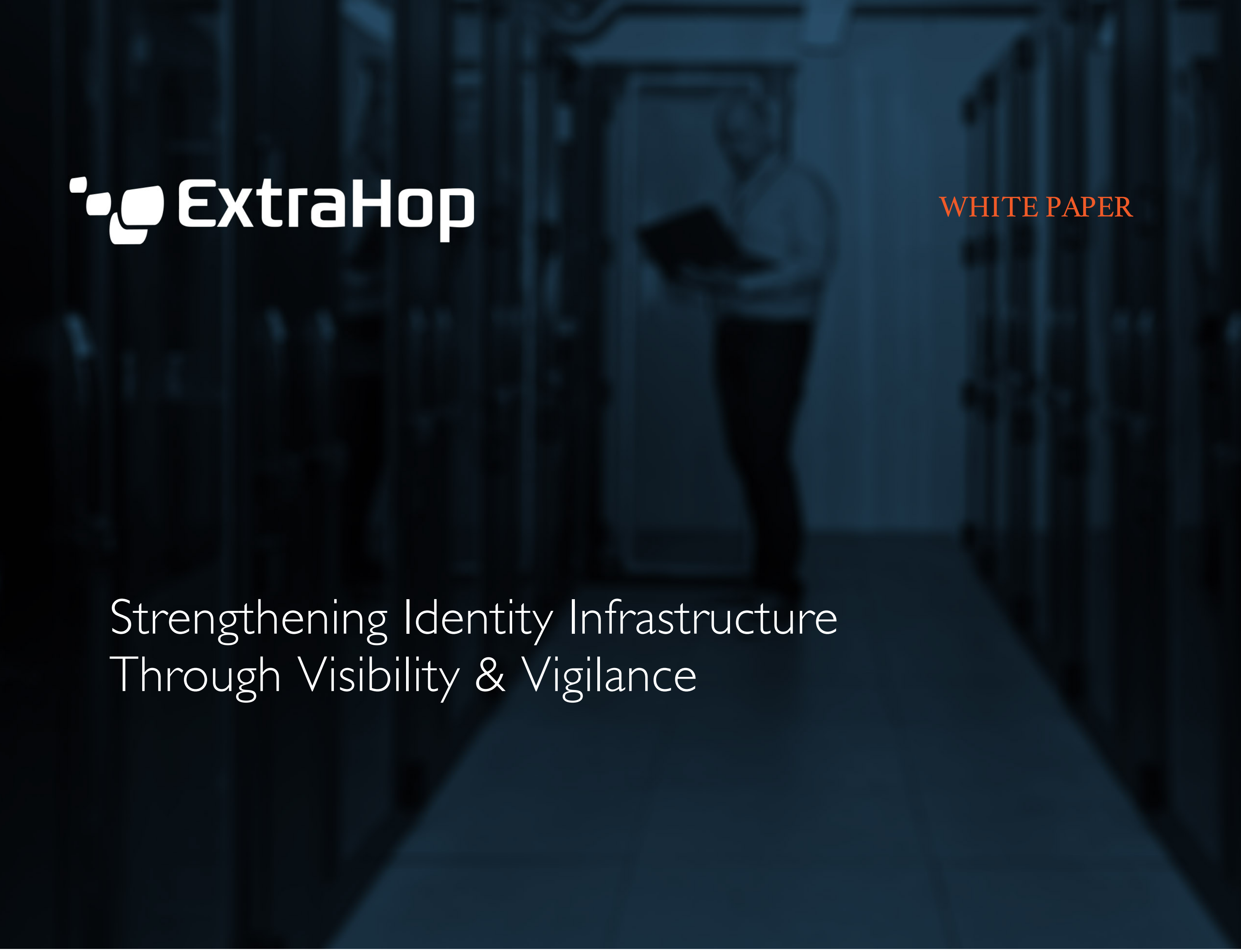


ExtraHop

WHITE PAPER

Strengthening Identity Infrastructure Through Visibility & Vigilance

Abstract

Few things are as essential to organizational health as identity infrastructure, which has greatly increased in importance because of new service models. To take control of your identity infrastructure, greater visibility into its health and function is critical. The ExtraHop platform allows organizations to cut complexity and regain control of IT services, including identity systems, by unlocking the hidden value in data flowing through your network. You can see which systems and users are not adhering to prescribed policies, detect anomalous behavior such as brute-force attacks in real time, and audit security events after the fact to determine who accessed what and when. This paper will explain how wire data can be used to address persistent identity management issues that often plague complex IT environments and how real-time visibility can strengthen your identity infrastructure and therefore the entire organization's security posture.

How Did We Get Here?

As more and more business functions go digital, identity infrastructure plays a role of the utmost importance. A poor implementation can block users from needed resources, lead to widespread outages, create an infuriating workflow to access essential services, or worst of all create the appearance of protection where there is none. Contrast this with a dynamic identity solution that allows employees to access needed documents from anywhere, enables new customer and partnership business models, simplifies their lives by adding single sign-on (SSO) and limits exposure to risk while ensuring compliance objectives. In short: getting identity right matters a lot.

When Directory Services were first introduced at the onset of the datacenter server and client model, the scope of what they were intended to manage was much different. There were fewer users, identities were usually tied to a single console, and an application was self-contained in a single server. Now, even the most basic of services must deliver at scale. Users choose from many devices (sometimes even concurrently), and the applications interact with myriad patchwork systems, APIs and cloud services. To put it simply, these aren't your parents' identity services.

When so much is riding on this critical service, its important to establish an effective strategy for your identity infrastructure and then manage against it. Failure to do so will lead to poor customer experience, leave the organization exposed to massive losses due to outages or attacks, and create a barrier to innovation in IT service delivery that's vital to the business.

An Identity Primer

Before we go too far we should land on a loose set of definitions of terms that show up in this paper.

IDENTITIES: Defined permissions that are tied back to a set of credentials that work with the security infrastructure. Identities can be established for a user, device, service, or a combination of these characteristics. In some use cases, such as IoT, they can also be defined by a session ID.

PRIVILEGED IDENTITIES: These are the most critical accounts that organizations have. Often they are given elevated permissions, which are necessary to complete a specific task. When major breaches occur it is usually as a result of bad actors gaining access to these accounts.

