

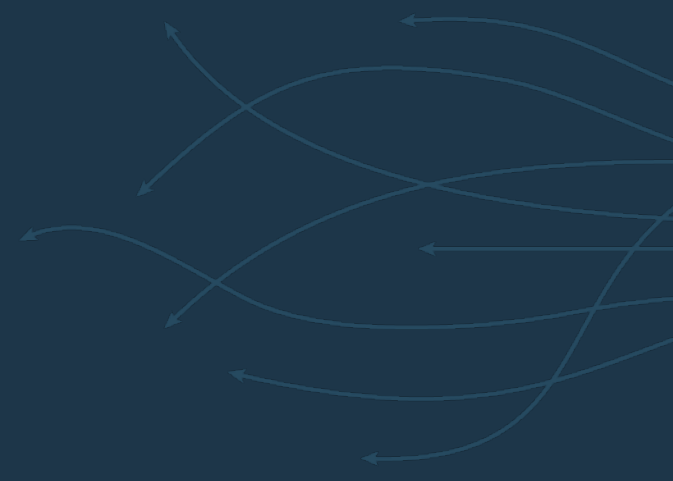
QRadar Compelling Use Cases

THE INTELLIGENT SIEM



Chris Meenan

Director, Security Intelligence Offering Management and Strategy



What is interesting out there ?

- Advanced threat detection and AI
- User Behavior Analytics and Insider Threats
- Securing the Cloud
- Network Visibility
- Open Platform
- Deployment Options

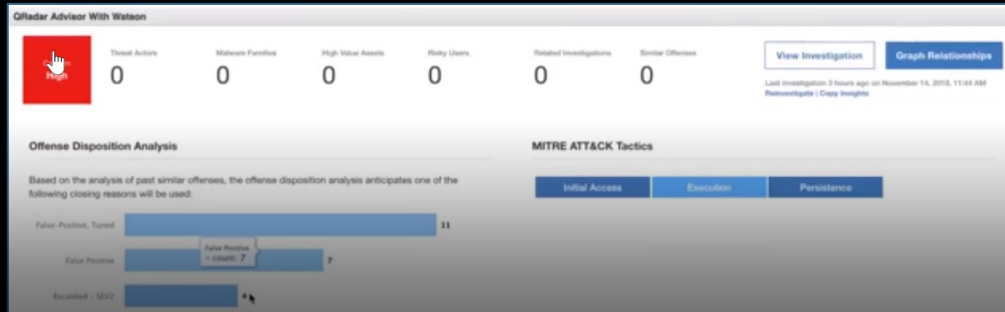
Advanced Threat Detection and AI : How can organizations...

Address these concerns:

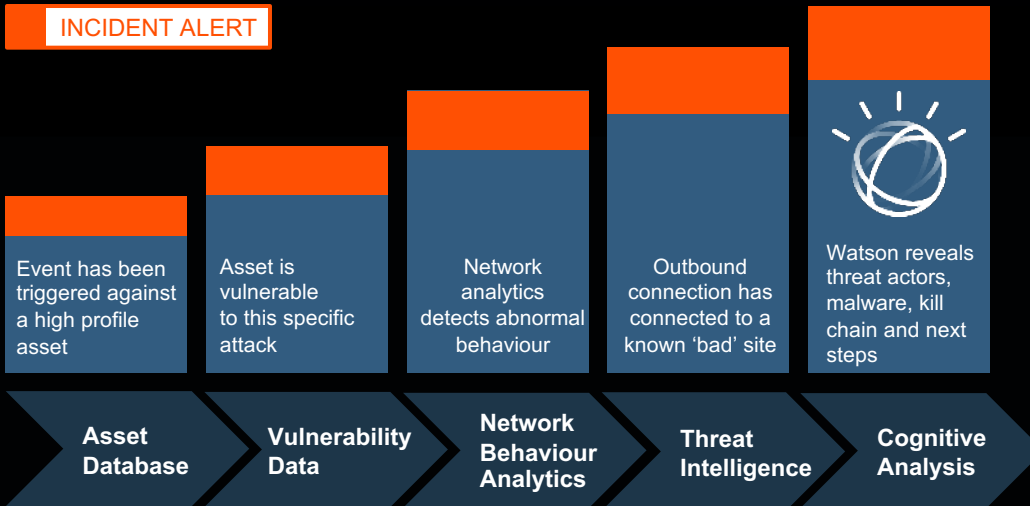
- Getting complete visibility across endpoint, network, cloud, user and application
- Identification threats in real time and escalate to identify the most critical ones to focus on
- Detection of long and slow attacks
- Avoid alert fatigue, analyst burnt out and missing threats



