SANS

Analyst Program

Product Review

Your Network, Under Control

Written by **Matt Bromiley**

August 2021

FORENOVA

Introduction

You cannot protect what you cannot see.

Truer words may not exist when it comes to enterprise information security. Many organizations are caught off guard when they suffer an intrusion, only to realize that they did not have complete visibility of their enterprise. Matters only grow worse when an investigation reveals the adversary's foothold as either wider or older than previously detected (possibly both).

Security teams should look for tooling that helps them capture more of the environment at one time, rather than piecemealing multiple tools together. Luckily, every organization has a "common denominator" that every connected asset utilizes: the network. Network detection and response (NDR) serves as the right approach to increase enterprise visibility and detect adversaries because adversaries simply cannot avoid the network. NDR often proves to be easier said than done, however, because networks inherently contain large amounts of data moving at breakneck speeds.

In this product review, we examine a platform that helps organizations make sense of their network and operationalize NDR: ForeNova. ForeNova's easy-to-use platform, NovaCommand, makes examining and contextualizing your network data simple. NovaCommand couples real-time asset identification and classification with robust detection and response capabilities that give analysts a single resource for enhanced visibility over their environment.

After using NovaCommand, we especially appreciated:

- Real-time visibility into an organization's *entire* network with immediate insight and asset identification
- Automatic server and non-server asset classification, allowing granular asset controls and evaluation of each group's *expected* traffic versus *actual* traffic
- Threat detection and incident response all bundled into one platform to create a powerful tool that will level up any security team immediately
- Network-centric detection and response for an organization, including north-south and east-west traffic
- Third-party integration to easily incorporate NDR with other security controls already deployed in your environment.

NovaCommand takes a complex and multilayered topic like NDR and makes it immediately actionable for security teams. When it comes to detecting and stopping adversaries today, don’t exclude your network from your telemetry. As you read through this review, ask yourself these questions:

- Do I have an equal level of visibility within my environment?
- Does my security team utilize the network as a common source of truth to help detect and respond to threats?
- If my organization utilizes network data, how do we ingest it? Do we simply ingest logs and correlate with data, or can we action on the network just like endpoints?

If any of the above questions gave you pause, or you question your own enterprise visibility, let’s look at how an NDR platform might be exactly what your team needs.

Visibility with NovaCommand

We begin our review where analysts being their day: at the initial dashboard. NovaCommand’s dashboard, a snippet of which Figure 1 shows here, is packed with insight into the organization and actions awaiting analysis and response.

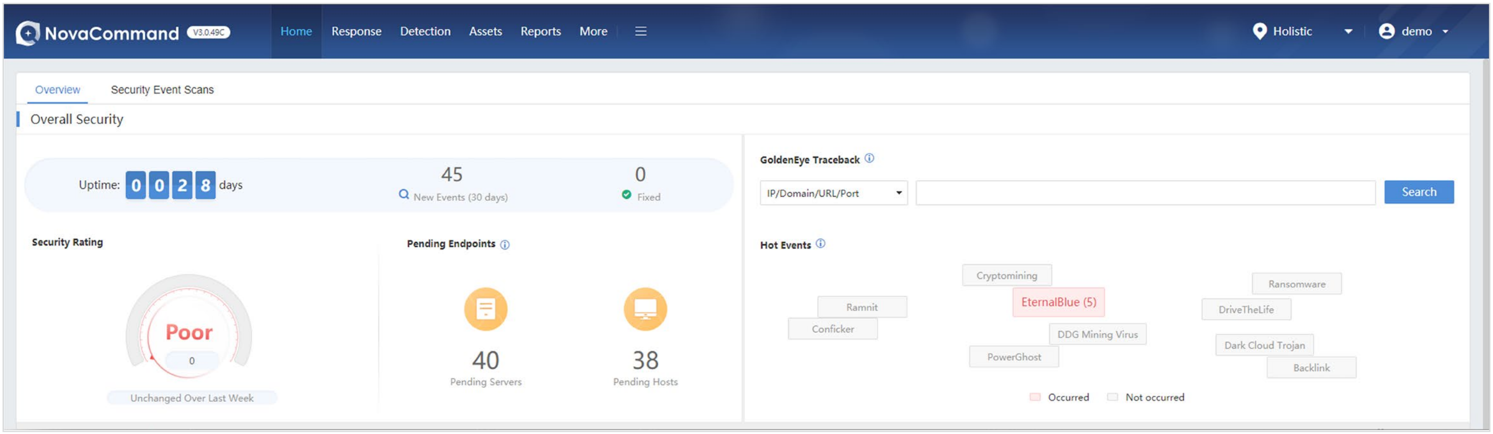


Figure 1. First Row of NovaCommand Platform’s Initial Dashboard

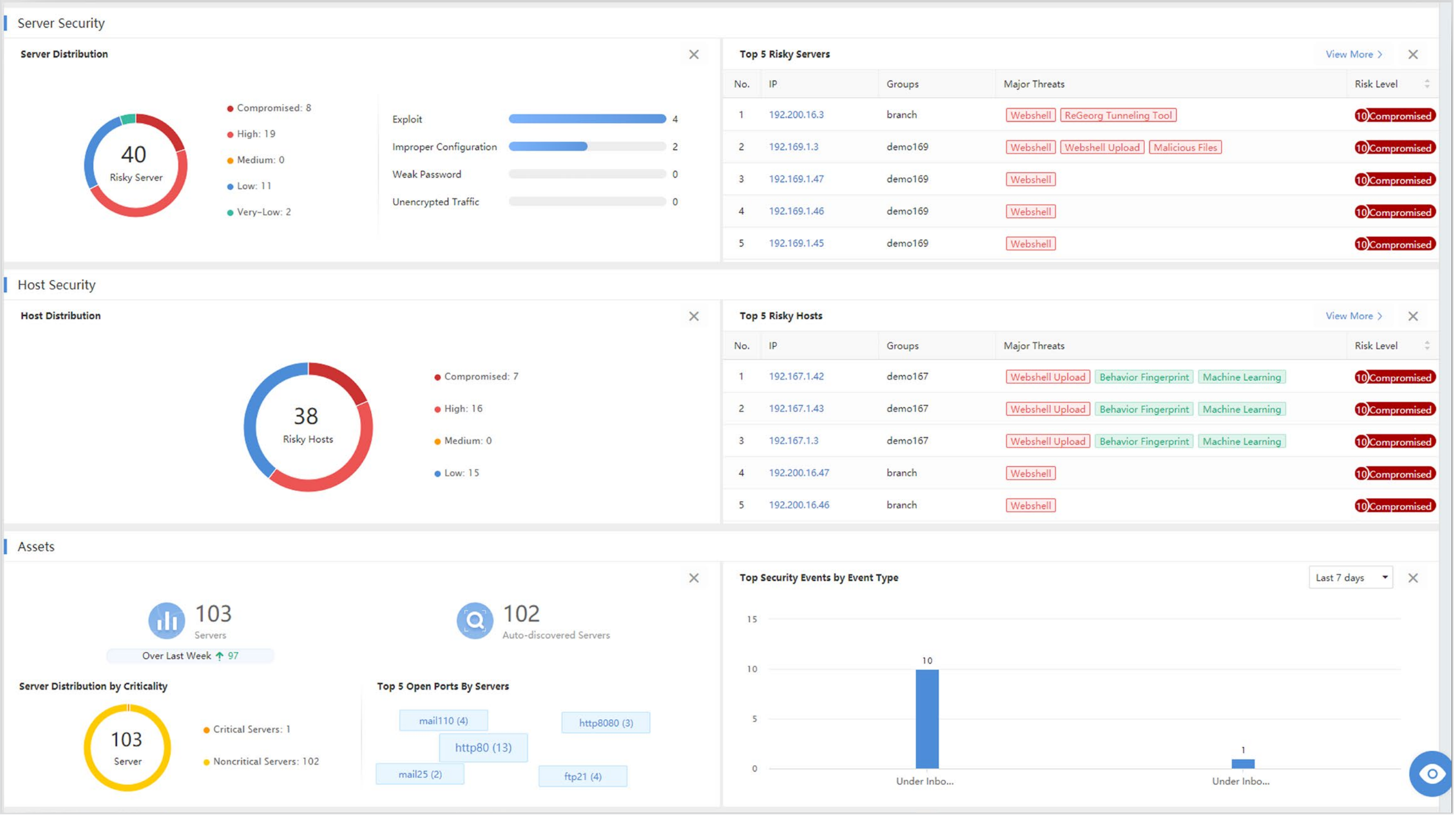
As the figure illustrates, the first row of the dashboard provides summarized analyses and key data points such as:

- A live, overall security rating of the enterprise network
- “Hot” events observed in the network
- Pending endpoints, split into servers and hosts
- Network uptime
- A GoldenEye Traceback search bar (more on this later)

Throughout this review, we touch on each of the data points multiple times. A consistent theme runs through them all: **What is going on in my network right now?** We are huge fans of dashboards that "get to the point," and NovaCommand does this immediately.

The initial dashboard continues. The top row, described previously, provides a summarized viewpoint. The latter portion, shown in Figure 2, provides more detailed insight into the organization and NovaCommand's true capabilities with the data it receives.

In this product review, we examine NovaCommand, the platform one would use to analyze traffic and detect and respond to incidents. NovaCommand is fed traffic from ForeNova's NovaSensor, itself a powerful sensor that can classify data based on intelligence and user-defined rules. While we do not discuss NovaSensor, readers should keep in mind its necessity for forwarding traffic and traffic metadata to the NovaCommand platform.



Top 5 Risky Servers

No.	IP	Groups	Major Threats	Risk Level
1	192.200.16.3	branch	Webshell ReGeorg Tunneling Tool	10 Compromised
2	192.169.1.3	demo169	Webshell Webshell Upload Malicious Files	10 Compromised
3	192.169.1.47	demo169	Webshell	10 Compromised
4	192.169.1.46	demo169	Webshell	10 Compromised
5	192.169.1.45	demo169	Webshell	10 Compromised

Top 5 Risky Hosts

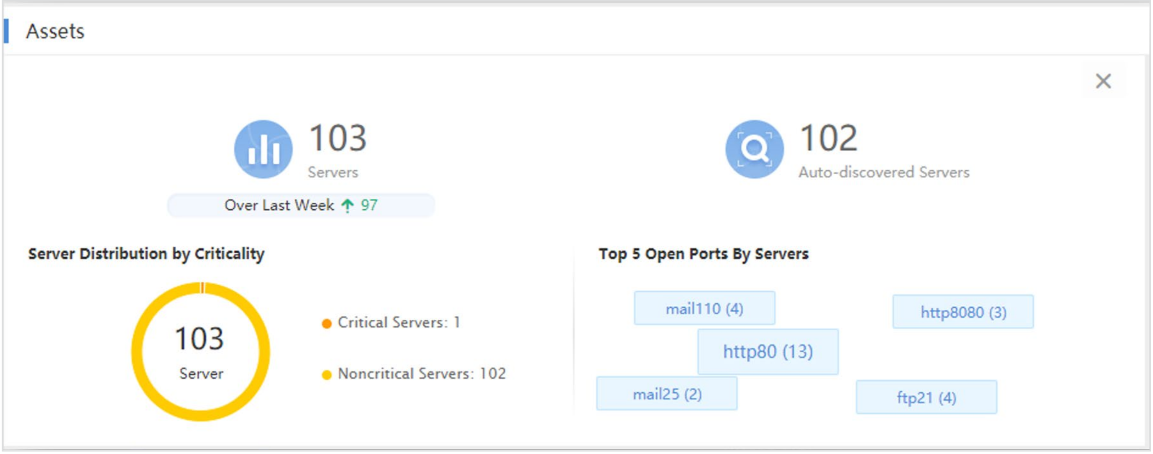
No.	IP	Groups	Major Threats	Risk Level
1	192.167.1.42	demo167	Webshell Upload Behavior Fingerprint Machine Learning	10 Compromised
2	192.167.1.43	demo167	Webshell Upload Behavior Fingerprint Machine Learning	10 Compromised
3	192.167.1.3	demo167	Webshell Upload Behavior Fingerprint Machine Learning	10 Compromised
4	192.200.16.47	branch	Webshell	10 Compromised
5	192.200.16.46	branch	Webshell	10 Compromised

Figure 2. Latter Portion of NovaCommand Platform's Initial Dashboard

Notice in Figure 2 that NovaCommand automatically separates the environment based on server vs. host (we interpret host to mean a non-server endpoint). We appreciate the asset classification as servers vs. non-servers. Some analysts may argue that splitting data between servers and non-servers does not matter if an adversary gains a foothold on either. However, remember that we are looking at the enterprise from a *network* perspective. We would *expect* server traffic to differ greatly from that of a non-server.