CREDENTIALS: The token or key presented and validated by the system to grant access. The traditional form of this is the user ID and password system. As more and more accounts have become compromised, organizations have become more creative in how they handle this area, things like: key fobs, chip-and-pin technologies, cryptographic certs, or other multi-factor authentication solutions have become common.

DOMAINS OR REALMS: Think of a domain as a perimeter that helps define the security of the environment. Typically there will be a group of users, systems, and services that are sharing different resources within this trust hierarchy and governed by a common security policy.

FEDERATION: Allows end users to use their credentials to access applications and systems outside the corporate firewall, or to join multiple Directory Forests. This has become a critical requirement for modern IT as mergers & acquisitions lead to more complexity in the environment. It is also vital when users need to access SaaS applications or partners' systems.

ACCESS CONTROLS: On the back end we have a series of management policies defined. You can use group- or role-based access controls that will control user-permissions based on relationships. This can affect who has access, as well as what level of access an individual or group has. Fine grained controls can lower risk, but also can make it more challenging to be agile and meet business needs.

SECURITY CERTIFICATES: If a security certificate has expired, access controls will often step in and disallow a connection between the device, user, or service and the other end of that connection. This is a common point of failure, especially with cloud services and 3rd party services.

SINGLE SIGN-ON: is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications.

Building an Identity Solution With a Feedback Loop

Initial Policy Definition

The foundation of your identity solution will be in the definition of policies and how you choose to enforce them. So, lets talk about creating an identity management framework. This is the first step in determining what your environment should look like. There are several vendors and governing bodies with prescriptive models that can help you establish a strong framework. ExtraHop can operate alongside any of these models, but explaining the models themselves is beyond the scope of this paper. If you are still defining your policy you can pick up some foundational knowledge from the National Institute of Standards and Technology (NIST) a non-regulatory federal agency of the United States. Their model can be found here. You can also look to companies like Microsoft or Okta for examples of frameworks.

Business considerations should be weighed alongside security objectives and regulatory requirements when defining your approach. A few helpful tips:

1. Identities are not all created equal. You should consider stronger access controls for privileged identities that enjoy elevated permissions.

2. If your organization has multiple domain forests, federating them on the front end could save you substantial time managing on the back end.

3. When establishing policies, you should create a consistent experience and user education about identity best practices to avoid confusion. Consistent policies also reduce weak points in defense or gaps in coverage that can be exploited.

4. User education is an enormously important part of identity and access management. Users need to understand the correct way to use and protect privileged credentials and sensitive data. This means everything from not writing passwords on sticky notes to recognizing phishing scams and more.

5. Standardizing around multi-factor authentication and leveraging single sign-on can be a great way to meet business objectives for speed and simplicity while providing the appropriate level of protection.

6. Stale credentials are the bane of good security models. You can invest as much infrastructure as you want to, if you don't implement processes that police users credentials and ensure they are adhering to your policies, then your policies are no good.

7. Security certificates are an important topic often neglected in the identity and access management conversation. Keep them current or you'll be sorry.

8. You need a practice of regular auditing and monitoring of identity infrastructure, and a corresponding reporting structure. This is one spot where ExtraHop can be invaluable.

Establishing Baselines

Setting a baseline for behavior in your IT environment is vital. By understanding what is normal, and comparing that to what's happening at any given moment, you greatly increase your chances of noticing anomalous, possibly malicious behavior before it becomes an emergency. Comparing activity against a baseline manually is a ton of work, and as environments have grown more complex even the best funded and supported security teams are taxed by potential threats. Identity solutions have traditionally been a great way to reduce the workloads of those keeping a watchful eye on the domain by automating much of this work. That, however, isn't enough to protect against many common threats:

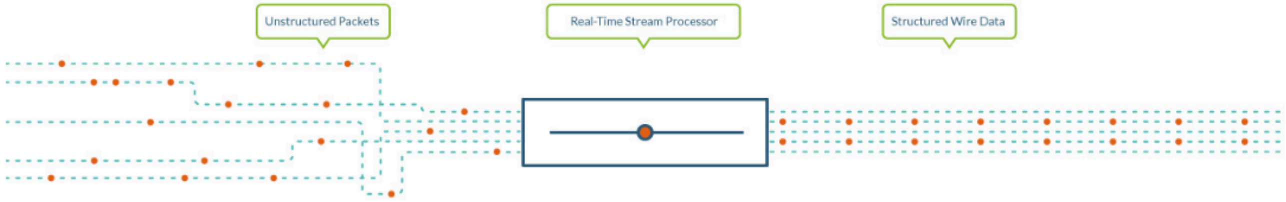
- What happens when access controls are misconfigured?

- How do you account for insider threats that operate within the confines of their permission levels?
- When credentials are compromised, how do you know?
- When one system is compromised how do you contain the threat?

Answering these questions becomes much easier when you have a robust monitoring solution in place that provides visibility into the identity infrastructure, and correlates behavior across all other systems to spot threats before they become escalated incidents.

That's Where the ExtraHop Platform Comes In

The ExtraHop platform is a simple turnkey solution that enables you to make sense of all data passing over the network. All applications transact on the wire, and all technology communicates on the wire. If you want to gain visibility and control risk, it all starts there—analyzing your data while it's in motion.



Wire data comprises L2-L7 data spanning the entire application delivery chain. Through full-stream processing, unstructured data is reassembled into structured wire data that can be analyzed in real time and mined for insights.