Advanced and persistent threats



INCIDENT ALERT



- **SINGLE, REAL-TIME ATTACK VIEW**
 - Intelligently gathers all attack related activities into a single pain of glass and updates in real time as attack unfolds minimizing noise
- **BUSINESS DRIVEN PRIORITIZATION**
 - Automatically adjusts severity based on business impact, and evidence as attack progresses
- **WATSON ANALYSIS**
 - Accelerates alert triage and threat discovery with cognitive incident analysis
- **COMPREHENSIVE INVESTIGATION**
 - Enables full forensics analysis of log, network PCAP, and Endpoint data from single screen

What do customers say ?

"WITH QRadar SIEM, NO MORE CYBER THREAT OR ATTACK !!!!"

Last Updated: January 12, 2019

[Email this page](#)

★★★★★ Overall User Rating

Product(s): QRadar SIEM

Overall Comment: "Cyber Threat Intelligence. To my biggest Surprise! QRadar SIEM and we were able to secure our data and reliable device in our company, it because QRadar SIEM is proactively monitoring and detecting threats."



Evaluation & Contracting



Service & Support

"When You Absolutely Positively Need To Find The Bad Guys, Get QRadar"

Last Updated: August 27, 2018

[Email this page](#)

★★★★★ Overall User Rating

Product(s): QRadar SIEM

Overall Comment: "a top-notch SIEM that has the unique ability to correlate time-series information with point-in-time events. It provides a comprehensive environment for threat modeling and asset management as well as vulnerability management. This is provided remarkable insights and resulted in detection and prevention of numerous penetration attempts."



Evaluation & Contracting



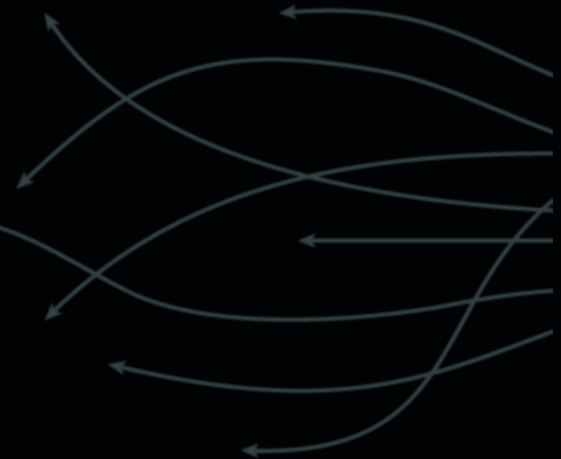
Integration & Deployment

"Within minutes of Watson installation, what normally took hours of analysis in mapping out the understanding of the identified offenses and threat now takes few minutes. That's allow an average of 50% or more improved response process"