Our first hint of the level of visibility begins with the classification of servers vs. non-servers. We should expect these two asset groups to display different types of traffic. Therefore, they should be analyzed and reported on differently.

We would also expect that a mix of systems within the server group would be exposed to the internet, whereas we would not expect that from non-servers. Another benefit to this type of high-level classification is that analysts can use NovaCommand to write detections based on host type, thereby writing better detections. As Figure 2 shows, NovaCommand provides server-specific details about attacks, such as whether an exploit was used or a server was improperly configured. As shown to the right in Figure 2, NovaCommand also enumerates the riskiest assets in each group, providing high-level details about the threat(s) observed and the risk level of the system. We will examine this further in a subsequent section.


Assets

103 Servers

Over Last Week ↑ 97

102 Auto-discovered Servers

Server Distribution by Criticality

103 Server

● Critical Servers: 1

● Noncritical Servers: 102

Top 5 Open Ports By Servers

mail110 (4)	http8080 (3)
http80 (13)	
mail25 (2)	ftp21 (4)

Figure 3. Snippet of the Assets Widget from the NovaCommand Dashboard

With its immense visibility from a network standpoint, ForeNova designed NovaCommand as more than just a detection and response platform. It is also an incredibly powerful asset management tool. Just as adversaries cannot escape the network, neither can networked assets. NovaCommand provides asset classification that does not require the use of endpoint- or domain-based inventory tools (see Figure 3).

Note that NovaCommand includes "Auto-discovered Servers," an autogenerated category based on observed traffic—again, capitalizing on the depth of visibility offered by the network. Another data point we found useful, if even from an informational perspective, is the inclusion of open ports as observed in traffic. We found this data point can serve as a quick check for analysts and server administrators. An odd or unexpected port in this category might offer a simple and efficient way to determine a potential misconfiguration or whether suspicious activity has occurred.

Actionable Visibility

Before we examine detection and response with NovaCommand, let's continue exploring the platform's use as an asset classification tool. Far too often, security incidents occur because a system remains outside the visibility/control of the security team. We solve this problem only with visibility and classification, both essential traits to successful incident detection and response. ForeNova recognized this and built in classification of assets as a key feature of the platform (see Figure 4).

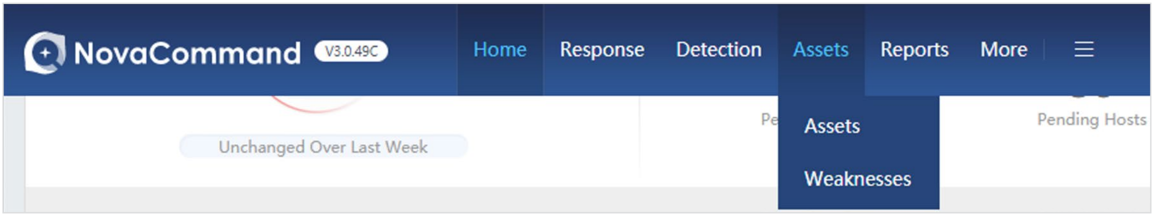


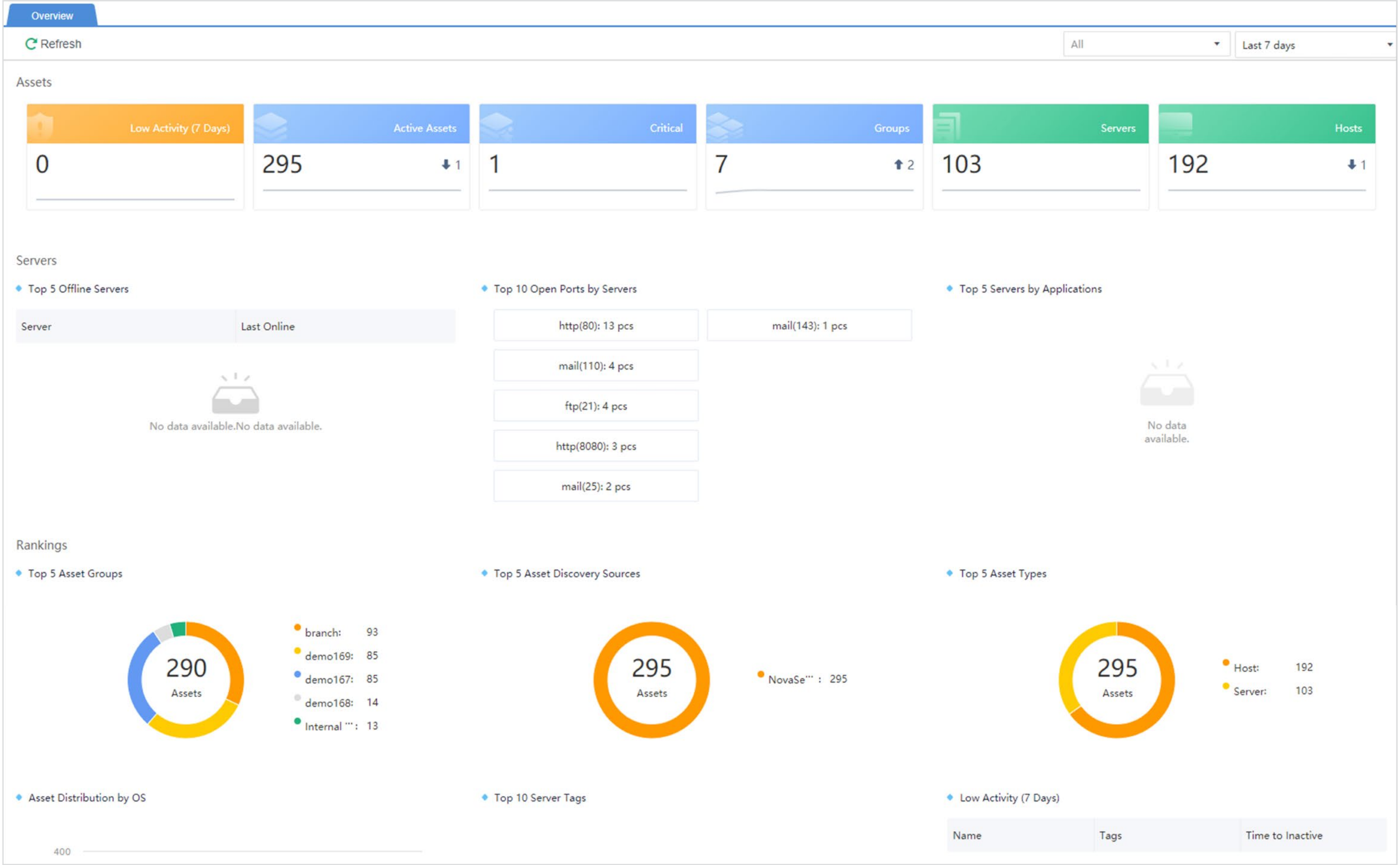
Figure 4. Snippet of the NovaCommand Nav Bar, Showing Assets as a Key Function of the Platform

As Figure 4 shows, NovaCommand not only includes Assets as a key part of the platform but also offers the option to categorize assets based on weaknesses as determined by the platform's analytics and integrated threat intelligence.

The Assets Overview page provides the first step to gaining *actionable visibility* into the organization.

As Figure 5 shows, NovaCommand's Assets page provides even more insight into assets as observed in network traffic. In addition to servers vs. non-servers, NovaCommand allows for asset grouping, criticality rankings, OS identification, and changes (increases or decreases) in asset numbers. Like the initial dashboard, this useful screen provides a single point of asset visibility.

For years, conventional wisdom held visibility as essential to successful detection and response. However, simply "knowing" of an asset is not enough. NovaCommand provides security teams *actionable visibility*—data points that teams can use to write better detections, contribute to response plans, and help keep the environment more secure.



Assets

Low Activity (7 Days)	Active Assets	Critical	Groups	Servers	Hosts
0	295 ⬇1	1	7 ⬆2	103	192 ⬇1

Servers

- Top 5 Offline Servers

Server	Last Online

No data available.No data available.

- Top 10 Open Ports by Servers

http(80): 13 pcs
mail(143): 1 pcs
mail(110): 4 pcs
ftp(21): 4 pcs
http(8080): 3 pcs
mail(25): 2 pcs

- Top 5 Servers by Applications

No data available.