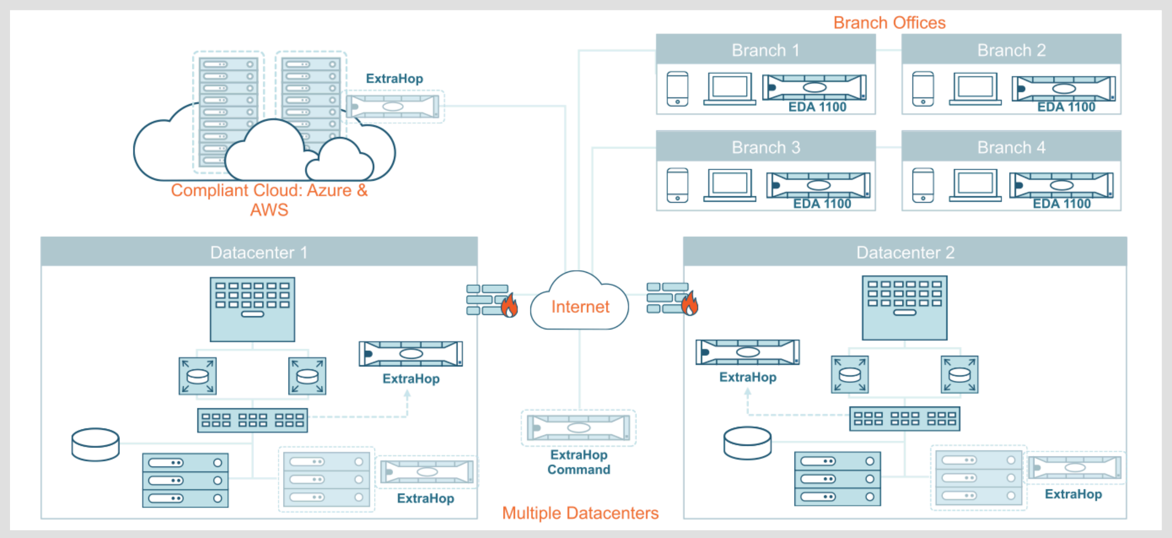
Data in motion across your network is inherently more current, and therefore contains more relevant insights, than data at rest, which is the information that you've stored to analyze later. Your data in motion is the most valuable source of information that your organization can mine for insights. But to access your data in motion, you need a platform for transforming large volumes of unstructured network packets into structured wire data. The ExtraHop platform is built to do exactly that at unprecedented scale.

It is important to understand that the ExtraHop Platform is a completely passive solution, requiring no agents, no host configurations, and no credentialed access. It will provide comprehensive visibility into the transactions occurring within your network with no degradation or disruption to the existing system, applications, or users. It will not actively interrogate any devices, nor will it open additional ports, start new services, or add any additional traffic to the network it is monitoring.

Enterprise-wide Visibility

As an information security professional, you can't live with reduced insight due to increased scale, dynamism, and complexity in your environment. Limited visibility leads to a loss of compliance control, inability to assess and report, data breaches, and frustrated analysts.

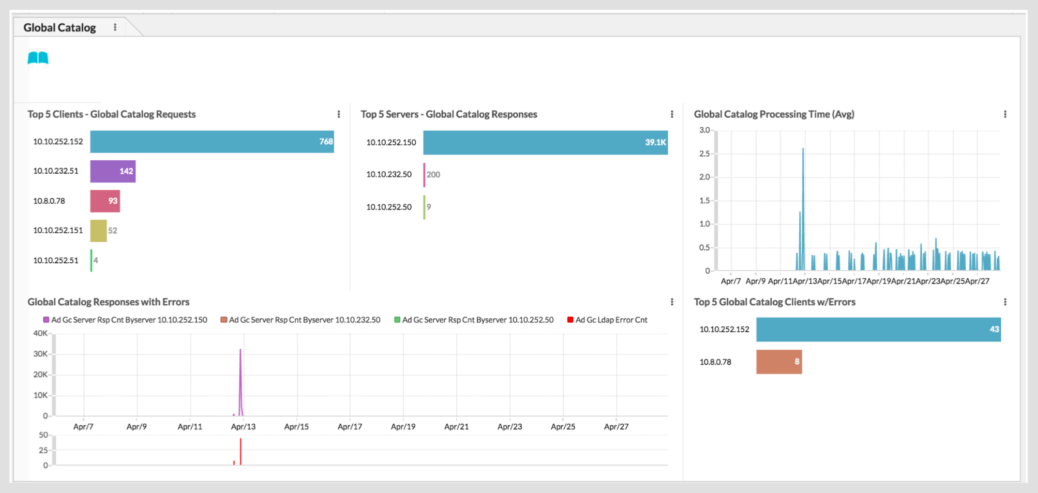
The ExtraHop platform can provide insight across a large geographically dispersed enterprise for a holistic view of all wire transactions throughout the network. The approach is simple and scalable, whether the network to be analyzed is physical, virtual, private or public cloud. ExtraHop can be deployed in a heterogeneous environment without issue. The connectivity between the ExtraHop appliances is secured via SSL (TLS 1.2) and uses very little bandwidth, making it a great choice for remote sites that have minimal wide-area connectivity.



The ExtraHop platform supports traditional datacenter deployments as well as the public and private cloud.

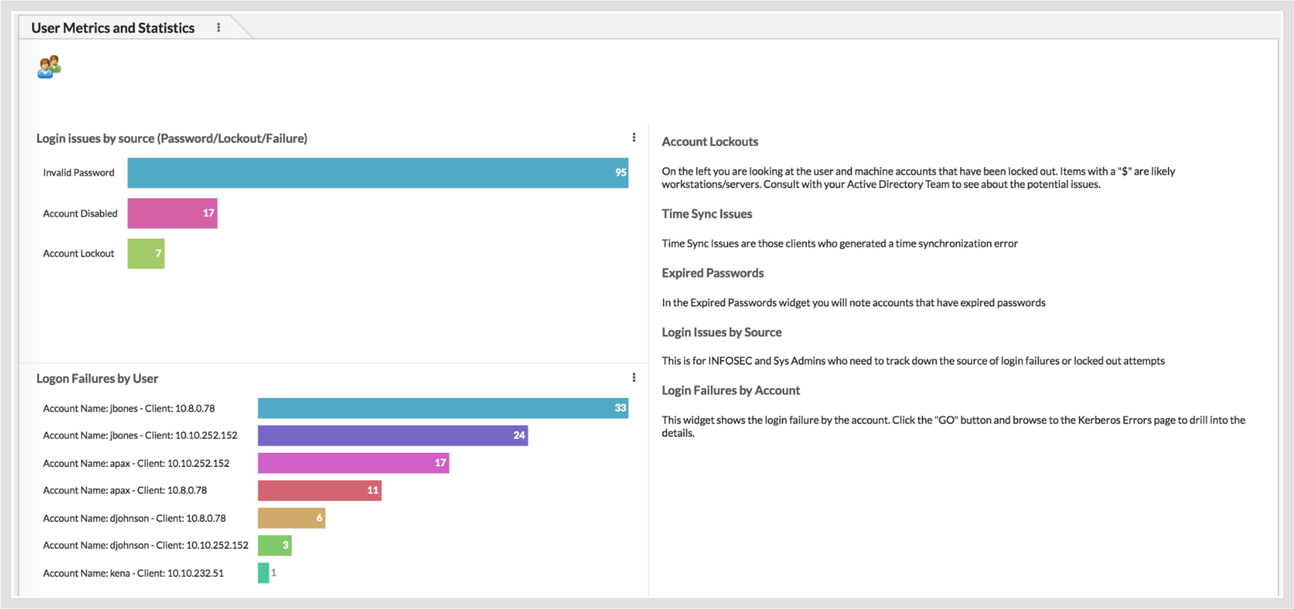
Continuous Observation of Identity Infrastructure

