Corvil | Cisco Tetration Analytics™

DYNAMIC DATA CENTER SECURITY AND SERVICE ASSURANCE

CHALLENGE

SECURITY AND PERFORMANCE ACROSS DYNAMIC INFRASTRUCTURES

Today's business transactions and applications span a broad and ever-changing array of physical and virtual infrastructures across data center and hybrid cloud deployments. Increased infrastructure dynamism combined with DevOps-driven application changes has made it more challenging for organizations to understand how applications are performing in support of the business and to assure their delivery, performance, and security.

Static, perimeter-based security models and log data sources are no longer adequate to protect against attacks and to gain actionable insight into infrastructure and application service delivery. With the majority of cyberattacks carried out by inadvertent or malicious insiders, organizations must continuously monitor and analyze the behaviors of application communications and users and take rapid action where required.

Often problems are caused by the complex and ever-changing interactions between different service components. Operations teams are challenged by:

- Limited understanding of current and historical business transaction and application communication
- Isolation of root cause of problems across dynamic infrastructures
- Designing and enforcing application segmentation and security policies
- Understanding how dynamic application and network services are impacting customer experience

Understanding dynamic environments demands richer information generated by continuous analysis of diverse and granular data sources.

SOLUTION OVERVIEW

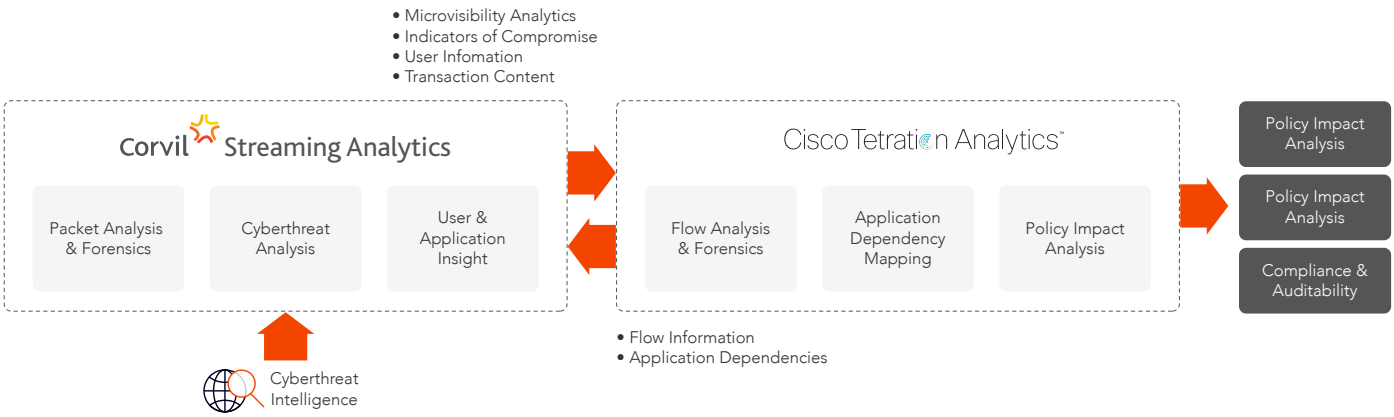
ENRICHED COMMUNICATIONS ANALYSIS FOR DYNAMIC INSIGHT, POLICY ENFORCEMENT AND RESPONSE

Corvil complements Cisco Tetration Analytics by enhancing the L2-4 flow-based information with richer details obtained through Corvil's continuous real-time application-level analysis of packet data. By enriching Tetration Analytics with Corvil's unique visibility, customers gain the ability to better understand application dependencies, to develop more detailed and effective policies for security enforcement and application segmentation, to save time for operations teams, and to provide better protection for their business.

BENEFITS

- More detailed and effective policies for security enforcement and application segmentation
- Additional context to annotate Tetration's network flow analysis and inform application policy and security orchestration
- Faster and more comprehensive detection and diagnosis of performance issues by combining advanced flow and packet analysis
- Improved user experience optimization combining application flows with deeper transaction content analysis

> *"The depth and insight from Corvil analytics combined with Cisco's Tetration Analytics will provide richer understanding of workload characteristics, improved detection of evasive security threats, and more effective transaction insight. This type of integration is needed to drive tighter alignment between network, application, security, and business teams."*
>
> EMA™



Corvil's integration with Cisco Tetration Analytics seeks to deliver increased security and performance for business applications through dynamic policy enforcement, response, and visibility. The combination provides for:

- Expanded data sets for visibility and analysis across network and applications
- Rich, historical big data set for forensics, historical activity and trending
- Dynamic response for automation, service improvement and security response

Corvil provides information to annotate Tetration Analytics flows in four key areas: Service Assurance, Cybersecurity, Application Dependencies/Behaviors, and Business Transactions with future phased collaboration focused on delivering dynamic responses.

INTEGRATION AREAS OF CONTINUED FOCUS AND FUTURE DEVELOPMENT

CATEGORY	ANALYTICS	ACTIONS
Service Assurance	Machine-time analysis Packet decoding	Workload orchestration Application segmentation Error code specific reaction
Cybersecurity	Indicators of compromise Suspect user activities	Host quarantine Application policy updates
Application Dependencies	User response times Multi-hop/tier performance benchmarking	Information updates Policy enforcement
Business Transactions	Real-time user/customer identification Business-relevant transaction classifications	QoS service profiling Transaction flow reporting

cisco | Cisco Tetration Analytics™

The Cisco Tetration Analytics™ platform addresses important data center operational and security challenges by providing behavior-based application insight, automating policy generation, and enabling zero-trust deployment using application segmentation.

Corvil

Corvil is the industry leader for deriving IT, Security, and Business intelligence from network data. As companies adopt faster and smarter machine technology, it becomes critical to tap into richer and more granular machine data sources to safeguard the transparency, performance and security of critical infrastructure and business applications. The Corvil streaming analytics platform captures, decodes, and learns from network data on the fly, transforming it into machine-time intelligence for network, IT, security and business teams to operate efficiently and securely in this new machine world. Corvil uses an open architecture to integrate the power of its network data analytics with the overall IT ecosystem providing increased automation and greater operational and business value outcomes for its users. The Corvil solution is trusted by leading financial institutions to safeguard their businesses across the globe involving 354 trillion messages with a daily transaction value in excess of $1 trillion.

CDS-240617