Rankings

- Top 5 Asset Groups

290 Assets

branch:	93
demo169:	85
demo167:	85
demo168:	14
Internal ˙˙˙:	13

- Top 5 Asset Discovery Sources

295 Assets

NovaSe˙˙˙ : 295

- Top 5 Asset Types

295 Assets

Host:	192
Server:	103

- Asset Distribution by OS

400

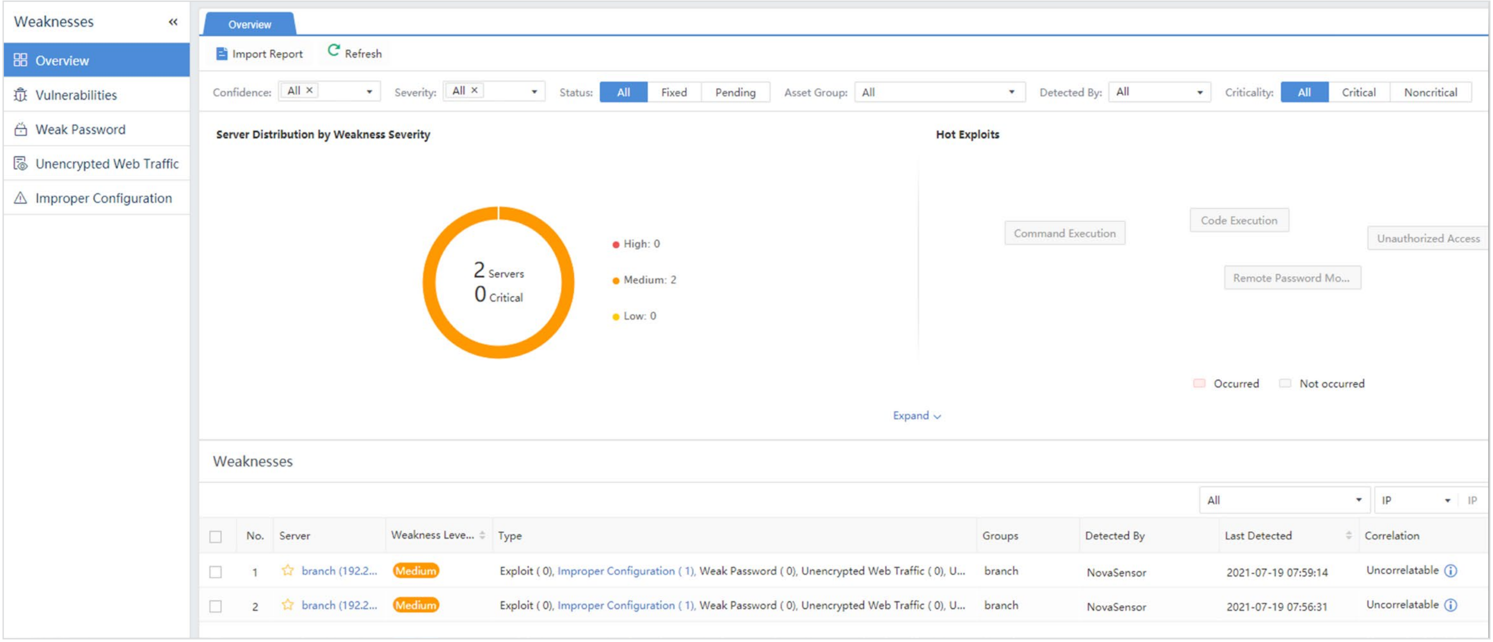
- Top 10 Server Tags

- Low Activity (7 Days)

Name	Tags	Time to Inactive

Figure 5. Screenshot of the Assets Overview Dashboard

Within its asset classification capabilities, NovaCommand also includes a *Weaknesses* viewpoint. We found the Weaknesses tab to be a more direct form of asset visibility and management.

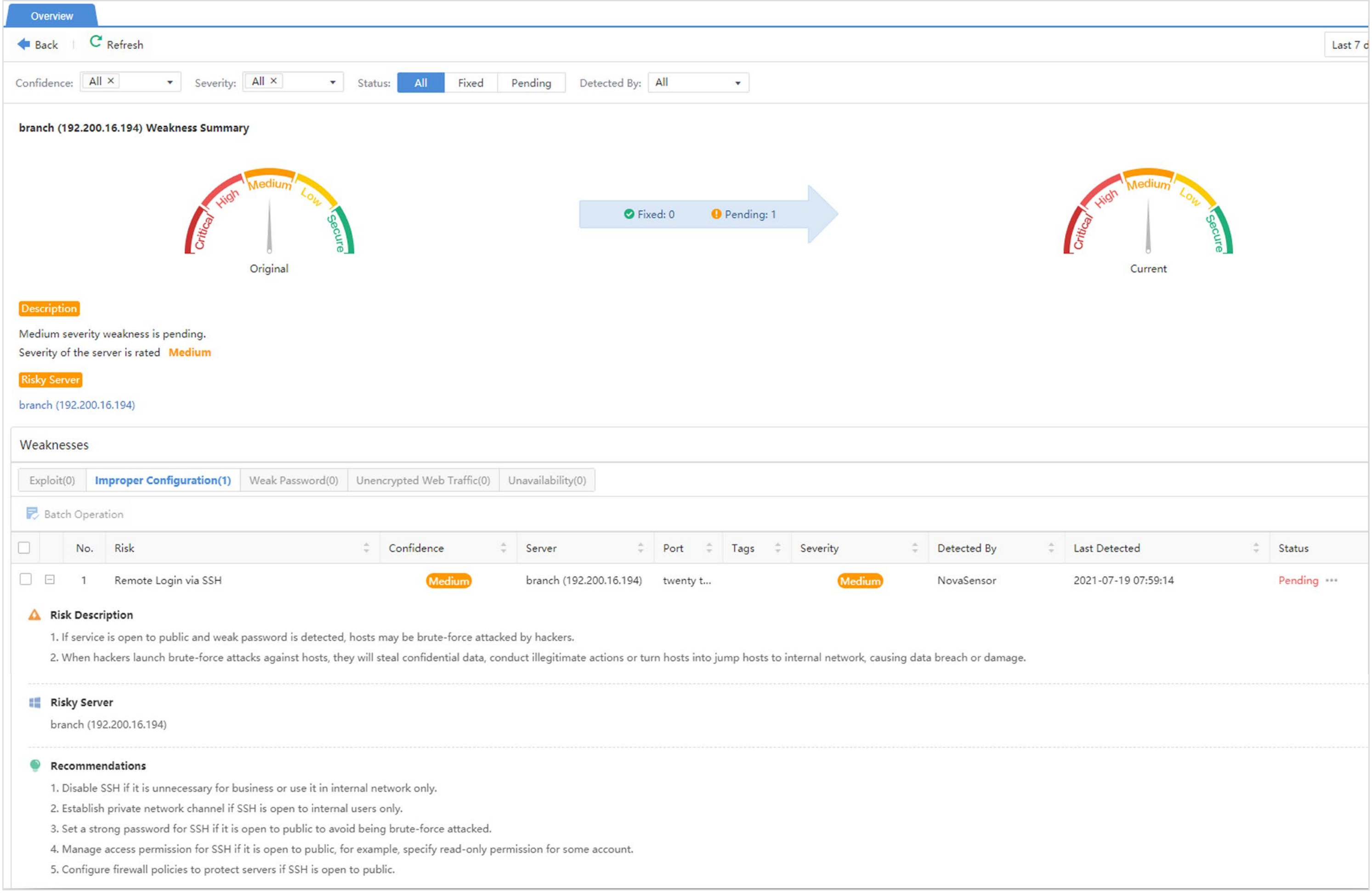


☐	No.	Server	Weakness Leve...	Type	Groups	Detected By	Last Detected	Correlation
☐	1	☆ branch (192.2...	Medium	Exploit (0), Improper Configuration (1), Weak Password (0), Unencrypted Web Traffic (0), U...	branch	NovaSensor	2021-07-19 07:59:14	Uncorrelatable ⓘ
☐	2	☆ branch (192.2...	Medium	Exploit (0), Improper Configuration (1), Weak Password (0), Unencrypted Web Traffic (0), U...	branch	NovaSensor	2021-07-19 07:56:31	Uncorrelatable ⓘ

Figure 6. Snippet of the Weaknesses Tab, an Asset Viewpoint from Within NovaCommand

As Figure 6 shows, Weaknesses identifies key weaknesses or misconfigurations in the environment that warrant remediation. At this one point, NovaCommand truly differentiates itself from others in asset classification. This page provides actionable details on “things to be fixed” within the environment to prevent future security concerns. Zooming in on the first server identified with a weakness, Figure 7 shows the level of detail that NovaCommand provides on a detected weakness.

Figure 7. Snippet of the Weakness Overview Tab for a Demo System



branch (192.200.16.194) Weakness Summary

Description

Medium severity weakness is pending.

Severity of the server is rated Medium

Risky Server

branch (192.200.16.194)

Weaknesses

☐		No.	Risk	Confidence	Server	Port	Tags	Severity	Detected By	Last Detected	Status
☐	⊟	1	Remote Login via SSH	Medium	branch (192.200.16.194)	twenty t...		Medium	NovaSensor	2021-07-19 07:59:14	Pending ···

Risk Description

1. If service is open to public and weak password is detected, hosts may be brute-force attacked by hackers.
2. When hackers launch brute-force attacks against hosts, they will steal confidential data, conduct illegitimate actions or turn hosts into jump hosts to internal network, causing data breach or damage.

Risky Server

branch (192.200.16.194)

Recommendations

1. Disable SSH if it is unnecessary for business or use it in internal network only.
2. Establish private network channel if SSH is open to internal users only.
3. Set a strong password for SSH if it is open to public to avoid being brute-force attacked.
4. Manage access permission for SSH if it is open to public, for example, specify read-only permission for some account.
5. Configure firewall policies to protect servers if SSH is open to public.

The weakness identified in Figure 7 is an open SSH port that could be exploited for remote login into the environment. As we mentioned earlier, actionable visibility remains the goal for security teams. NovaCommand not only identifies the weakness (which is rated a Medium criticality) but also provides the analysts with a description of the potential risks and recommendations for remediating the weakness.

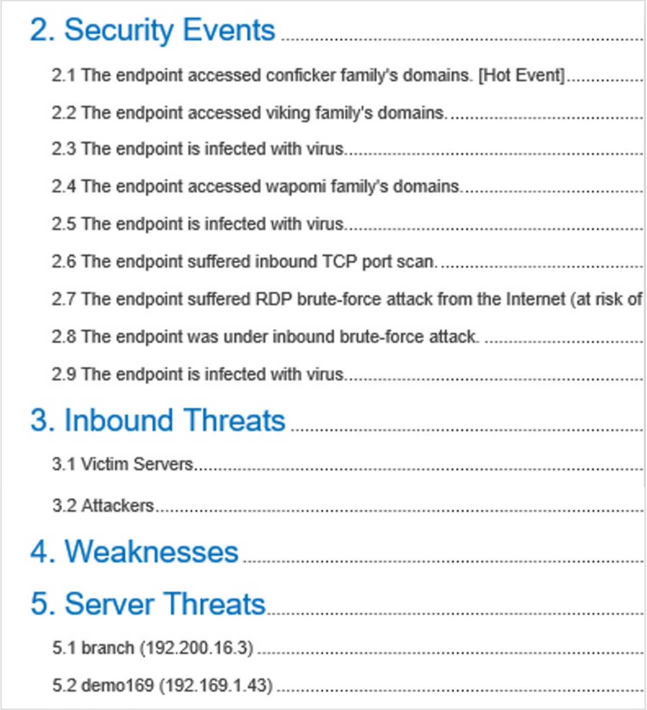
These data points offer immense value to the security team. We are always fans of *proactive* knowledge that we can use to help secure an organization. Misconfigurations, weak passwords, or unencrypted web traffic exemplify things that security teams should seek to rectify as soon as possible. Fortunately, NovaCommand meets this need by providing multiple recommendations, each of which can help mitigate the issue. Note as well that NovaCommand does not simply recommend "disable the port." Understanding that this server weakness may represent a critical weakness for business operations, NovaCommand also provides guidance about account permissions, password complexity, and firewall policies.

You may have noticed in Figure 7 that NovaCommand also includes future changes in a system weakness. If the misconfiguration is rectified, the criticality of the system will change appropriately in the top portion of Figure 7. The value for security teams appears obvious immediately. As they make positive changes in the environment, NovaCommand updates (based on traffic observed and system inspection) its rankings. The security team gets a valuable and immediate ranking of the organization and knows how to prioritize tasks.