With ExtraHop, you can analyze the systems that makeup your identity solution and gain rich insights at every layer, such as the Global Catalog, Key Distribution Center (Kerberos), LDAP, DNS, and Group Policy. By being proactive in your monitoring of this critical infrastructure you can strengthen it's health and detect early warning signs of risk.



Real-time visibility into the Global Catalog with full payload analysis

Gain an understanding of authorization issues before having to investigate a potential security incident by tapping into Key Distribution Center metrics that are being delivered through Kerberos. See every time a computer or user requests access to a resource, and the exchange of credentials. Since these credentials are established for machines in addition to user and service accounts it is common to experience issues where a failure isn't reported, which can leave you with a service disruption or a security issue. Conversely, having access to this information by gaining visibility from ExtraHop into Kerberos can let you know which services are impacted.



User Metrics and Statistics

Login issues by source (Password/Lockout/Failure)

Invalid Password	95
Account Disabled	17
Account Lockout	7

Logon Failures by User

Account Name: jbones - Client: 10.8.0.78	33
Account Name: jbones - Client: 10.10.252.152	24
Account Name: apax - Client: 10.10.252.152	17
Account Name: apax - Client: 10.8.0.78	11
Account Name: djohnson - Client: 10.8.0.78	6
Account Name: djohnson - Client: 10.10.252.152	3
Account Name: kena - Client: 10.10.232.51	1

Account Lockouts

On the left you are looking at the user and machine accounts that have been locked out. Items with a "$" are likely workstations/servers. Consult with your Active Directory Team to see about the potential issues.

Time Sync Issues

Time Sync Issues are those clients who generated a time synchronization error

Expired Passwords

In the Expired Passwords widget you will note accounts that have expired passwords

Login Issues by Source

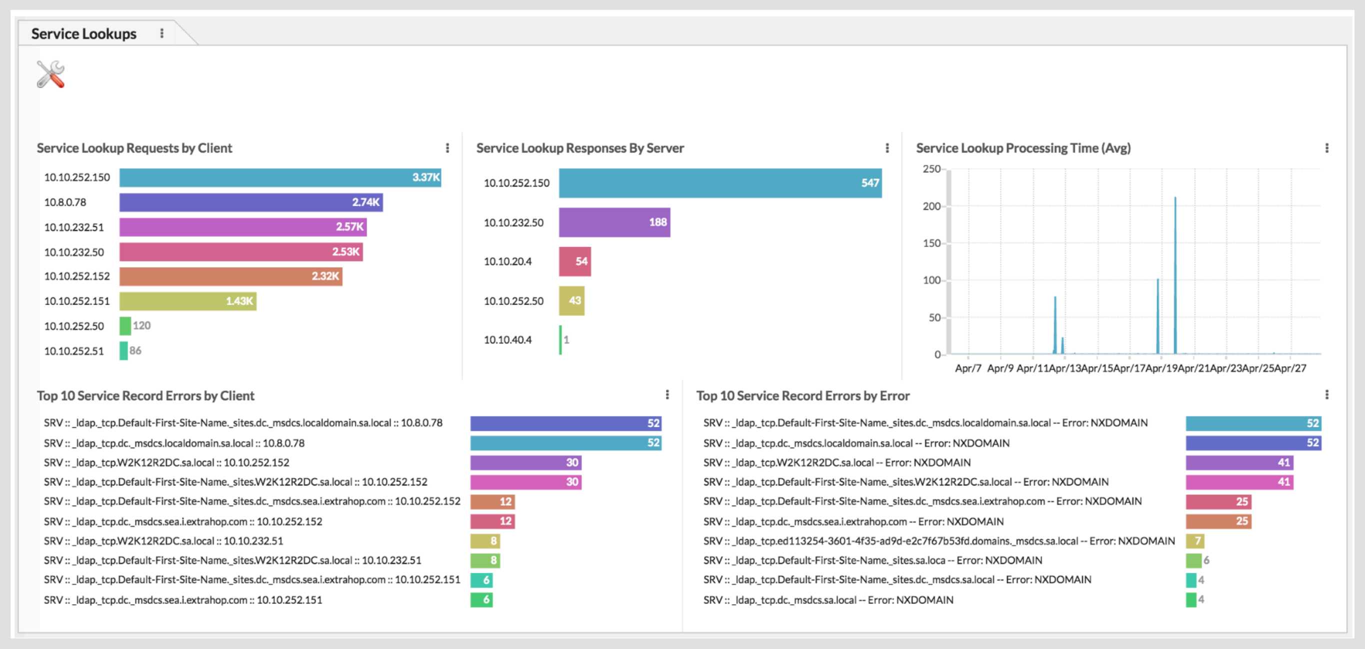
This is for INFOSEC and Sys Admins who need to track down the source of login failures or locked out attempts

Login Failures by Account

This widget shows the login failure by the account. Click the "GO" button and browse to the Kerberos Errors page to drill into the details.

Simplify your authentication monitoring with simplified dashboards

Active Directory, the most common directory service, is built on Lightweight Directory Access Protocol (LDAP). ExtraHop provides insights into LDAP and its connection point with the Domain Name System (DNS). By analyzing these two protocols, the platform enables you to easily spot lookups that are generating errors and see which clients are receiving those errors, making troubleshooting much easier.



