ExtraHop | Tetration Analytics™

Cisco Tetration & ExtraHop: Real-Time Analytics for Security Policy Enforcement

Take fast action against threats like ransomware and brute force login attempts by combining real-time application (L7) visibility and machine learning capabilities from ExtraHop with Tetration's powerful security policy enforcement.

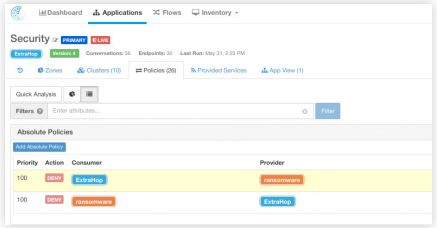
Essential threat detection and security policy enforcement from the datacenter to the cloud to the edge

The Cisco Tetration and Extrahop Open Data Stream integration combines real-time application layer visibility from ExtraHop with Cisco Tetration's automated policy enforcement in order to simplify zero-trust implementations, detect anomalous network behavior, and automatically trigger enforcement policies – ultimately, delivering a new layer of valuable context through real-time application-level visibility which reveals the specific activity behind abnormal network traffic patterns.

This allows you to analyze and baseline traffic behavior so that you can solidify your security policies and micro-segmentation plans: Segment your application servers from your database servers and external clients; apply appropriate firewall policies at your endpoints immediately and automatically; and thwart major threats like ransomware with the industry's most targeted, accurate, and rapid security policy enforcement.

How it Works

This integration delivers both powerful insight, as well as the ability to detect incidents including brute force logins, ransomware attacks, and expired certificates. Deep analysis of packets flowing between applications ensures the detection of security issues in real time. A perfect example is the ability to detect ransomware attacks and tag a compromised host. Tetration can then enforce a restricted security policy on that host. This integration can be realized by having an ExtraHop ransomware detection trigger call to the Tetration REST API to apply the custom tag.



Key Features

Industries most targeted, accurate, rapid security policy enforcement

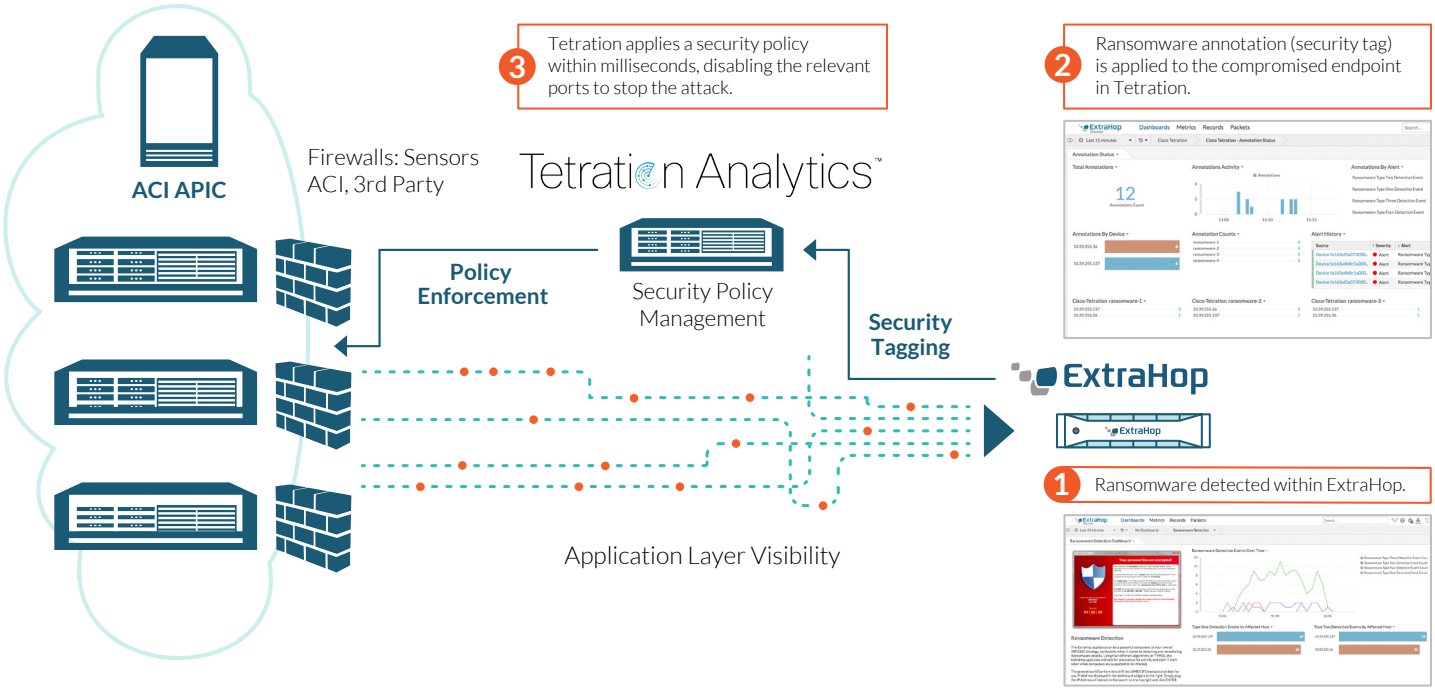
Tetration can apply security policies at endpoint sensors, ACI, or third-party firewalls. These security policies can be enhanced with custom tagging to provide additional context. Tetration's endpoint sensor machine metrics (L2-L4) combined with ExtraHop's L7 application layer visibility can provide a much deeper context to support better custom tagging for security policy enforcement.

ExtraHop | Tetration Analytics™

Cisco Tetration & ExtraHop: Real-Time Analytics for Security Policy Enforcement

Use Case

Application Level Attacks	Example: Ransomware • ExtraHop tags a compromised host • Tetration enforces a restricted security policy on that host • ExtraHop Ransomware detection trigger calls the Tetration REST API to apply the custom tag
Brute Force Logins	• Users have the power to both detect a spike in database traffic and determine whether the traffic spike is due to brute-force login attempts, along with which specific tables are being queried
Ransomware	• Examine CIFS traffic to spot ransomware and automatically tag compromised hosts to stop the spread of the attack.
Certificate Audits	• Identify specific server or servers on which the certificate has expired • Identify rogue certificates
Cipher Audits	• Identify specific server or servers with weak cipher suites
Network Forensics	• Users have access to detailed application transactions and packets to determine circumstances of incident



Next Steps

For more information about the Cisco Tetration and ExtraHop integration, please visit www.extrahop.com/company/tech-partners

To follow up directly with the ExtraHop sales team, email us at sales@extrahop.com