Incident Detection

While we appreciate data and insight that gives the security team a proactive edge on adversaries, we recognize incident detection and handling to be just as critical as proactive remediation. Luckily, as an NDR platform, NovaCommand provides security teams with a powerful capability to address threats from the network perspective.

In addition to rich data reporting and classification, ForeNova also includes robust reporting capabilities. Reports are generated on demand and contain a wealth of enterprise security details, making it easy to export and share throughout the security team (see Figure 8).



2. Security Events ....

2.1 The endpoint accessed conficker family's domains. [Hot Event]................

2.2 The endpoint accessed viking family's domains. ....

2.3 The endpoint is infected with virus. ....

2.4 The endpoint accessed wapomi family's domains. ....

2.5 The endpoint is infected with virus. ....

2.6 The endpoint suffered inbound TCP port scan. ....

2.7 The endpoint suffered RDP brute-force attack from the Internet (at risk of

2.8 The endpoint was under inbound brute-force attack. ....

2.9 The endpoint is infected with virus. ....

3. Inbound Threats ....

3.1 Victim Servers ....

3.2 Attackers ....

4. Weaknesses ....

5. Server Threats ....

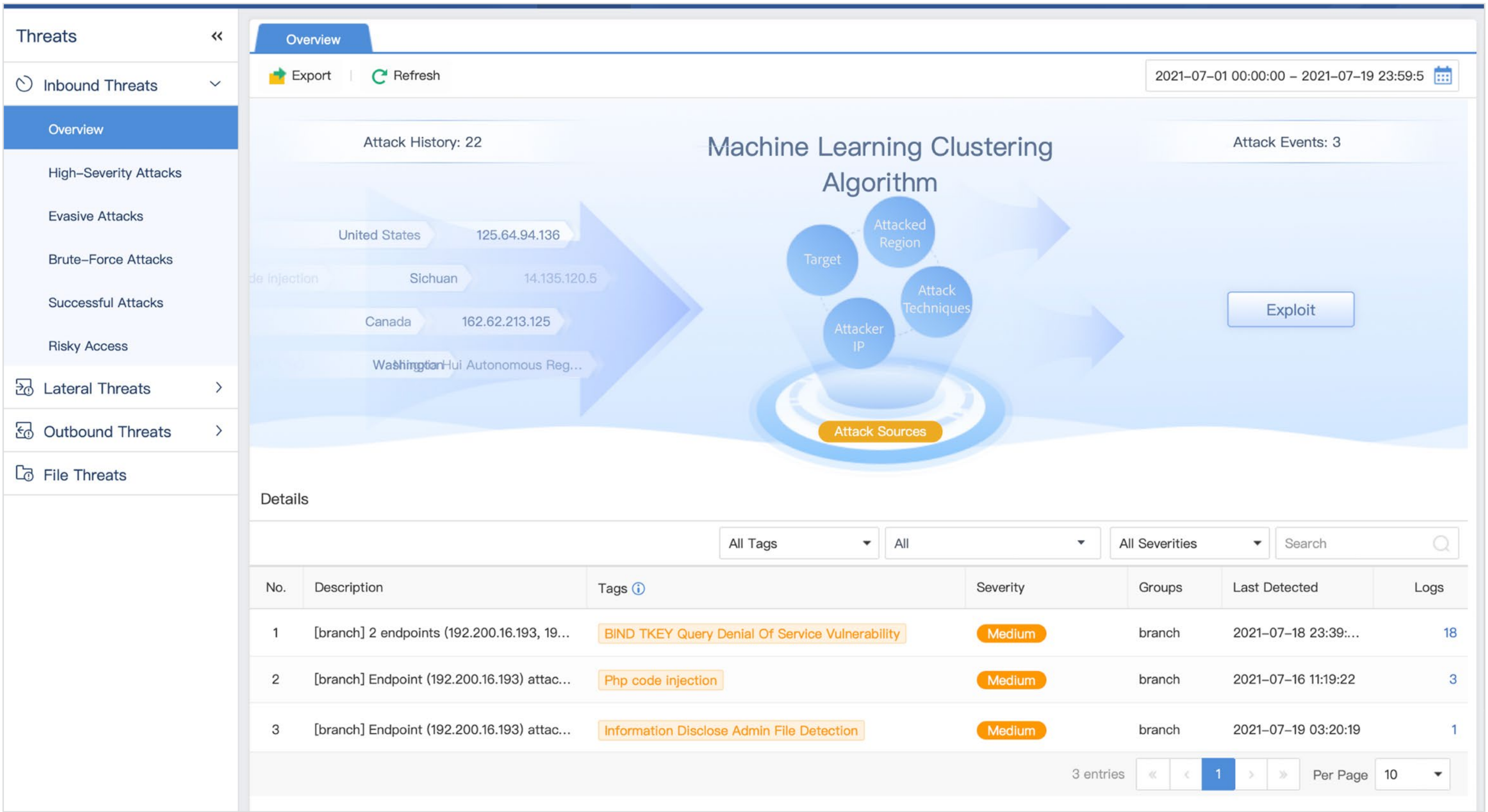
5.1 branch (192.200.16.3) ....

5.2 demo169 (192.169.1.43) ....

Figure 8. Sample Report Listing

Robust reporting also allows security leaders and managers to track security weaknesses and patterns in the environment and prioritize analysts' tasks accordingly.

The Detection functionality, shown in Figure 9, presents a unique, animated (unseen here) dashboard that summarizes attack details into high-level focus points.



No.	Description	Tags	Severity	Groups	Last Detected	Logs
1	[branch] 2 endpoints (192.200.16.193, 19...	BIND TKEY Query Denial Of Service Vulnerability	Medium	branch	2021-07-18 23:39:...	18
2	[branch] Endpoint (192.200.16.193) attac...	Php code injection	Medium	branch	2021-07-16 11:19:22	3
3	[branch] Endpoint (192.200.16.193) attac...	Information Disclose Admin File Detection	Medium	branch	2021-07-19 03:20:19	1

3 entries « ‹ 1 › » Per Page 10

Figure 9. Snippet of the Detection Screen from the NovaCommand Platform

As Figure 9 shows, NovaCommand does not just simply provide analysts with a list of detections. Instead, it provides summarized details with an easy-to-use screen that allows analysts to drill down as needed. Alerts are "rolled up," and analysts can see a description, tags, severity, and asset group(s) up front. We'll examine a threat shortly.

As shown on the left side of the dashboard, NovaCommand also breaks threats down into key categories, each of which offers specific value to an NDR platform not found in other security controls. Table 1 enumerates each high-level threat category and the value to an NDR platform.

We appreciated NovaCommand's threat classification as shown in Table 1. Keep in mind that with an NDR platform, your team should take a network-centric approach toward threats. High-level directionality classifications not only help describe the key components of an attack but also help teams prioritize which alerts require immediate response. The threat sub-types are also dynamic, proving that as a platform NovaCommand is directional aware.

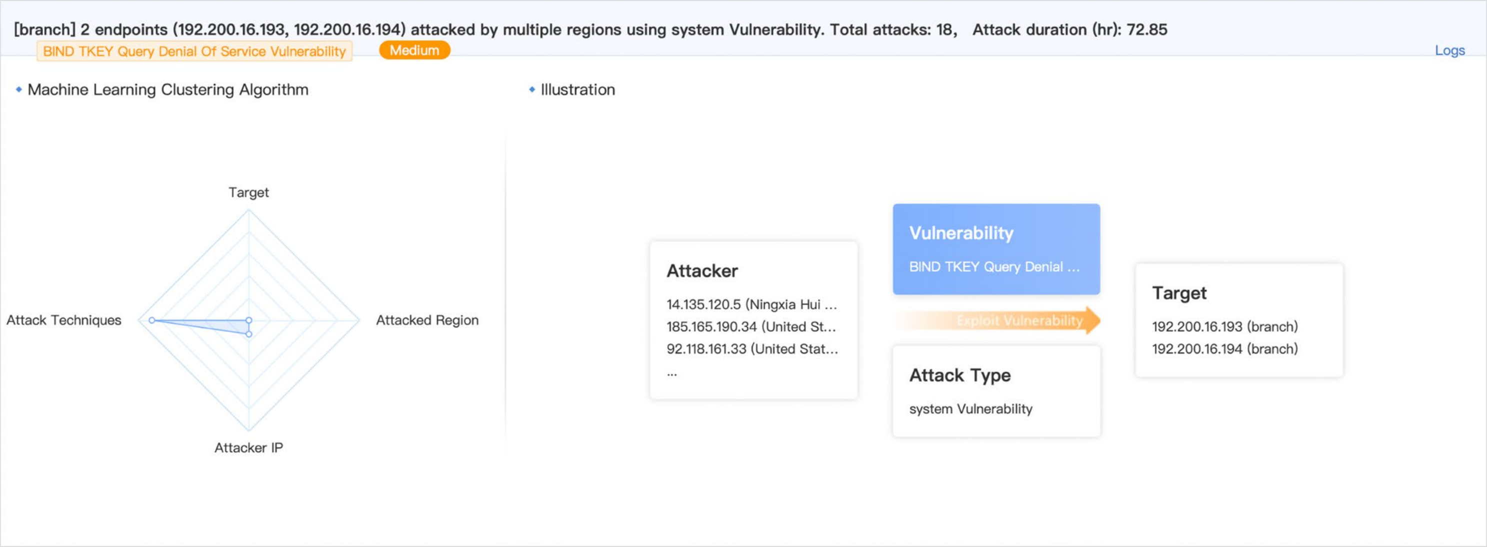
Table 1. List of NovaCommand Threat Types and the Value to an NDR Platform

	Threat Sub-Types	NDR Value
Inbound	• High-severity • Evasive • Brute-force • Successful • Risky	Attacks that originate from *outside* the network, targeting assets within the organization
Lateral	• Lateral attacks • Unauthorized access • Suspicious activities • Risky access	Attacks that are *entirely internal*, representing lateral movement between enterprise-owned assets
Outbound	• Outbound attacks • APT C&C (C2) • Suspicious activities • Stealth communications • Unauthorized access • Risky access	Attacks that originate from *inside* the network, attempting to reach outbound and/or attack external assets
File-based	N/A	A companion data point, files that are observed within network traffic (regardless of direction) are also extracted and available for further analysis (malware execution, document inspection)

With these threat types and sub-types, NovaCommand has provided a unique way for analysts to approach handling. Metadata points such as directionality or attack "type" are often embedded in an alert, provided as a tag, or are part of threat enrichment in competitor platforms. ForeNova brings these to the front, instead allowing analysts to focus their efforts on C2 communications or lateral movement, which not only saves time but also ensures that security teams utilize response resources in the appropriate areas.

> **Attack directionality is a key component that NovaCommand offers to analysts. A quick assessment of an attack's direction—such as inbound or east-west—can help prioritize alerts and determine where teams should focus their energy first.**

Of course, analysts can utilize the rich metadata captured about an event to understand a particular attack. Figure 10 provides insight into an alert of system vulnerability exploitation.



[branch] 2 endpoints (192.200.16.193, 192.200.16.194) attacked by multiple regions using system Vulnerability. Total attacks: 18, Attack duration (hr): 72.85

BIND TKEY Query Denial Of Service Vulnerability Medium

Logs

- Machine Learning Clustering Algorithm
- Illustration

Attacker
14.135.120.5 (Ningxia Hui ...
185.165.190.34 (United St...
92.118.161.33 (United Stat...
...