Service Lookups

Service Lookup Requests by Client

10.10.252.150	3.37K
10.8.0.78	2.74K
10.10.232.51	2.57K
10.10.232.50	2.53K
10.10.252.152	2.32K
10.10.252.151	1.43K
10.10.252.50	120
10.10.252.51	86

Service Lookup Responses By Server

10.10.252.150	547
10.10.232.50	188
10.10.20.4	54
10.10.252.50	43
10.10.40.4	1

Top 10 Service Record Errors by Client

SRV :: _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.localdomain.sa.local :: 10.8.0.78	52
SRV :: _ldap._tcp.dc._msdcs.localdomain.sa.local :: 10.8.0.78	52
SRV :: _ldap._tcp.W2K12R2DC.sa.local :: 10.10.252.152	30
SRV :: _ldap._tcp.Default-First-Site-Name._sites.W2K12R2DC.sa.local :: 10.10.252.152	30
SRV :: _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.sea.i.extrahop.com :: 10.10.252.152	12
SRV :: _ldap._tcp.dc._msdcs.sea.i.extrahop.com :: 10.10.252.152	12
SRV :: _ldap._tcp.W2K12R2DC.sa.local :: 10.10.232.51	8
SRV :: _ldap._tcp.Default-First-Site-Name._sites.W2K12R2DC.sa.local :: 10.10.232.51	8
SRV :: _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.sea.i.extrahop.com :: 10.10.252.151	6
SRV :: _ldap._tcp.dc._msdcs.sea.i.extrahop.com :: 10.10.252.151	6

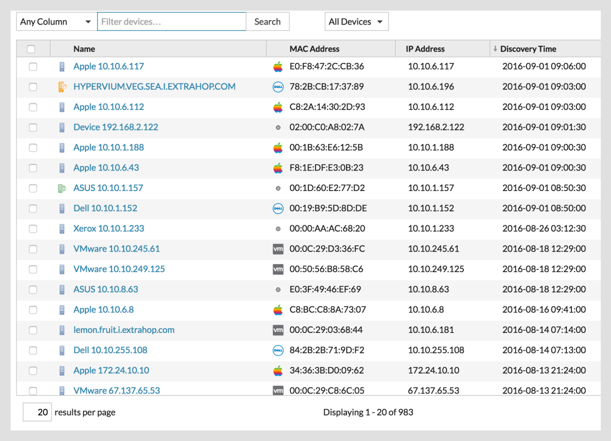
Top 10 Service Record Errors by Error

SRV :: _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.localdomain.sa.local -- Error: NXDOMAIN	52
SRV :: _ldap._tcp.dc._msdcs.localdomain.sa.local -- Error: NXDOMAIN	52
SRV :: _ldap._tcp.W2K12R2DC.sa.local -- Error: NXDOMAIN	41
SRV :: _ldap._tcp.Default-First-Site-Name._sites.W2K12R2DC.sa.local -- Error: NXDOMAIN	41
SRV :: _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.sea.i.extrahop.com -- Error: NXDOMAIN	25
SRV :: _ldap._tcp.dc._msdcs.sea.i.extrahop.com -- Error: NXDOMAIN	25
SRV :: _ldap._tcp.ed113254-3601-4f35-ad9d-e2c7f67b53fd.domains._msdcs.sa.local -- Error: NXDOMAIN	7
SRV :: _ldap._tcp.Default-First-Site-Name._sites.sa.loca -- Error: NXDOMAIN	6
SRV :: _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.sa.local -- Error: NXDOMAIN	4
SRV :: _ldap._tcp.dc._msdcs.sa.local -- Error: NXDOMAIN	4

Determine where service outages are occurring and proactively

Application & Systems Activity Monitoring

In order to defend your environment, you must have a complete view of it. ExtraHop makes this easy by auto-discovering and classifying all systems within your environment.

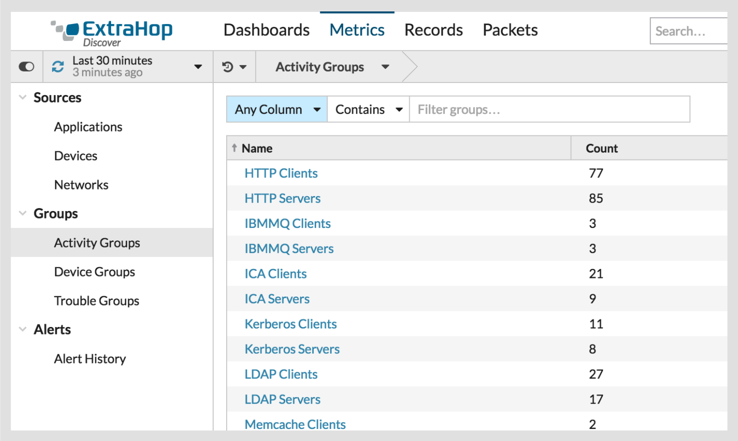


□	Name	MAC Address	IP Address	Discovery Time
□	Apple 10.10.6.117	E0:F8:47:2C:CB:36	10.10.6.117	2016-09-01 09:06:00
□	HYPERVIUM.VEG.SEA.I.EXTRAHOP.COM	78:2B:CB:17:37:89	10.10.6.196	2016-09-01 09:03:00
□	Apple 10.10.6.112	C8:2A:14:30:2D:93	10.10.6.112	2016-09-01 09:03:00
□	Device 192.168.2.122	02:00:C0:A8:02:7A	192.168.2.122	2016-09-01 09:01:30
□	Apple 10.10.1.188	00:1B:63:E6:12:5B	10.10.1.188	2016-09-01 09:00:30
□	Apple 10.10.6.43	F8:1E:DF:E3:0B:23	10.10.6.43	2016-09-01 09:00:30
□	ASUS 10.10.1.157	00:1D:60:E2:77:D2	10.10.1.157	2016-09-01 08:50:30
□	Dell 10.10.1.152	00:19:B9:5D:8D:DE	10.10.1.152	2016-09-01 08:50:00
□	Xerox 10.10.1.233	00:00:AA:AC:68:20	10.10.1.233	2016-08-26 03:12:30
□	VMware 10.10.245.61	00:0C:29:D3:36:FC	10.10.245.61	2016-08-18 12:29:00
□	VMware 10.10.249.125	00:50:56:B8:58:C6	10.10.249.125	2016-08-18 12:29:00
□	ASUS 10.10.8.63	E0:3F:49:46:EF:69	10.10.8.63	2016-08-18 12:29:00
□	Apple 10.10.6.8	C8:BC:C8:8A:73:07	10.10.6.8	2016-08-16 09:41:00
□	lemon.fruit.i.extrahop.com	00:0C:29:03:68:44	10.10.6.181	2016-08-14 07:14:00
□	Dell 10.10.255.108	84:2B:2B:71:9D:F2	10.10.255.108	2016-08-14 07:13:00
□	Apple 172.24.10.10	34:36:3B:D0:09:62	172.24.10.10	2016-08-13 21:24:00
□	VMware 67.137.65.53	00:0C:29:C8:6C:05	67.137.65.53	2016-08-13 21:24:00

