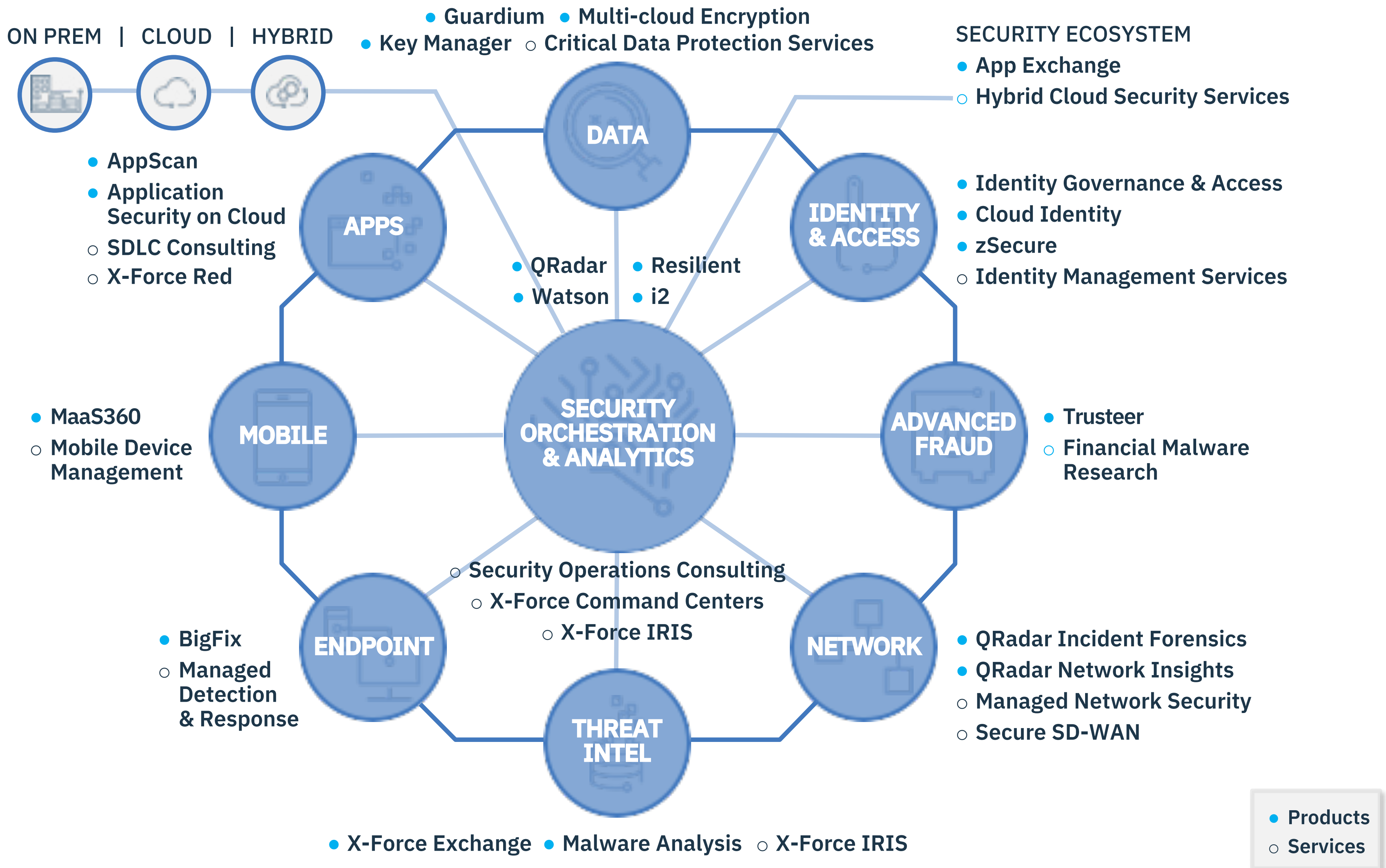
		50%
●		142
●		127
●		52
●	3.3.2.190	10
●		10
●		9
●	156.198....	8
●	3.3.0.53	8
●	3.3.3.37	7

Highlight Colors... | Set Line Width | Highlight Top 8 | Undo Highlighting

i2 at the Core of the IBM Security Immune System

- i2 is the tip of the spear in the modern SOC, proactively hunting threats before they cause damage
- Fuses internal and external, structured and unstructured data from across your security environment and organization
- Force multiplies the efforts of analysts to find threats faster, reduce dwell time and reduce the costs and impacts of attacks

Security Orchestration and analytics



ON PREM | CLOUD | HYBRID

● Guardium ● Multi-cloud Encryption
● Key Manager ○ Critical Data Protection Services

SECURITY ECOSYSTEM
● App Exchange
○ Hybrid Cloud Security Services

● AppScan
● Application Security on Cloud
○ SDLC Consulting
○ X-Force Red

● QRadar ● Resilient
● Watson ● i2

● Identity Governance & Access
● Cloud Identity
● zSecure
○ Identity Management Services

● MaaS360
○ Mobile Device Management

● Trusteer
○ Financial Malware Research

○ Security Operations Consulting
○ X-Force Command Centers
○ X-Force IRIS

● BigFix
○ Managed Detection & Response

● QRadar Incident Forensics
● QRadar Network Insights
○ Managed Network Security
○ Secure SD-WAN

● X-Force Exchange ● Malware Analysis ○ X-Force IRIS

● Products
○ Services

Why IBM?

IBM i2 solutions are backed by the power of IBM, including in-house intelligence analysis subject matter experts, IBM services, and the IBM partner ecosystem for design, install, support and training to handle even the most complex challenges. IBM i2 offers proven subject expertise, longevity in the market and experience in global deployments of all sizes that is unmatched.

Now is the time for a cyber threat hunting solution designed to help solve the problem of advanced threats in a world where threat actors have the skills and the tools necessary to stay under the radar of traditional policy-based security solutions.

IBM i2 is committed to helping ensure a safer planet by arming analysts around the world with advanced analytics and intelligence analysis capabilities to detect, disrupt and defeat advanced physical and cyber threats.

IBM i2 fuses the power of human-led intelligence analysis and machine analytics to uncover patterns and find the signal in the noise.

Read the solution brief to learn more about IBM i2 solutions for cyber threat hunting.

For more information

To learn more about IBM i2 Enterprise Insight Analysis, contact your IBM representative, or visit: ibm.com/us-en/marketplace/enterprise-insight-analysis

View a demo of IBM i2 Enterprise Insight Analysis at: ibm.com/security/resources/demos/i2-enterprise-insight-analysis-yber

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors more than one trillion events per month in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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.