Vulnerability
BIND TKEY Query Denial ...

Exploit Vulnerability

Attack Type
system Vulnerability

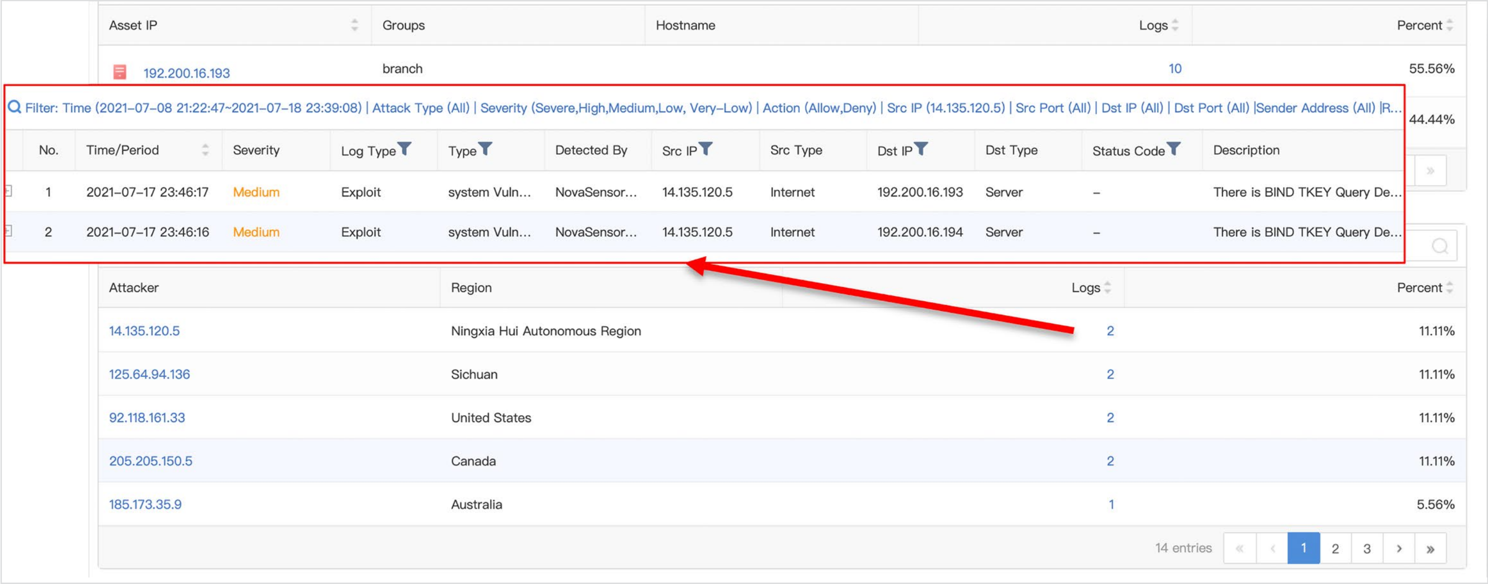
Target
192.200.16.193 (branch)
192.200.16.194 (branch)

Figure 10. Snippet of an Attack Detail

Note that in screen after screen NovaCommand provides analysts with summarized data points. As Figure 10 shows, for example, analysts see a graphical representation of attacker IP addresses, attack type(s), and the targeted system(s). Logs are just a click away, but we appreciate how NovaCommand attempts to make analysts' jobs easier by providing what they need up front.

As shown on the left side of Figure 10, NovaCommand also provides its machine learning clustering activity front and center for the user. This represents an interesting perspective: A lot of tools that utilize machine learning do so behind the scenes to help drive alerting and increase fidelity. NovaCommand provides this analysis in the main page—we think, again, to increase an analyst's quick understanding of what the observed activity may represent.

Of course, we can expand each data point and attack observation within the attack description. NovaCommand will also trace key data points to specific log entries. Figure 11 explores this correlation further.



Asset IP	Groups	Hostname	Logs	Percent
192.200.16.193	branch		10	55.56%
				44.44%

Filter: Time (2021–07–08 21:22:47~2021–07–18 23:39:08) \| Attack Type (All) \| Severity (Severe,High,Medium,Low, Very–Low) \| Action (Allow,Deny) \| Src IP (14.135.120.5) \| Src Port (All) \| Dst IP (All) \| Dst Port (All) \|Sender Address (All) \|R...

No.	Time/Period	Severity	Log Type	Type	Detected By	Src IP	Src Type	Dst IP	Dst Type	Status Code	Description
1	2021–07–17 23:46:17	Medium	Exploit	system Vuln...	NovaSensor...	14.135.120.5	Internet	192.200.16.193	Server	–	There is BIND TKEY Query De...
2	2021–07–17 23:46:16	Medium	Exploit	system Vuln...	NovaSensor...	14.135.120.5	Internet	192.200.16.194	Server	–	There is BIND TKEY Query De...

Attacker	Region	Logs	Percent
14.135.120.5	Ningxia Hui Autonomous Region	2	11.11%
125.64.94.136	Sichuan	2	11.11%
92.118.161.33	United States	2	11.11%
205.205.150.5	Canada	2	11.11%
185.173.35.9	Australia	1	5.56%

Figure 11. Snippet of Detailed Alert Activity with Corresponding Logs Highlighted

As Figure 11 shows, the alert overview easily summarizes key alert details for the analysts. However, if necessary, they can also access the "raw" log data in the platform for deeper insight. We can display logs in table or JSON formats and export them easily for sharing or additional analysis off-platform if necessary.

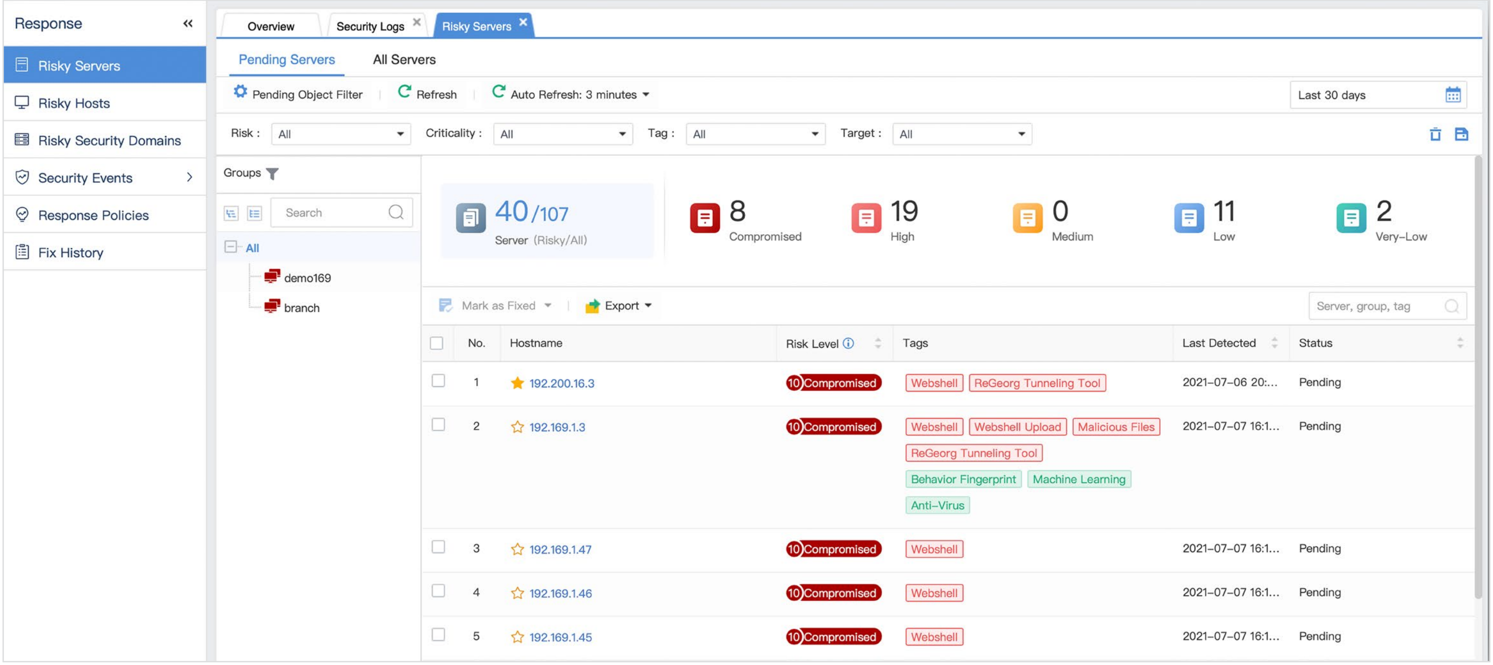
The powerful Detection portion of the NovaCommand platform provides enormous insight into the organization. Our primary finding is that it is quite analyst friendly. Where available, the platform provides summarized insight and data that allow analysts to make quick yet informed decisions. Is the traffic lateral, inbound, or outbound? How many external IP addresses are involved in the attack? What key vulnerability is being exploited? All these critical questions are addressed up front. Analysts need only to dig into raw events if they deem necessary.

By answering key questions, NovaCommand offers another hidden benefit: Analysts need not waste too much time on analysis if the relevant data is presented to them up front. For example, consider an alert of malicious lateral movement between two different subnets. Analysts can design their response procedures around these metadata points rather than design processes to *find* these metadata points. And with faster decision making comes faster response, and less time for adversaries to roam the network.

Incident Response

As we have detailed, NovaCommand provides analysts valuable insight for asset classification and adversary detection. Its response capabilities prove just as powerful, and analysts will certainly welcome them as they look to address the issues that Assets or Detections may have surfaced.

NovaCommand's Response screen proves just as informative as other dashboards and initial screens. Figure 12 shows a screenshot of the initial Response page.