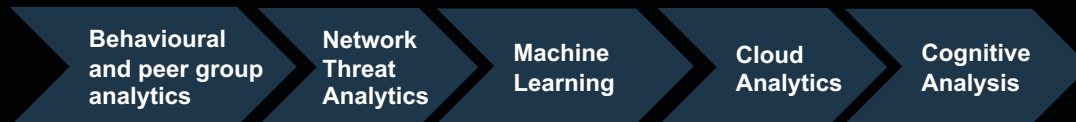
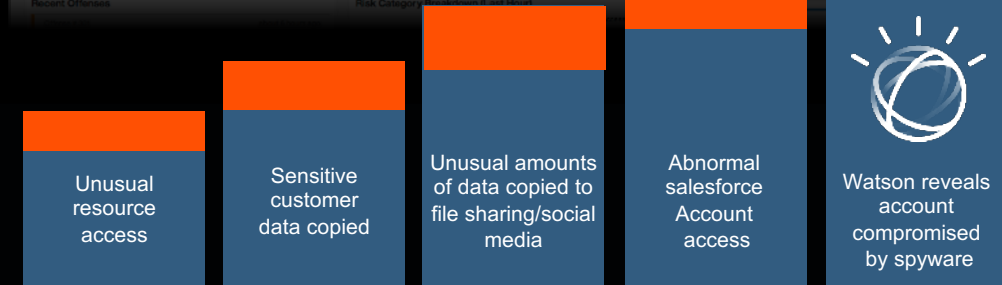
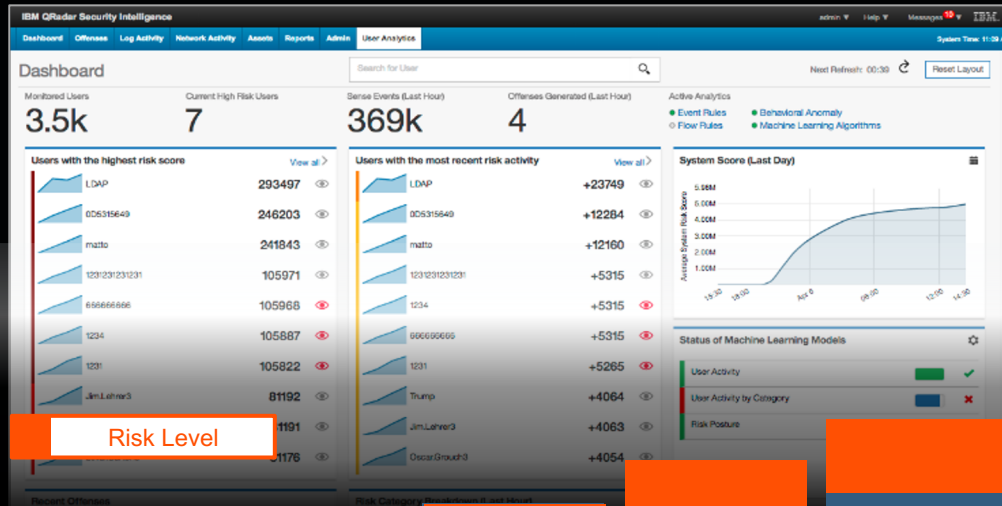
Insider Threats : How can organizations...

Address these concerns:

- Have credentials been stolen via phishing or malware account takeover
- Are credentials being misused
- Are there double earners and career jumpers stealing customer data and/or intellectual property
- Are users performing activities that are putting themselves and the organization at increased risk



Identify insider threats



- **IDENTIFY AT RISK USERS**
 - Account takeover, disgruntled employees, malware actions
- **STREAMLINED INCIDENT INVESTIGATIONS**
 - Immediate insights into risky user behaviors, action and activity history
- **360° ANALYSIS**
 - Performs analysis of activities at the end point, insights from network data, and cloud activities
- **FAST TIME TO VALUE**
 - Deploys in minutes from the IBM App Exchange and leverages existing QRadar data sets immediately

What do customers say ?