20 results per page

Displaying 1 - 20 of 983

Real-time discovery of all systems both server and client and physical or virtual



Name	Count
HTTP Clients	77
HTTP Servers	85
IBMMQ Clients	3
IBMMQ Servers	3
ICA Clients	21
ICA Servers	9
Kerberos Clients	11
Kerberos Servers	8
LDAP Clients	27
LDAP Servers	17
Memcache Clients	2

If it's communicating on the network, ExtraHop will see it and classify it.

This is often where many organizations fail, and where attackers can gain a foothold in the organization. Without a complete view of all these systems there is no way to ensure they are being operated according to policy and not introducing risk. Even more alarming is the ability of an attacker to setup their own IT assets, such as a SSH server or SQL database, that they solely control. These assets then stay under the radar, collecting sensitive data until the hacker is ready to do a major dump and only then when the FTP traffic spikes does the organization realize something is wrong.

Proactive Threat Detection & Remediation

What makes ExtraHop different than other monitoring solutions is that it provides observed behavior rather than reported behavior. You're actively watching the traffic that is traversing the network, instead of trusting hosts and devices to accurately report what they did at any given time in the past. Observed behavior on the network contains vastly more useful information than reported behavior, since the network is the backbone of every digital interaction in your environment and is the starting point of any persistent attack on the environment. It can also expose vulnerability such as passwords that are transmitted in clear text that could be intercepted.

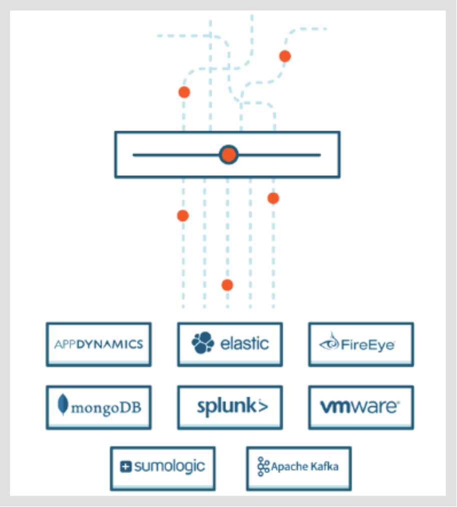
Anomalous Behavior Detection

ExtraHop's visibility across systems, applications, and identity infrastructure provides the key to early detection of problems within the environment. It's not enough to have siloed security tools that identify issues with one system; you need a way to correlate across different systems to understand threats. For instance, if you see port scanning from a host, or brute-force login attempts, or even an insider who is accessing sensitive information in an internal database, you need to be able to correlate the behavior to specific users, and trace the path of the threatening behavior down to where it started.

That's the unique thing about ExtraHop: getting this level of visibility would typically mean instrumenting every application, installing agents on every server, and putting profilers on the database. That just isn't scalable. Being able to watch an attacker jump from server to server, pivoting and targeting a different application here, extracting data there, that's the kind of visibility that any organization can benefit from.

Real-Time Threat Response

ExtraHop believes that you own your data, so we do not make you pay a "data tax" or lock you into a proprietary data store. The ExtraHop Open Data Stream capability enables you to stream precise, real-time events and metrics from ExtraHop to your management systems including: Identity, Operations, and SIEM platforms through syslog or a REST API. These events and metrics can be customized to match the platform. The Open Data Stream feature is included and enables you to make the most of the data that you already own through correlation with other data sets.



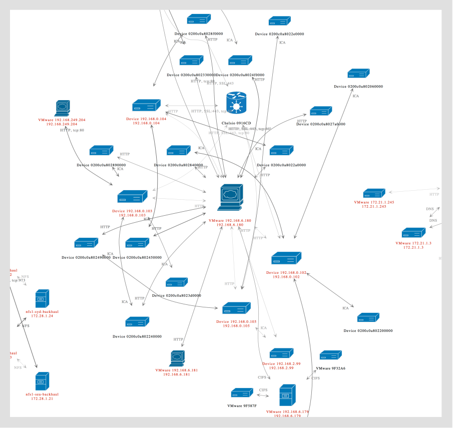
The ExtraHop community has documented integrations for Splunk, VMware, and Sumo Logic, as well as other third-party security analytics systems such as the FireEye Threat Analytics Platform. The platform even supports the security data lake concept through MongoDB and Kafka feeds.

These integrations are the foundation for the ability to build self-healing into your environment. When you see a certain type of activity that is expressly prohibited you can kick off automatic workflows to stop this activity for example blocking access at the firewall, rotating passwords for a compromised system, or taking a compromised server out of production.

Forensics & Compliance

Compliance is yet another critical part of the security, identity, and access management discussion. How can you ever be certain you are adhering to the regulations that govern your organization, or are within policy you need to measure what is occurring in your environment?

Once a credible threat is detected its critical to limit their access and the ability to spread to other systems. This is one of the advantages of using wire data. You can respond much more quickly if you're seeing the behavior in real-time, not waiting for all the logs to be ingested.