Auto Refresh: 3 minutes

Last 30 days

Risk : All | Criticality : All | Tag : All | Target : All

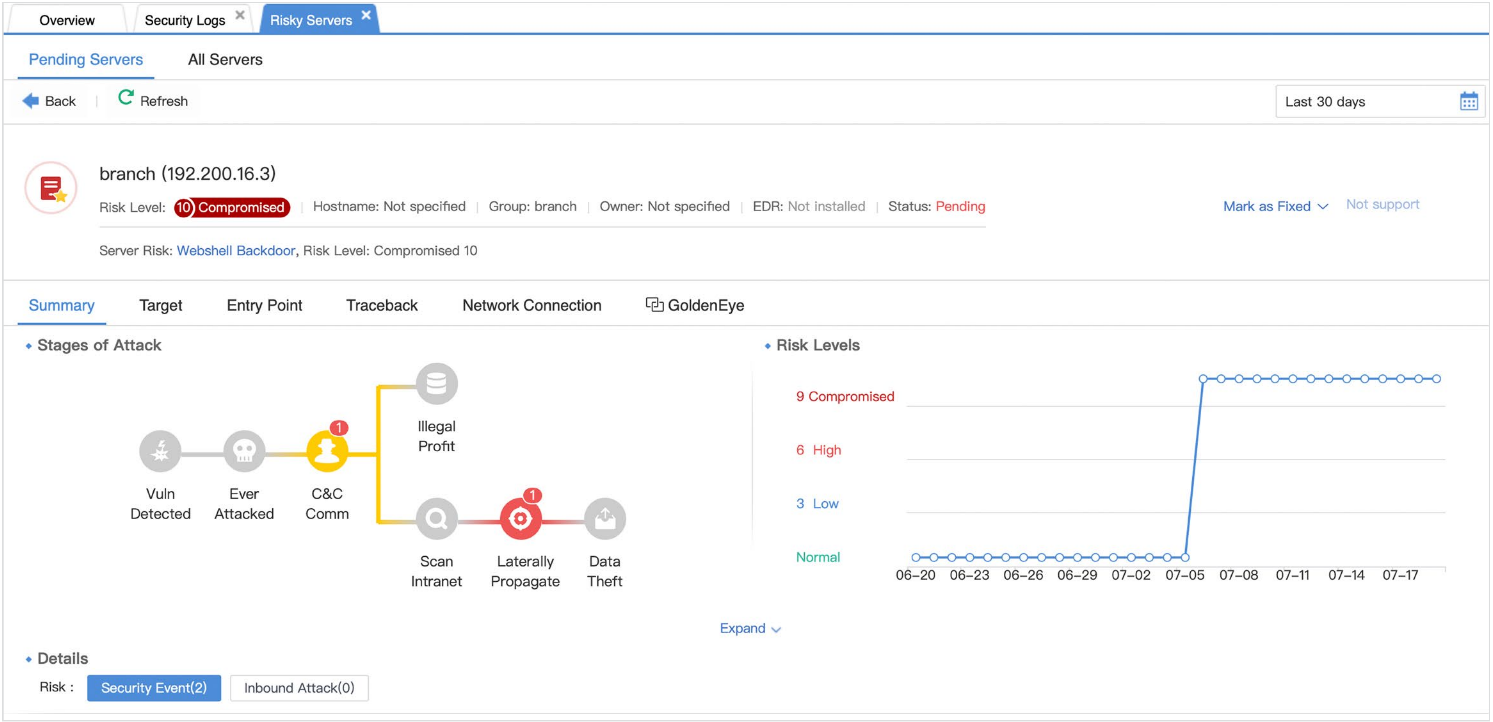
40/107 Server (Risky/All) | 8 Compromised | 19 High | 0 Medium | 11 Low | 2 Very–Low

□	No.	Hostname	Risk Level	Tags	Last Detected	Status
□	1	★ 192.200.16.3	10 Compromised	Webshell ReGeorg Tunneling Tool	2021–07–06 20:...	Pending
□	2	☆ 192.169.1.3	10 Compromised	Webshell Webshell Upload Malicious Files ReGeorg Tunneling Tool Behavior Fingerprint Machine Learning Anti–Virus	2021–07–07 16:1...	Pending
□	3	☆ 192.169.1.47	10 Compromised	Webshell	2021–07–07 16:1...	Pending
□	4	☆ 192.169.1.46	10 Compromised	Webshell	2021–07–07 16:1...	Pending
□	5	☆ 192.169.1.45	10 Compromised	Webshell	2021–07–07 16:1...	Pending

Figure 12. Snippet of the NovaCommand Response Page: Focused on Risky Servers

Just like other screens, NovaCommand provides its own insight and classification. Hosts are once again appropriately classified as risky server or hosts, domains, and security events. As Figure 12 shows, the platform also provides the type of unique high-level insights that can help gauge the state of and need for response within the environment. Figure 12 shows, for example, 40 risky servers, with eight showing compromised status. Below these high-level metrics, NovaCommand provides data similar to that of the Detections screen, including hostname, risk level, event tags, and timestamps. Like the Detections screen, most data points are also interactive and analysts can use them to drill down as necessary.

Drilling into a particular event provides analysts perhaps some of the best metadata about a particular event. Figure 13 examines a compromised system tagged with a web shell and tunneling tool.



branch (192.200.16.3)

Risk Level: 10 Compromised | Hostname: Not specified | Group: branch | Owner: Not specified | EDR: Not installed | Status: Pending

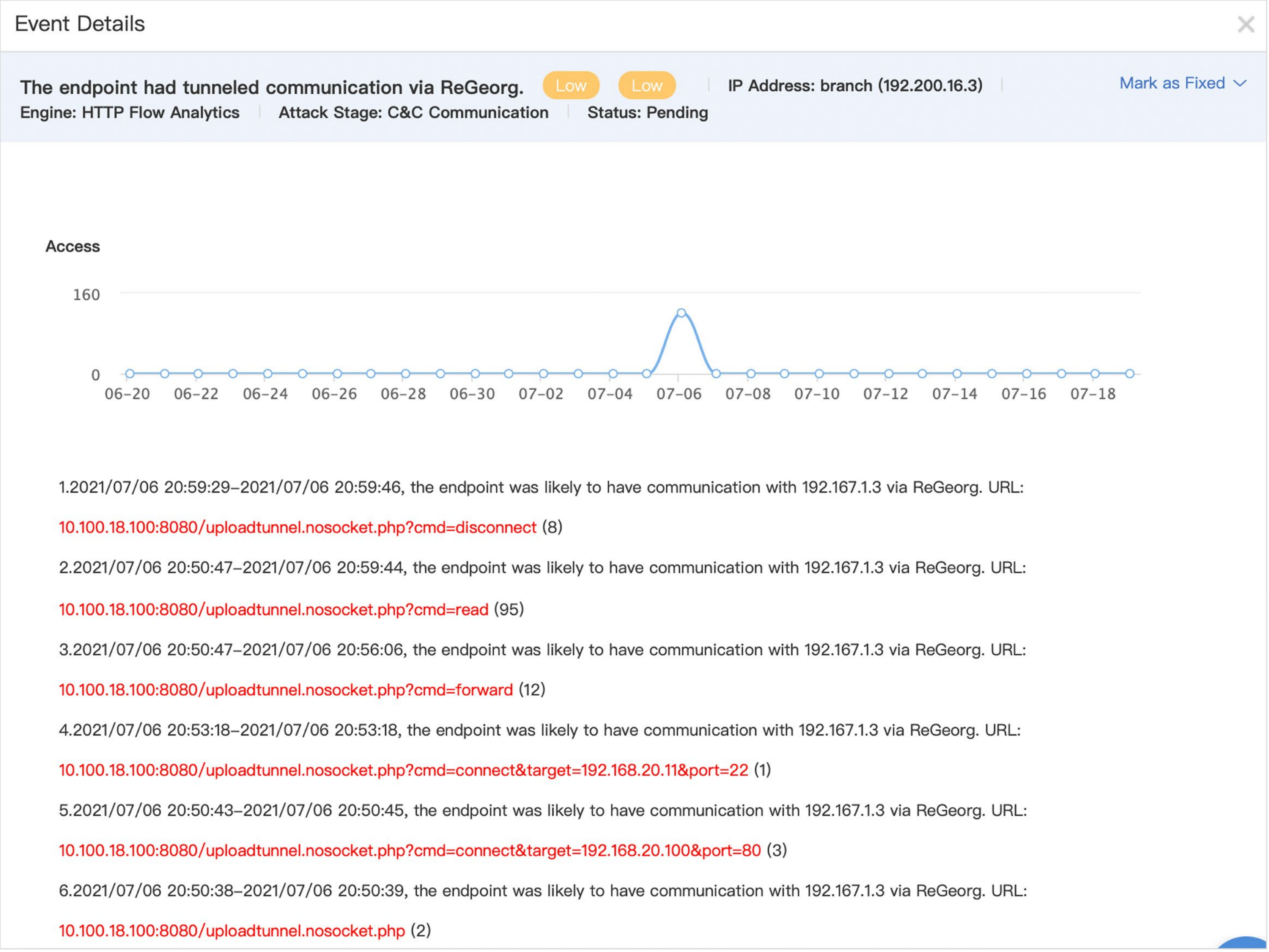
Server Risk: Webshell Backdoor, Risk Level: Compromised 10

Risk : Security Event(2) Inbound Attack(0)

Figure 13. Snippet of a Compromise: Risky Server from the Response Tab

Figure 13 may be our favorite screen of the entire platform. NovaCommand provides an immense amount of data about an incident, including a detailed map of attack stages, a history of observed system criticality, and key stages the adversary has achieved. As this figure shows, NovaCommand recognized that the adversary had achieved C2 communications and lateral movement. The system criticality also increased suddenly, indicating that this malicious activity occurred recently. NovaCommand subsequently escalated the system.

Within the Response tab, we can also drill into a particular event further via the Event Details option (similar to the log entries in Detection). Figure 14 on the next page shows an example of the event details for a detected web shell.



The endpoint had tunneled communication via ReGeorg. | IP Address: branch (192.200.16.3)

Engine: HTTP Flow Analytics | Attack Stage: C&C Communication | Status: Pending

1.2021/07/06 20:59:29–2021/07/06 20:59:46, the endpoint was likely to have communication with 192.167.1.3 via ReGeorg. URL:

10.100.18.100:8080/uploadtunnel.nosocket.php?cmd=disconnect (8)

2.2021/07/06 20:50:47–2021/07/06 20:59:44, the endpoint was likely to have communication with 192.167.1.3 via ReGeorg. URL:

10.100.18.100:8080/uploadtunnel.nosocket.php?cmd=read (95)

3.2021/07/06 20:50:47–2021/07/06 20:56:06, the endpoint was likely to have communication with 192.167.1.3 via ReGeorg. URL:

10.100.18.100:8080/uploadtunnel.nosocket.php?cmd=forward (12)

4.2021/07/06 20:53:18–2021/07/06 20:53:18, the endpoint was likely to have communication with 192.167.1.3 via ReGeorg. URL:

10.100.18.100:8080/uploadtunnel.nosocket.php?cmd=connect&target=192.168.20.11&port=22 (1)

5.2021/07/06 20:50:43–2021/07/06 20:50:45, the endpoint was likely to have communication with 192.167.1.3 via ReGeorg. URL:

10.100.18.100:8080/uploadtunnel.nosocket.php?cmd=connect&target=192.168.20.100&port=80 (3)

6.2021/07/06 20:50:38–2021/07/06 20:50:39, the endpoint was likely to have communication with 192.167.1.3 via ReGeorg. URL:

10.100.18.100:8080/uploadtunnel.nosocket.php (2)