“UBA is extremely useful and I consider it a core part of the QRadar product functionality in order to maximize what it is capable of providing to an organization”

“We had to change our processes and carry out an internal audit because UBA was so effective at catching our Red team”

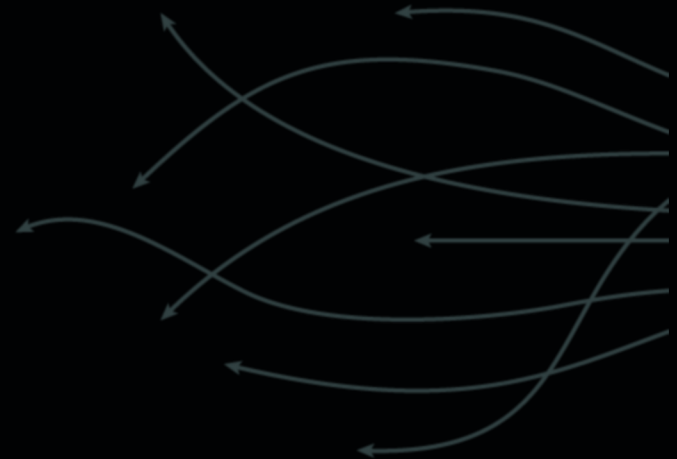
“Very good product, out of the box detects things that few other systems do”

“Solid Insight Quick time to value. Highly accurate alerts”

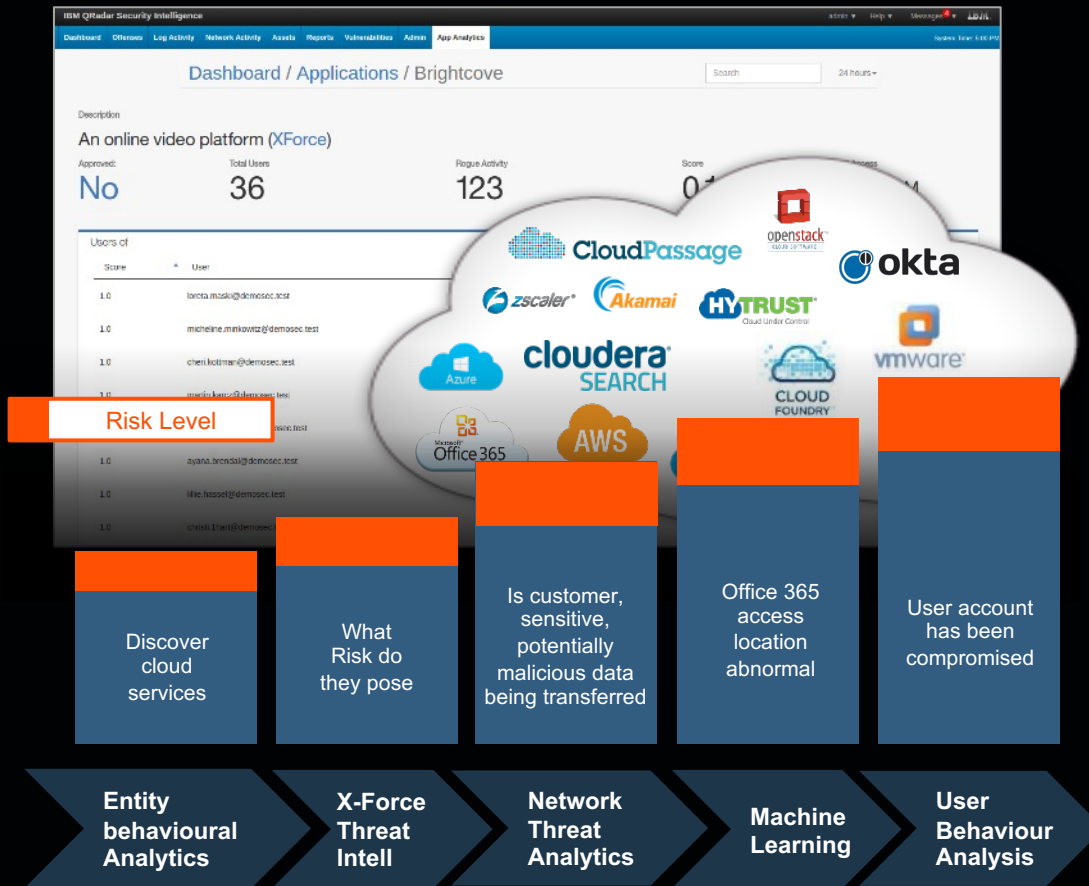
Cloud Security : How can organizations...