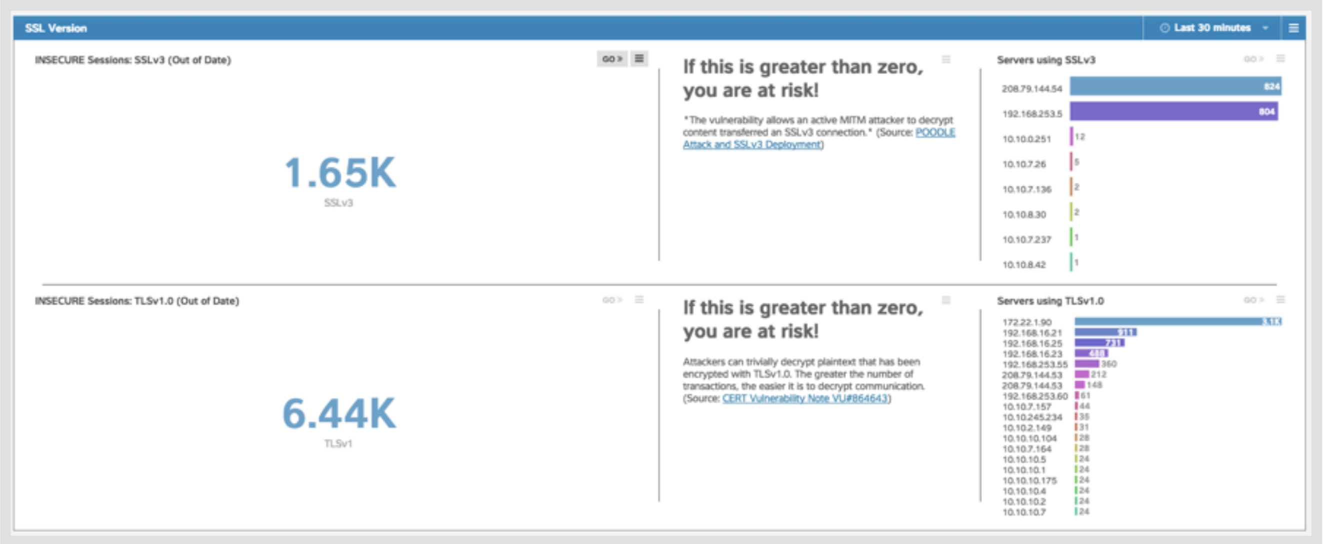
Gain a complete view of which systems are interacting.

Immediately upon detecting the anomalous behavior you're going to want to know which machine was acting that way, what the corresponding credentials being used are, how widespread the incident is, and finally what does the damage look like.

With ExtraHop it is easy to isolate and map the issue so you can determine which other machines need to be quarantined and simplify the path to answers by accelerating the forensics process. This mapping can also uncover behavior that appears legitimate, but may actually be malicious, hiding in the internal traffic in your network.

Risk Profiling

Risk profiling is the front end of compliance; whether for regulatory reasons or for internal requirements. It's making sure that systems and users are operating, as they should be: that security certificates are not about to expire, or that passwords and encryption algorithms are suitably strong across the organization. These metrics are not tied to specific incidents but they frame a picture of health for the entire organization and shed light into areas which could potentially already have been compromised.



SSL Version

INSECURE Sessions: SSLv3 (Out of Date)

1.65K SSLv3

If this is greater than zero, you are at risk!

The vulnerability allows an active MITM attacker to decrypt content transferred an SSLv3 connection. (Source: POODLE Attack and SSLv3 Deployment)

INSECURE Sessions: TLSv1.0 (Out of Date)

6.44K TLSv1

If this is greater than zero, you are at risk!

Attackers can trivially decrypt plaintext that has been encrypted with TLSv1.0. The greater the number of transactions, the easier it is to decrypt communication. (Source: CERT Vulnerability Note VU#864643)

Incident Response

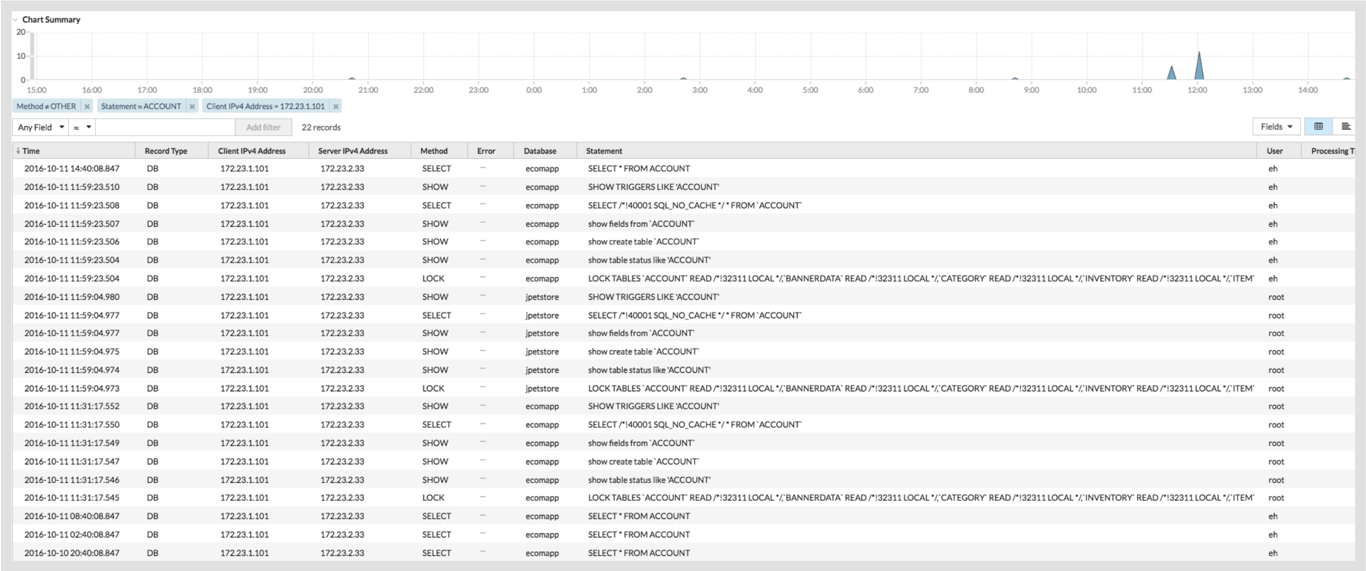
After a security incident, you need to audit the incident and understand the extent of the damage, how the lapse occurred, and most importantly, if the cause of the breach has been addressed.