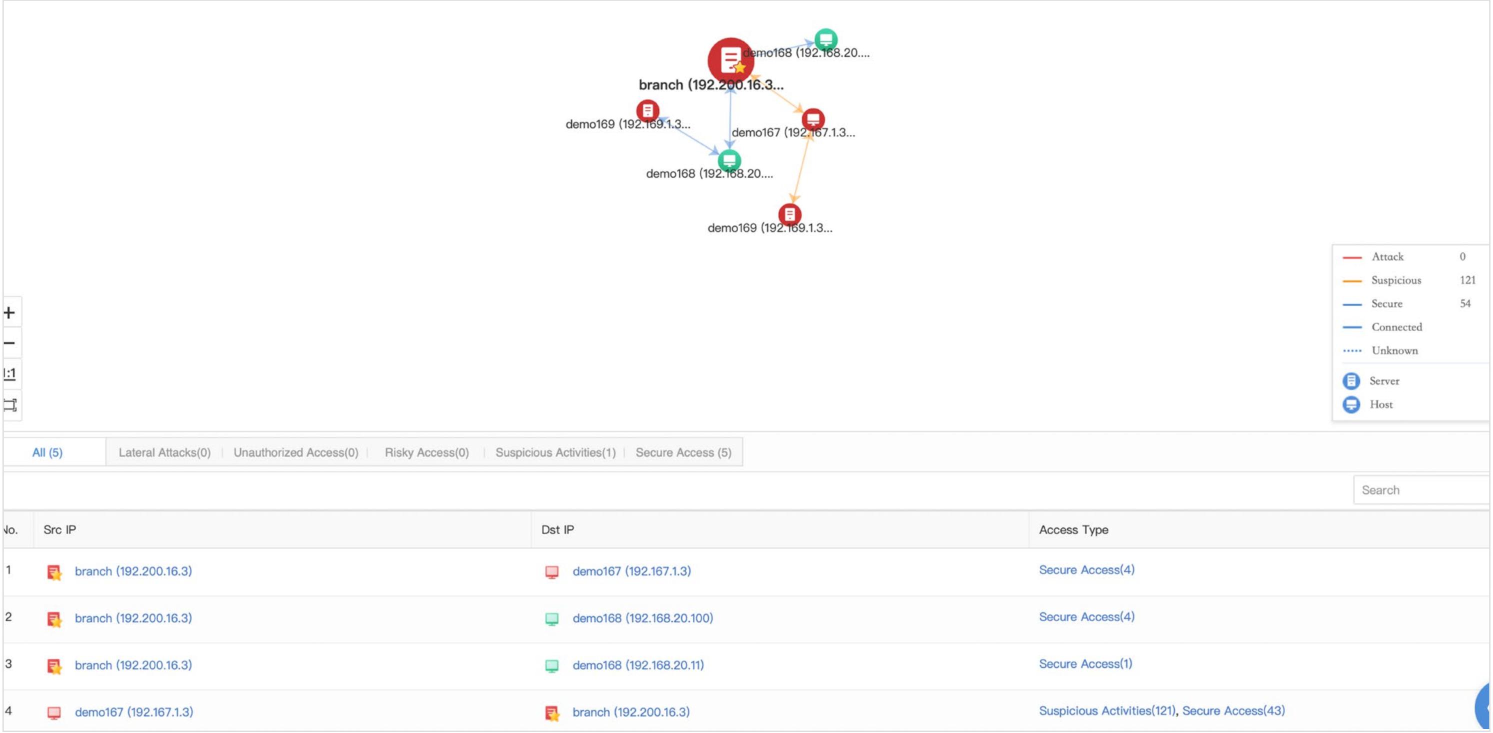
Figure 14. Snippet of Event Details for a Compromised System with a Web Shell Detection

The data points in Figure 14 are typically those that a team might pull as part of an incident response. Instead, NovaCommand brings these data points to the surface, saving analysts time when responding to attacks.

A final feature worth mentioning, and one that analysts will also appreciate to aid in their investigations, is NovaCommand's unique GoldenEye Traceback feature. A searchable field that analysts can put any network indicator into, GoldenEye provides event-based link analysis on key indicators observed in an attack. Figure 15 on the next page provides a snippet of a GoldenEye traceback.

KEY TAKEAWAY

As we emphasized earlier, this type of amplification exemplifies a consistent theme in our review of the NovaCommand platform. Incident responders are used to receiving alerts and needing to dig through logs, PCAPs, and other artifacts to compile the full story of an incident. These activities take time and rely on visibility to be correct. NovaCommand beats analysts to the punch; with visibility, it can compile the story of an attack and allow analysts to remediate faster, limiting the time an adversary has in the environment.



No.	Src IP	Dst IP	Access Type
1	branch (192.200.16.3)	demo167 (192.167.1.3)	Secure Access(4)
2	branch (192.200.16.3)	demo168 (192.168.20.100)	Secure Access(4)
3	branch (192.200.16.3)	demo168 (192.168.20.11)	Secure Access(1)
4	demo167 (192.167.1.3)	branch (192.200.16.3)	Suspicious Activities(121), Secure Access(43)

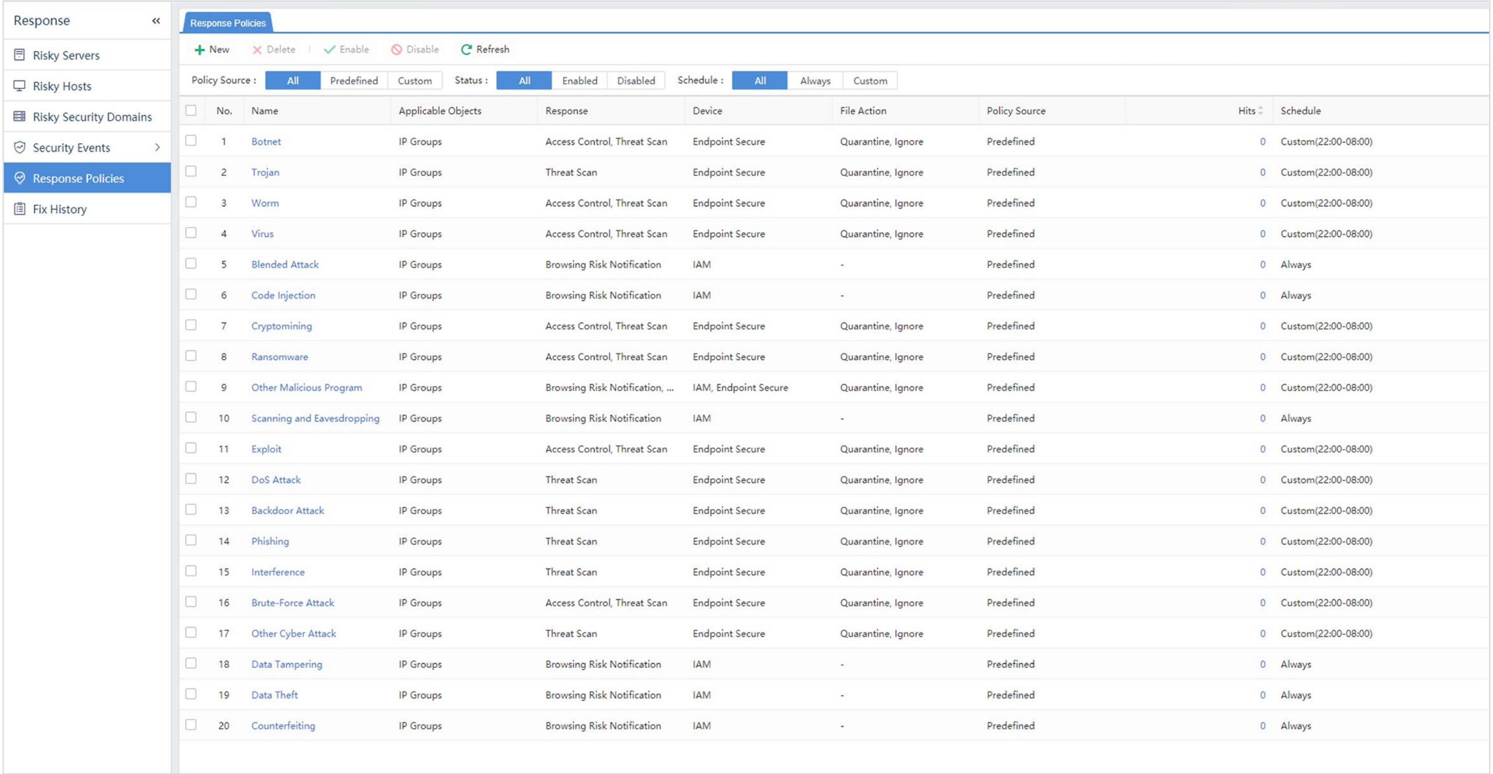
Figure 15. Snippet of a GoldenEye Traceback for a Malicious IP Address

As Figure 15 shows, GoldenEye provides another interesting vantage point for analysts. Rather than compile indicators to identify links to other systems, attacks, or incidents in the environment, they can rely on the platform to make that link for them. This serves as a very useful, forward-thinking feature within the platform. Adversary attacks often include multiple systems, and attempting to manually correlate is another rabbit hole that analysts may know all too well and dread. NovaCommand provides a graphical summary that analysts can click on and follow direct links—with all the metadata and data points we have seen in previous examples.

Automated Response

As an organization's security team, and thus its posture, matures, it will gradually move toward automating certain response processes. Of course, automation comes with a level of confidence in one's security controls. Given the plethora of capabilities we have discussed in previous pages, we can easily determine that analysts can quickly rely on ForeNova as a source of truth for network detection and response. The platform allows security teams to mature past manual analysis with automated response policies.

Tucked within ForeNova's Response options, and shown in Figure 16, we find the incredibly capable Response Policies.