Address these concerns:

- What cloud services are being used and who is using them
- Identify malicious and suspicious activities in cloud services
- Insider threats and stolen credentials being used to access cloud services
- Copying of sensitive and customer data to unapproved cloud services



Securing the cloud



- **IDENTIFY CLOUD APPS BEING USED**
 - Analyses proxy logs, with threat intelligence from IBM X-Force, combined with asset and use data to determine who is using what, how much they are using, and how risky it is
- **BUSINESS APPS VISIBILITY**
 - Native cloud usage collection enabling visibility into what is going on in my environment (O365, Salesforce, AWS, etc.) and if it is malicious
- **QUICKLY FIND THREATS IN THE CLOUD**
 - Immediately discovers malicious activities in the cloud using out of the box analytics and Apps from the App Exchange

What do customers say ?

“IBM CISO and HSBC used Cloud Discovery and immediately detected Shadow IT application usage within their enterprises – both were very surprised at what they found”

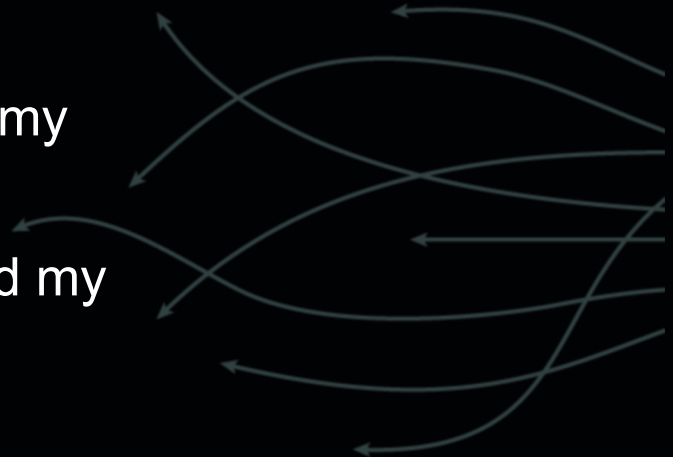
“We, The Chamberlain Group developed myQ software platform on Microsoft Azure. We added QRadar virtual deployment in Azure and Leveraged QRadar’s Event Hub integration to consume activity, infrastructure, and security logs and gain visibility into expanding cloud environment while maintaining an existing on premise security presence”

“Within Principal Financial, many separate business units and groups had independently migrated assets to cloud platforms (AWS, Azure, and Google Cloud) our CISO team was not alerted on these migrations – needed QRadar to extend into these cloud environments to better enable SOC analysts to provide security for expanding enterprise. We leveraged QRadar’s AWS and Azure integrations to ingest data from cloud log sources using cloud-native security findings from Amazon GuardDuty to supplement QRadar’s security analytics and correlation capabilities”

Network visibility : How can organizations...

Address these concerns:

- Have a record of everything that goes in and out or across my network
- What devices, assets, data and apps are on my network ?
- Are there any rogue users and apps misusing my network configuration ?
- Know about sensitive data movement around my network



Leveraging Flows

Visibility

QRadar Network Insights

QFlow

Netflow

Use Cases:

