IBM QRadar and Endace

IBM Security

Stay ahead of emerging threats with IBM Security and Endace Network History

Cybercriminals are more sophisticated than ever, and attacks on all types of organizations show no signs of slowing down. Endace and IBM Security have joined forces on the IBM Security App Exchange to help security teams combat growing threats using best-in-class solutions.

Combining IBM QRadar with EndaceProbe Analytics Platforms enables analysts to drastically reduce the time required to reconstruct security and network events, understand what's happened and take definitive action. In the QRadar console analysts can go directly from an alert to analyze the related recorded network traffic to see definitive evidence of what has taken place.

What is QRadar?

The IBM® QRadar® Security Intelligence Platform helps security teams accurately detect, understand and prioritize threats that matter most to the business. The solution ingests asset, cloud, network, endpoint, and user data, correlates it against vulnerability information and threat intelligence, and applies advanced analytics to identify and track the most serious threats as they progress through the kill chain.

QRadar allows analysts to:

- Gain comprehensive visibility into on-premises and cloud activity
- Easily view and understand the highest priority potential incidents, versus simply managing individual alerts
- Baseline and analyze asset, network and user activity to identify anomalies that may signal an unknown threat
- Correlate asset, network and user activity against threat intelligence and vulnerability data to identify known threats
- Seamlessly integrate an ecosystem of security solutions to gain greater capabilities from existing solutions
- Leverage artificial intelligence to automate and dramatically accelerate investigation processes
- Report on activities as needed for compliance purposes.

PRODUCTS

IBM QRadar

EndaceProbe with Application Dock

BENEFITS

- Analyze network traffic in real-time to detect and predict threats.
- Detect anomalous behavior that may signal an insider threat
- Neutralize threats quickly and efficiently with streamlined investigation workflows.
- Rapid, conclusive and actionable investigations with oneclick drill-down to packet-level detail.
- Easily extend security with QRadar apps from the Security App Exchange
- Deploy new security tools rapidly and on demand with EndaceProbe Application Dock.
- Reduce threat exposure through improved analyst productivity and faster incident investigation.
- Gain a complete, detailed history of network activity to quickly and easily re-trace an attacker's steps

What is the EndaceProbe Analytics Platform?

EndaceProbe™ Network Analytics Platforms capture, index and store network traffic with 100% accuracy while simultaneously hosting a wide variety of network security and performance monitoring applications in Application Dock™, EndaceProbe's built-in hosting environment.

Customers can extend their security monitoring capability by deploying security tools on demand, wherever EndaceProbes are deployed. Hosted instances can analyze recorded traffic in real time at full line-rate or analyze recorded Network History for back-in-time investigation.

Accelerating Security Investigations

The Network History recorded by EndaceProbes can be integrated into IBM QRadar using the Pivot-To Vision™ function of the EndaceProbe API. Pivot-To-Vision lets security analysts pivot from threat alerts in IBM QRadar directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History.

Using the IP address and time range of the trigger event, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts dissect, review and extract the relevant traffic from the terabytes of Network History recorded on the network with ease. Analysts can filter traffic, down to the microsecond level, Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