Traditionally, most organizations rely on logging everything, and backing this up with deep forensics into incidents with extensive packet capture analysis. This isn't scalable for two reasons:

1. The data and processing footprint as you grow becomes cost prohibitive. With logs, you're paying based on how much you ingest (the data tax), in addition to the infrastructure.
2. With continuous packet capture, you may not have enough look-back to have captured the incident.

Both of these methods require a lot of expert staff to set up and extract meaningful insights from the data. Whether it's defining logs, deploying them, and managing them, or the incredibly manual and time-consuming process of sifting through a sea of packets, these challenges only increase as your organization grows.

This is where wire data's advantages over other data sources really leap out. You can achieve look-back that wouldn't be possible from these other means by tapping into the rich metadata of all those communications that are occurring on the network. This means you see everything, even the things you didn't know to look for beforehand. In addition, the simplified workflows that wire data enable make it a data source that can keep pace with a growing enterprise.



Time	Record Type	Client IPv4 Address	Server IPv4 Address	Method	Error	Database	Statement	User	Processing T
2016-10-11 14:40:08.847	DB	172.23.1.101	172.23.2.33	SELECT	—	ecomapp	SELECT * FROM ACCOUNT	eh	
2016-10-11 11:59:23.510	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	SHOW TRIGGERS LIKE 'ACCOUNT'	eh	
2016-10-11 11:59:23.508	DB	172.23.1.101	172.23.2.33	SELECT	—	ecomapp	SELECT /*!40001 SQL_NO_CACHE */ * FROM `ACCOUNT`	eh	
2016-10-11 11:59:23.507	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	show fields from `ACCOUNT`	eh	
2016-10-11 11:59:23.506	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	show create table `ACCOUNT`	eh	
2016-10-11 11:59:23.504	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	show table status like 'ACCOUNT'	eh	
2016-10-11 11:59:23.504	DB	172.23.1.101	172.23.2.33	LOCK	—	ecomapp	LOCK TABLES `ACCOUNT` READ /*!32311 LOCAL */,`BANNERDATA` READ /*!32311 LOCAL */,`CATEGORY` READ /*!32311 LOCAL */,`INVENTORY` READ /*!32311 LOCAL */,`ITEM`	eh	
2016-10-11 11:59:04.980	DB	172.23.1.101	172.23.2.33	SHOW	—	jpetstore	SHOW TRIGGERS LIKE 'ACCOUNT'	root	
2016-10-11 11:59:04.977	DB	172.23.1.101	172.23.2.33	SELECT	—	jpetstore	SELECT /*!40001 SQL_NO_CACHE */ * FROM `ACCOUNT`	root	
2016-10-11 11:59:04.977	DB	172.23.1.101	172.23.2.33	SHOW	—	jpetstore	show fields from `ACCOUNT`	root	
2016-10-11 11:59:04.975	DB	172.23.1.101	172.23.2.33	SHOW	—	jpetstore	show create table `ACCOUNT`	root	
2016-10-11 11:59:04.974	DB	172.23.1.101	172.23.2.33	SHOW	—	jpetstore	show table status like 'ACCOUNT'	root	
2016-10-11 11:59:04.973	DB	172.23.1.101	172.23.2.33	LOCK	—	jpetstore	LOCK TABLES `ACCOUNT` READ /*!32311 LOCAL */,`BANNERDATA` READ /*!32311 LOCAL */,`CATEGORY` READ /*!32311 LOCAL */,`INVENTORY` READ /*!32311 LOCAL */,`ITEM`	root	
2016-10-11 11:31:17.552	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	SHOW TRIGGERS LIKE 'ACCOUNT'	root	
2016-10-11 11:31:17.550	DB	172.23.1.101	172.23.2.33	SELECT	—	ecomapp	SELECT /*!40001 SQL_NO_CACHE */ * FROM `ACCOUNT`	root	
2016-10-11 11:31:17.549	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	show fields from `ACCOUNT`	root	
2016-10-11 11:31:17.547	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	show create table `ACCOUNT`	root	
2016-10-11 11:31:17.546	DB	172.23.1.101	172.23.2.33	SHOW	—	ecomapp	show table status like 'ACCOUNT'	root	
2016-10-11 11:31:17.545	DB	172.23.1.101	172.23.2.33	LOCK	—	ecomapp	LOCK TABLES `ACCOUNT` READ /*!32311 LOCAL */,`BANNERDATA` READ /*!32311 LOCAL */,`CATEGORY` READ /*!32311 LOCAL */,`INVENTORY` READ /*!32311 LOCAL */,`ITEM`	root	
2016-10-11 08:40:08.847	DB	172.23.1.101	172.23.2.33	SELECT	—	ecomapp	SELECT * FROM ACCOUNT	eh	
2016-10-11 02:40:08.847	DB	172.23.1.101	172.23.2.33	SELECT	—	ecomapp	SELECT * FROM ACCOUNT	eh	
2016-10-10 20:40:08.847	DB	172.23.1.101	172.23.2.33	SELECT	—	ecomapp	SELECT * FROM ACCOUNT	eh	

See the queries in a database for instance without the need to install a profiler that takes up needed resources

Conclusion

ExtraHop offers the visibility necessary to strengthen and enhance your identity infrastructure. This is an area where many organizations fail to invest adequately. An IT environment is constantly evolving, and while your identity policies should be established and adhered to, enforcement just isn't possible without a complete view of the environment. ExtraHop will make it easier both to secure your environment and to prove its security by reporting on your own compliance.

About ExtraHop

ExtraHop makes real-time data-driven IT operations possible. By harnessing the power of wire data in real time, network, application, security, and business teams make faster, more accurate decisions that optimize performance and minimize risk. Hundreds of organizations, including Fortune 500 companies such as Sony, Lockheed Martin, Microsoft, Adobe, and Google, start with ExtraHop to discover, observe, analyze, and intelligently act on all data in flight on-premises and in the cloud.

ExtraHop Networks, Inc.

520 Pike Street, Suite 1700

Seattle, WA 98101 USA

www.extrahop.com

info@extrahop.com