*Threat Hunting
Enhanced Threat Detection
Sensitive Data Detection*

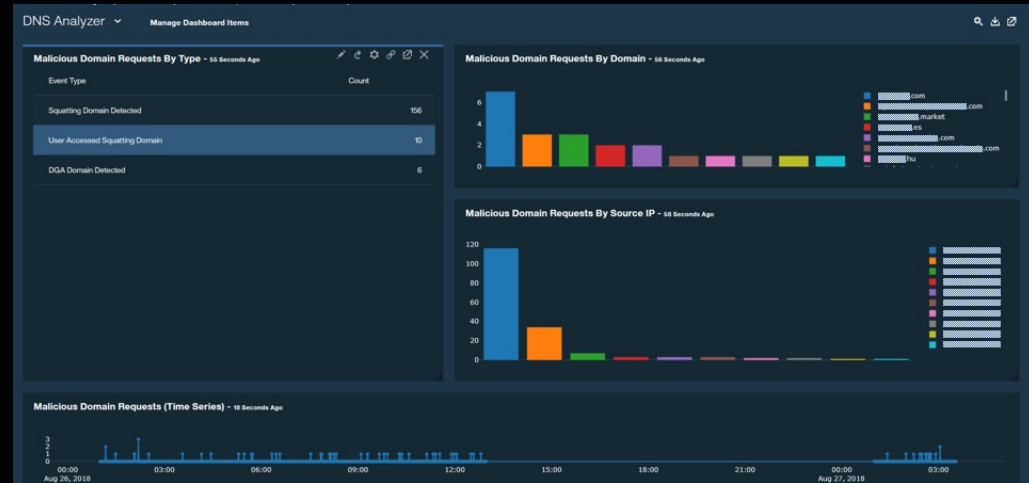
*Unauthorized Traffic
Visibility / Compliance
Protocol Misuse & Abuse*

*Anomaly Detection
Asset and Service Detection & Profiling
Full Record of Successful communication / Data transfer*

What do customers say ?

“We achieved the able to monitor East-West traffic and to be able to do DNS lookups, which is complicated in our heir environment...”

*“Immediately detected malicious DNS bypassing their DNS servers
...”*

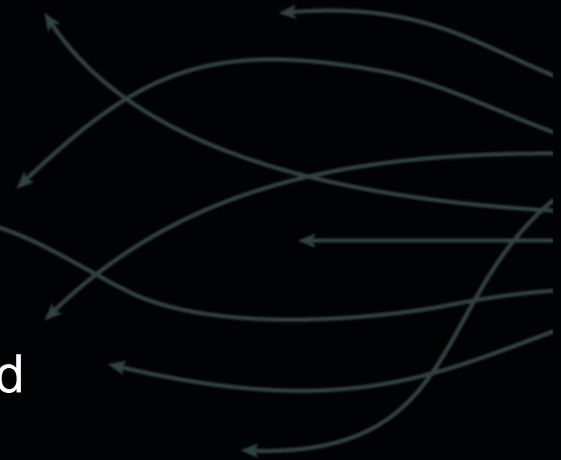


“We needed a way to ensure that sensitive customer data was protected in transit. Using QNI we now have the visibility to know how their data is being protected as it crosses their networks”

Eco System: How can organizations...

Address these concerns:

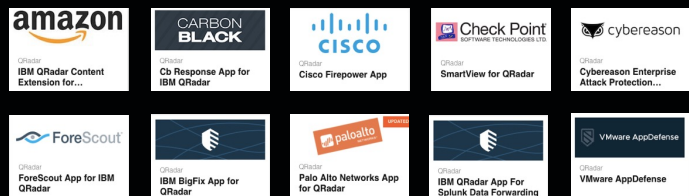
- The foundational platform of their SOC integrates with their existing infrastructure and investments, now and into the future
- Security staffing being consumed with integration work and context switching as they detect and investigate threats and risks
- That their SOC platform will be agile enough to respond to future requirements around data collection, threat detection analytics, workflow and visualization