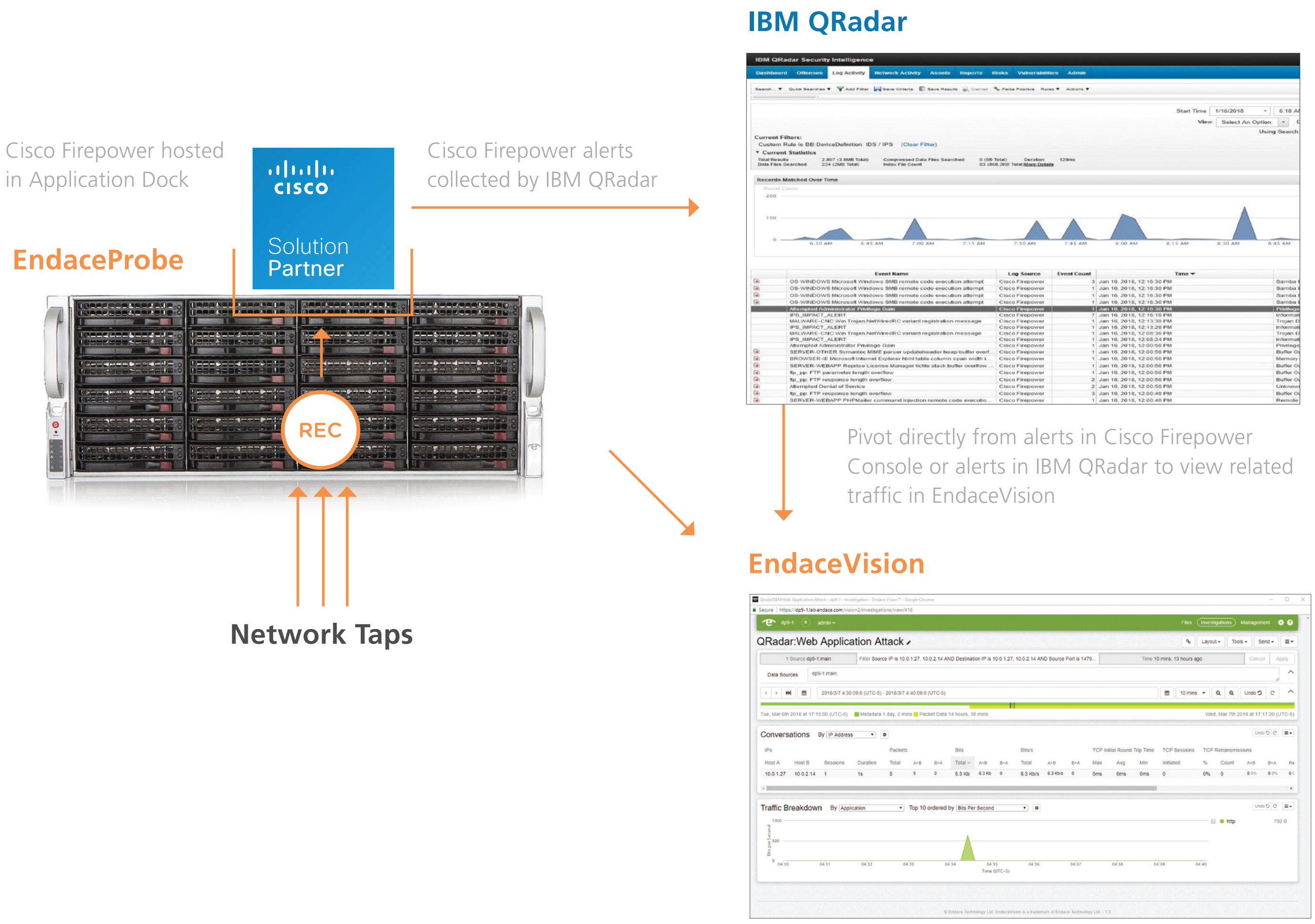
Single-click access to the related packets lets security analysts rapidly establish the root cause of issues, enabling them to act quickly and definitively to resolve critical incidents and to minimize the rest of security threats becoming serious breaches.

Conclusion

Deploying IBM QRadar with EndaceProbe Analytics Platforms allows analysts to extend security monitoring and network recording capability. Pivot-To-Vision allows analysts to drill down into QRadar alerts for the definitive evidence needed to act quickly and decisively.

The combination of Endace and IBM provides state-of-the-art network security management and 100% accurate Network History to give analysts a complete view of what's happening on the network.

Example Configuration with Cisco Firepower and IBM QRadar



IBM QRadar

Cisco Firepower hosted in Application Dock

Cisco Firepower alerts collected by IBM QRadar

EndaceProbe

Pivot directly from alerts in Cisco Firepower Console or alerts in IBM QRadar to view related traffic in EndaceVision

EndaceVision

Network Taps

cisco
Solution Partner
REC
IBM QRadar Security Intelligence
QRadar:Web Application Attack
Conversations
Traffic Breakdown

CE RoHS Compliant c UL us

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.

Endace™, the Endace logo and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com