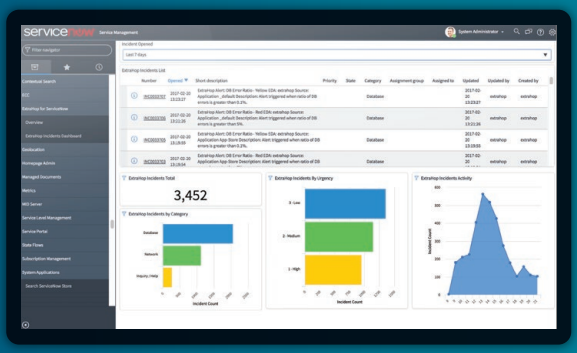
ExtraHop | servicenow

ExtraHop + ServiceNow Integration Brings Together Automated Discovery & Visibility with IT Service Management



REAL-TIME DATA MEETS INTELLIGENT CMDB

- Automate ticket creation for detection
- Trigger workflows based on events in your environment
- Discover and quarantine unregistered devices and insecure communications

ServiceNow delivers best in class IT service management that eliminates inefficiencies and allows IT to do more.
By combining real-time wire-data analytics from ExtraHop with intelligent IT services management from ServiceNow, IT organizations can operate with greater efficiency than ever before to keep critical business services up-and-running, and supports a secure digital experience for all end-users.

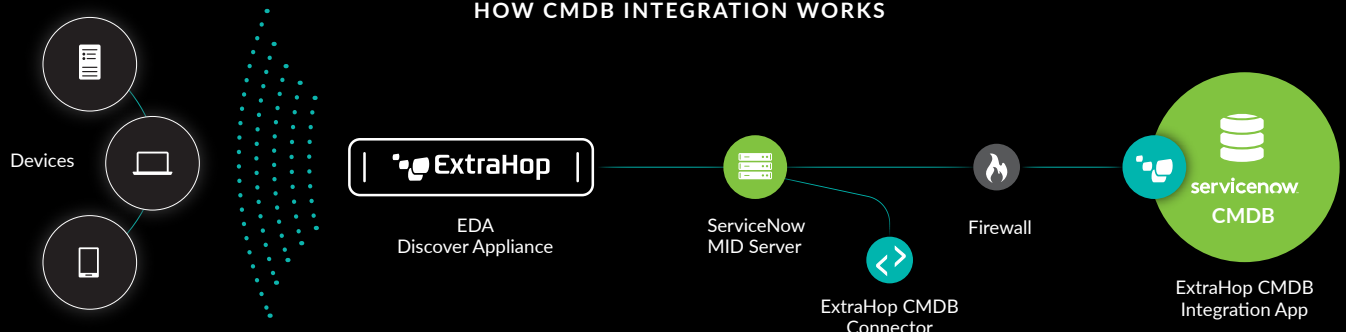
EXTRAHOP + SERVICENOW CMDB INTEGRATION

Real-Time Network Device Discovery

ExtraHop automatically discovers devices passively, with no agents or special authenticated access required. New discoveries and updates with broad, rich context are immediately sent to the ServiceNow CMDB in real time, including updates about all devices that are auto-discovered and auto-classified by your Discover appliance on your network. ExtraHop and ServiceNow allow a faster time to CMDB readiness, enabling responsive, agile IT and security for the business.

INVENTORY AUDITS | SECURITY AUDITS | LICENSING AUDITS | CHANGE MANAGEMENT

HOW CMDB INTEGRATION WORKS



- Passive discovery. No agents or special authenticated access framework required.
- Automatic discovery and updates to the CMDB.
- Accurate, real-time device and application contextual data added to the CMDB. The network is the source of truth.
- Broad device and application context added to CMDB.
- Web servers, database servers
  - Application versions
  - SSL rogue, expired certs, ciphers

ExtraHop | servicenow

Scale Your Security & IT Operations:
BI-DIRECTIONAL INTEGRATION OF DETECTIONS, ALERTS AND TICKETING

ExtraHop Ticketing App for ServiceNow

Speed incident resolution with seamless integration between network traffic analysis detections and automated response workflows:

- Improve Reveal(x) triage and investigation with visibility into ServiceNow ticket status
- Enrich ServiceNow alerts and incidents with network events, detections, and anomalies
- Supercharge IT Orchestration for automated rapid response in case and ticket management

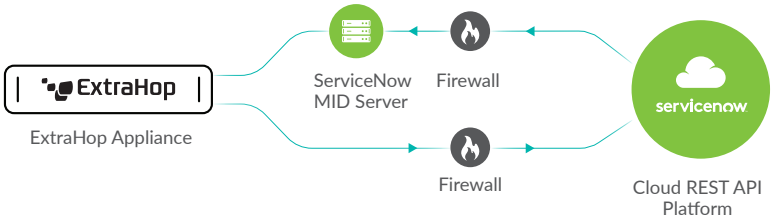
Security Analysts can now monitor ticketing status in real-time within their investigative workflow: The bi-directional Integration of ExtraHop Detections and ServiceNow Alerts and Ticketing now make it possible to initiate a ticket and then monitor an issue's status in real time. Within the Reveal(x) workflow, analysts can see if detections, associated ServiceNow alerts, and events are NEW, IN PROGRESS, or CLOSED and are linked directly to the ServiceNow Alert ticket. This knowledge helps the analysts direct energy efficiently in their investigative workflow. For instance, new events might merit immediate attention, in progress events might be ignored, and a closed incident might need to be revisited to see if an attack has re-occurred or perhaps wasn't fully investigated.

Bi-Directional Integration streamlines and automates response workflows: Automated ticket creation and remediation actions on your ServiceNow instance as a response to ExtraHop detections will help you to supercharge IT Orchestration in ServiceNow. Wire data collected from ExtraHop also provides additional telemetry for ServiceNow's intelligent algorithms to automate your IT Operations.

ServiceNow tickets are now connected to ExtraHop detections: The integration sends alert updates from ServiceNow to ExtraHop via REST APIs to ensure detections and resulting tickets are always up to date.

THERE ARE THREE COMPONENTS USED BY THE TICKET INTEGRATION SOLUTION:

1. ExtraHop Solution Bundle for ServiceNow Ticketing Integration
2. On-Prem MID Server (Supplied and supported by ServiceNow)
3. ServiceNow App that lives on ServiceNow Cloud REST API Platform



ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they can compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, organizations can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com