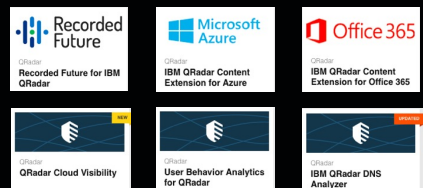
Open Platform

with hundreds of free integrations and content packs available via IBM Security App Exchange

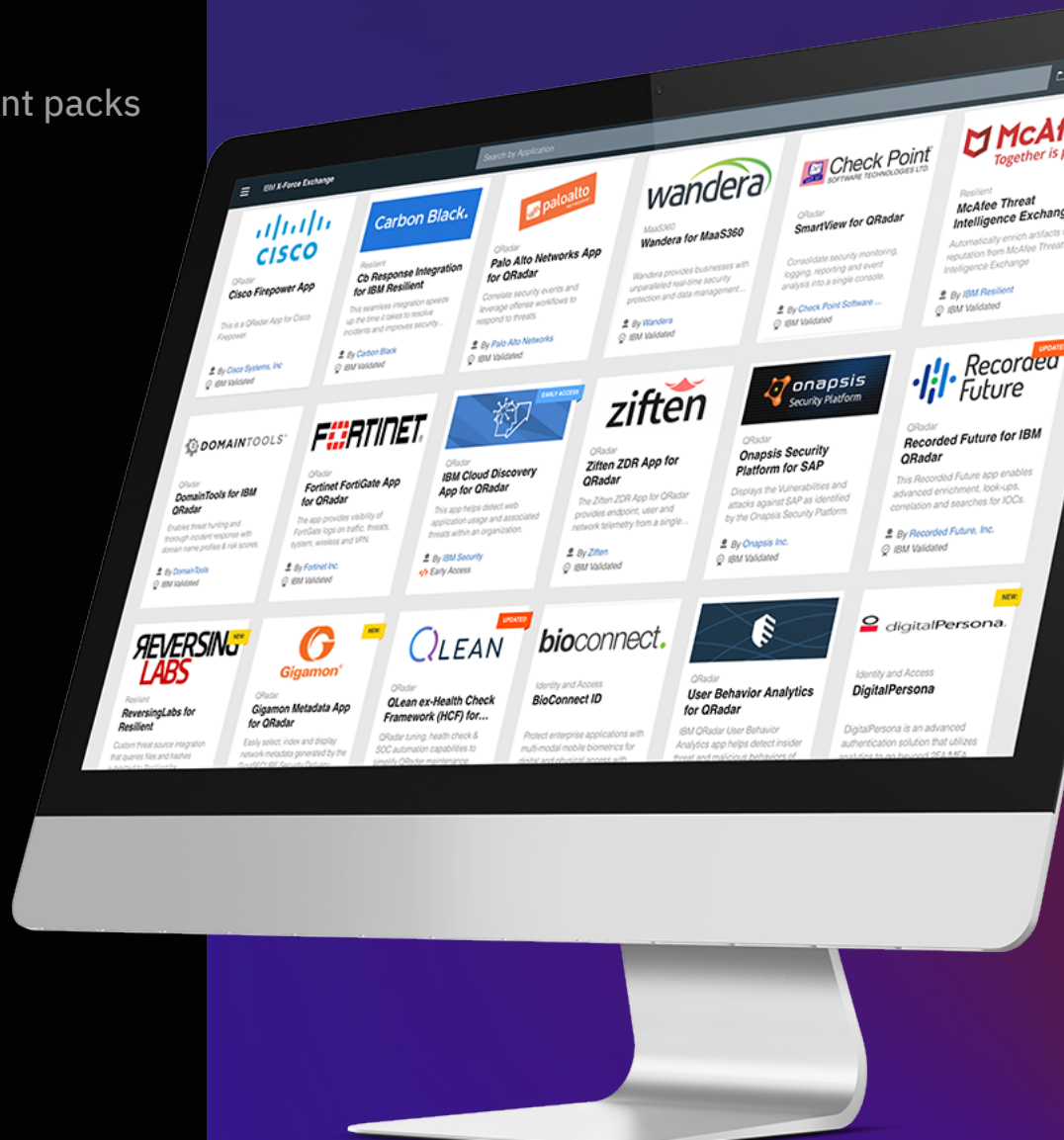
See Everything



Automate Intelligence



Be Proactive



What do customers say ?