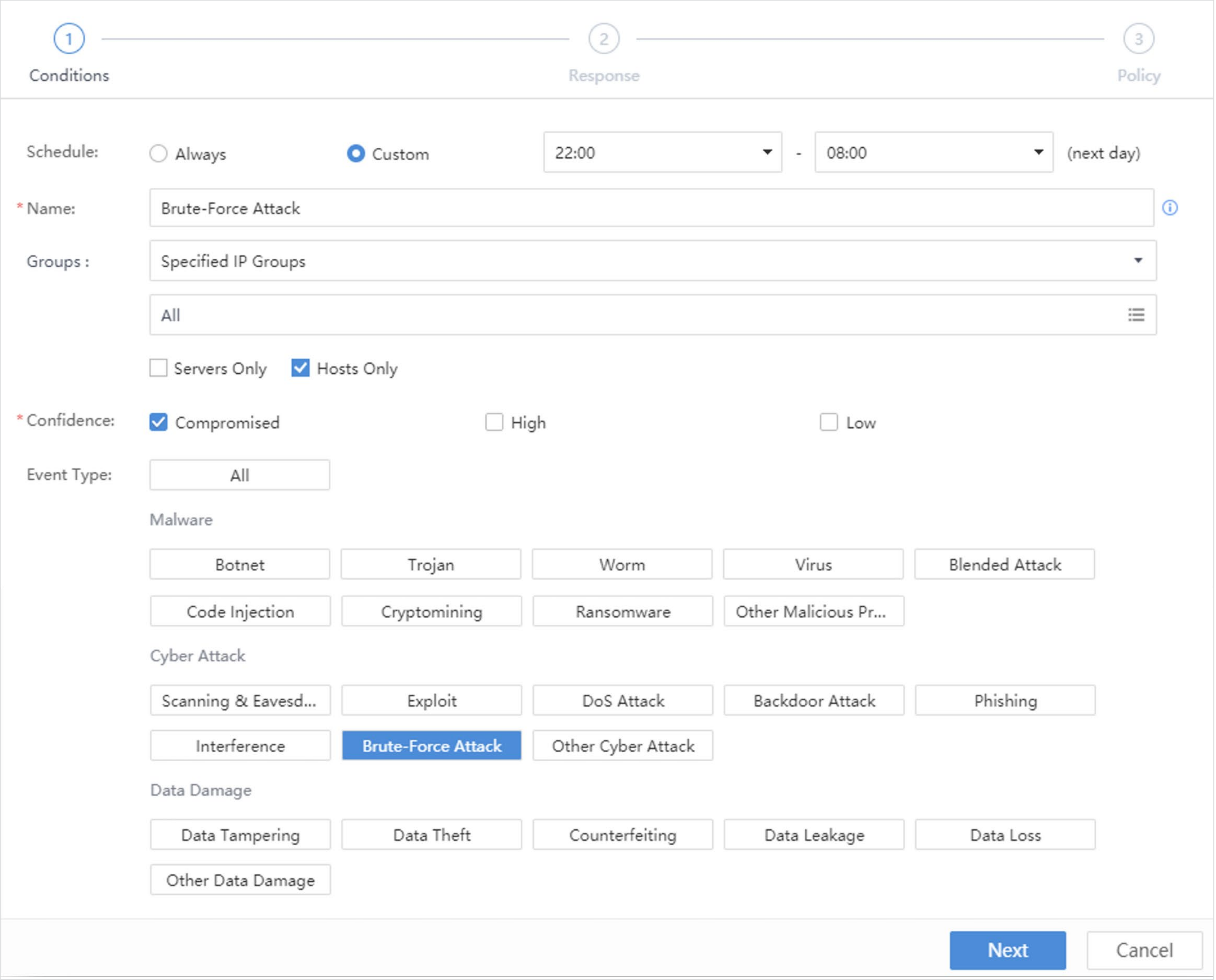


□	No.	Name	Applicable Objects	Response	Device	File Action	Policy Source	Hits	Schedule
□	1	Botnet	IP Groups	Access Control, Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	2	Trojan	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	3	Worm	IP Groups	Access Control, Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	4	Virus	IP Groups	Access Control, Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	5	Blended Attack	IP Groups	Browsing Risk Notification	IAM	-	Predefined	0	Always
□	6	Code Injection	IP Groups	Browsing Risk Notification	IAM	-	Predefined	0	Always
□	7	Cryptomining	IP Groups	Access Control, Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	8	Ransomware	IP Groups	Access Control, Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	9	Other Malicious Program	IP Groups	Browsing Risk Notification, ...	IAM, Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	10	Scanning and Eavesdropping	IP Groups	Browsing Risk Notification	IAM	-	Predefined	0	Always
□	11	Exploit	IP Groups	Access Control, Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	12	DoS Attack	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	13	Backdoor Attack	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	14	Phishing	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	15	Interference	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	16	Brute-Force Attack	IP Groups	Access Control, Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	17	Other Cyber Attack	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)
□	18	Data Tampering	IP Groups	Browsing Risk Notification	IAM	-	Predefined	0	Always
□	19	Data Theft	IP Groups	Browsing Risk Notification	IAM	-	Predefined	0	Always
□	20	Counterfeiting	IP Groups	Browsing Risk Notification	IAM	-	Predefined	0	Always

Figure 16. Snippet of ForeNova's Response Policies from the Response Tab

As Figure 16 shows, Response Policies combine ForeNova's threat intelligence, third-party product integration, and built-in detection/response capabilities. They allow a security team to automate a response to a particular event, all with the granular control and asset visibility we have reviewed in previous sections.

Creating a response policy is as simple as asking, “What do you want the platform to do in the event of an attack?” Let’s walk through the creation of a policy. Figure 17 provides a snippet of conditions available when creating a Response Policy.



Schedule: ○ Always ● Custom 22:00 - 08:00 (next day)

* Name: Brute-Force Attack

Groups : Specified IP Groups

All

□ Servers Only ☑ Hosts Only

* Confidence: ☑ Compromised □ High □ Low

Event Type: All

Malware

Botnet | Trojan | Worm | Virus | Blended Attack | Code Injection | Cryptomining | Ransomware | Other Malicious Pr...

Cyber Attack

Scanning & Eavesd... | Exploit | DoS Attack | Backdoor Attack | Phishing | Interference | **Brute-Force Attack** | Other Cyber Attack

Data Damage

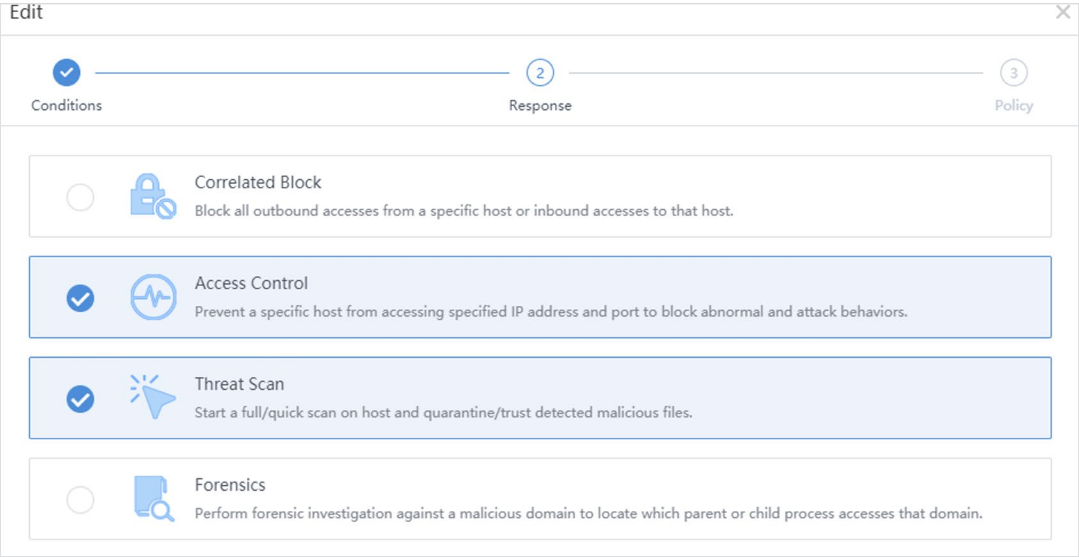
Data Tampering | Data Theft | Counterfeiting | Data Leakage | Data Loss | Other Data Damage

Figure 17. Snippet of the Conditions Tab from a Response Policy

Note that analysts can select specific groups, employ ForeNova’s confidence levels, and specify an event based on attack types. This provides a significant advantage for defenders because they do not need to write code or rules to determine what a “brute-force attack” might be; ForeNova abstracts this away from analysts, instead letting them focus on creating effective policies.

Figure 18 looks at the next step: What do you want the platform to do?

Figure 18 shows where analysts can truly level up their automated capabilities. Whereas analysts might be used to simply automating a firewall block, with ForeNova they can take advantage of advanced automations such as limiting access controls, running a threat scan on the system, and even automatically pulling forensic artifacts!



○ Correlated Block
Block all outbound accesses from a specific host or inbound accesses to that host.

✓ Access Control
Prevent a specific host from accessing specified IP address and port to block abnormal and attack behaviors.

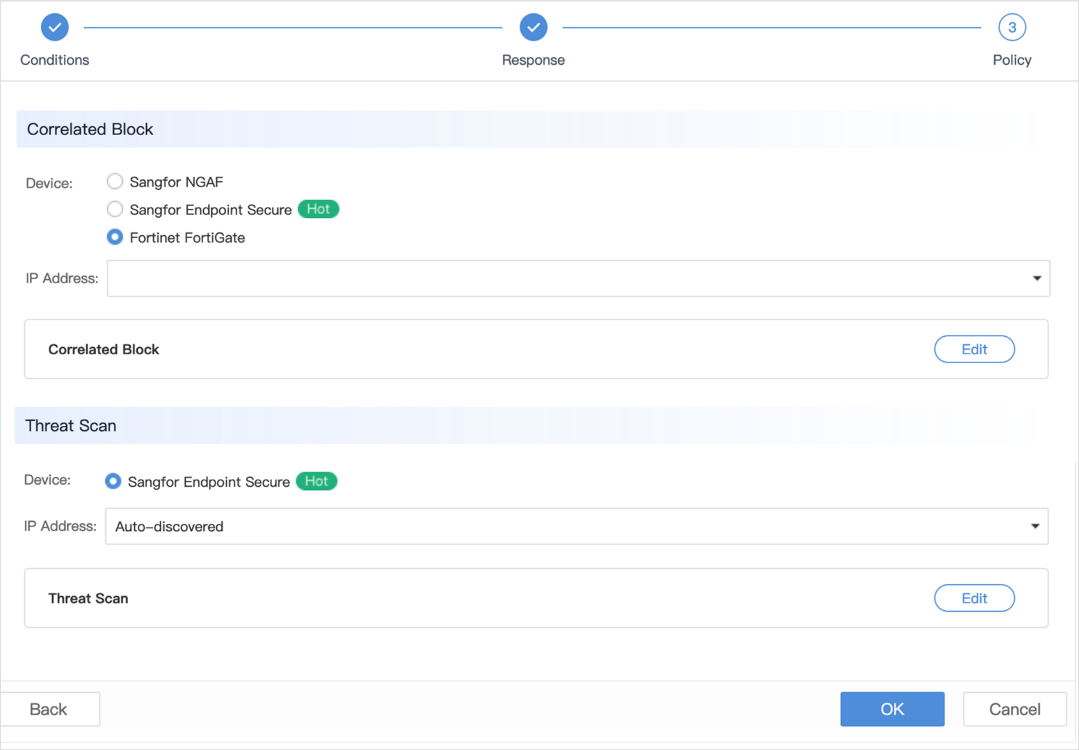
✓ Threat Scan
Start a full/quick scan on host and quarantine/trust detected malicious files.

○ Forensics
Perform forensic investigation against a malicious domain to locate which parent or child process accesses that domain.

Figure 18. Snippet of the Response Tab from a Response Policy

Finally, in Figure 19, we see available integration(s) to put the chosen policies into effect.

The Policy options allow the analysts to extend their automated response further by utilizing third-party tools to implement host scans or maintain access control (to list two among many examples). Here the platform sets itself apart from others in yet another area: Instead of forcing analysts to utilize *only* its platform, ForeNova allows analysts to bring multiple security controls together. The value here is that if an organization currently lacks NDR capabilities, they can easily implement *on top of* their current stack and allow network alerts to drive host-based policies.



Correlated Block

Device: ○ Sangfor NGAF
○ Sangfor Endpoint Secure Hot
● Fortinet FortiGate

IP Address:

Correlated Block Edit

Threat Scan

Device: ● Sangfor Endpoint Secure Hot

IP Address: Auto-discovered

Threat Scan Edit

Figure 19. Snippet of the Policy Tab from a Response Policy

Closing Thoughts

Network detection and response are not easy tasks. It can be an enormous undertaking to capture and enrich all the traffic an enterprise might observe. However, as we worked through the NovaCommand platform, our theme remained consistent: NovaCommand makes analysts jobs' easier. As an NDR platform, it does an excellent job of collating, correlating, and enriching events to help identify malicious activity within an enterprise network. Through automated asset and incident classification and enrichment, we constantly had the most important questions answered *first*, rather than needing to go dig up the answers.

"You cannot protect what you cannot see" remains true. Adversaries continue to find success day after day, with the year 2021 alone showing record ransomware extortion demands and attacks that have disrupted critical industries of multiple countries. If there were ever a time to seize back the advantage, that time is now. If you currently do not utilize network detection and response, you are ignoring a critical part of your enterprise that adversaries, thankfully, cannot evade.

About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a principal consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

FORENOVA