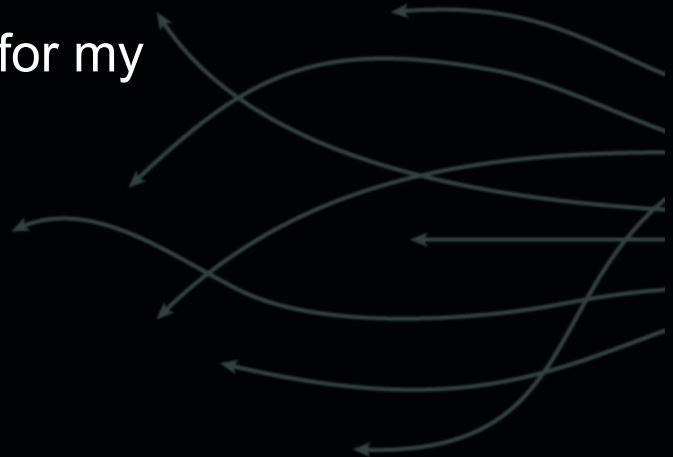
“The QRadar product has grown in features as we have used it. We started with just using it as a log aggregation tool for compliance but now use it for troubleshooting and security as well. With the opening up of the platform for custom applications, the product has become much more useful as we can mine the large store of data for user behavior and trends. Qradar Advisor and UBA from IBM, Carbon Black and Palo Alto, and our custom built applications have really enhanced our use of the Qradar product”

“As a provider a managed security services, we have been relying on QRadar for several years. QRadar and its growing ecosystem of components/ functionalities enables us to provide advanced services to satisfy demanding customers“

SOC Deployment: How can organizations...



Address these concerns:

- Align with my cloud and data center strategy
- Minimize cost and complexity of managing a big data systems (100's TBs/PB)
- Minimize internal IT charges and processes for my SOC platform
- No clear single vendor ownership for SIEM platform support



QRadar Deployment Models

Security Intelligence Platform

<p>ON PREM</p> <p>HW, SW, VM</p>	<p>FIS</p> <ul style="list-style-type: none">✓ Lost to LogRhythm 3 years ago (over committing, dropping price)✓ Came back to IBM 2 years later✓ Replaced 16 Log Rhythm appliances with a single Qradar server (xx48)
<p>AS A SERVICE</p> <p>QROC</p> <p>SaaS, Managed Service</p> 	<p>Ritchie Bros Auctioneers</p> <ul style="list-style-type: none">✓ The first customer meeting happened on a Friday✓ First QRoC demo was completed Monday✓ PoC up and running by Thursday✓ Beat Splunk they were in a PoC that failed✓ Customer quickly asked for the PoC to be turned into Production to meet SOX Compliance✓ Redeploying a planned FTE to other security imperatives rather than running a competitor's SIEM
<p>CLOUD</p> <p>AWS, Azure, Google Cloud</p> <p>HYBRID</p> <p>On-prem, SaaS, IaaS</p> 	<p>BRITISH TELECOM</p> <ul style="list-style-type: none">✓ McAfee deeply embedded in account✓ 3 years of demos, presentations, POC's✓ McAfee failed to deliver on AWS deployment✓ QRadar deployed 60k EPS system in two weeks✓ QRadar now the BT's primary goto market SIEM for their security services

Summary

- SIEM is a very active (and interesting !) market
- QRadar has proven ability to address all the current 'hot' use cases
- Customers looking for partnership, knowledge and leadership in these areas
- We are well down the track of investing in new and evolving use cases