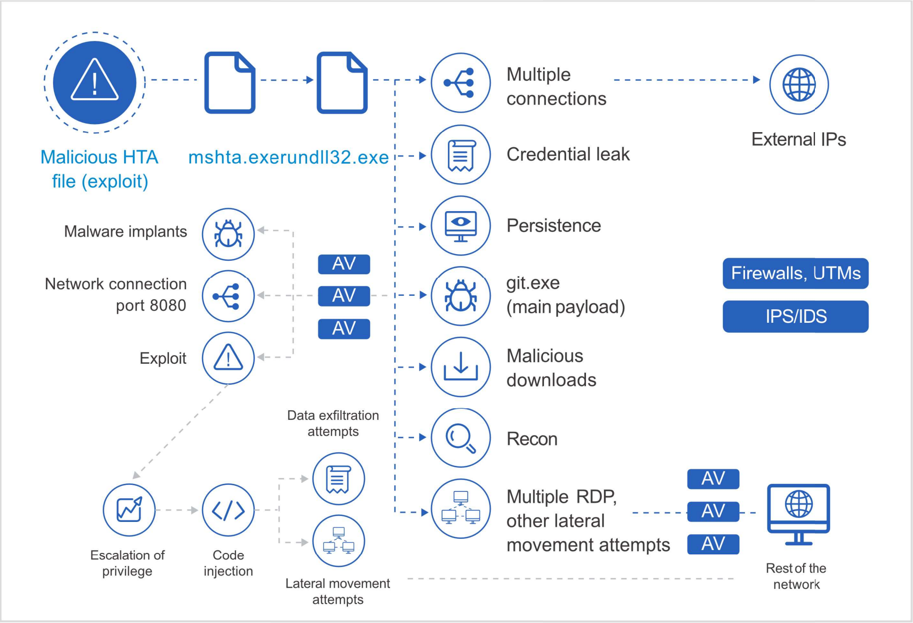
FORENOVA
SECURITY

ForeNova
NovaCommand

NovaCommand: Intelligent Threat Detection and Response Platform

www.forenova.com

Typical Cyber Security Approach



Focused on prevention

Attacks still bypass existing controls

Incident Response requires advanced expertise

Security operation is time consuming and ineffective

Operation and Management has limited visibility

Security Operation Challenges

01 Limited prevention allows for attacks to bypass existing security control

- Regardless of security technology, misconfigurations or missing controls are always the weakest link.
- Most security preventions rely on signature-based techniques (AV, NGFW and IPS),and often misidentify new or variant malware strains or abnormal behaviors.

02 Time Consuming Security Operation: Advanced Expertise Provides Limited Results

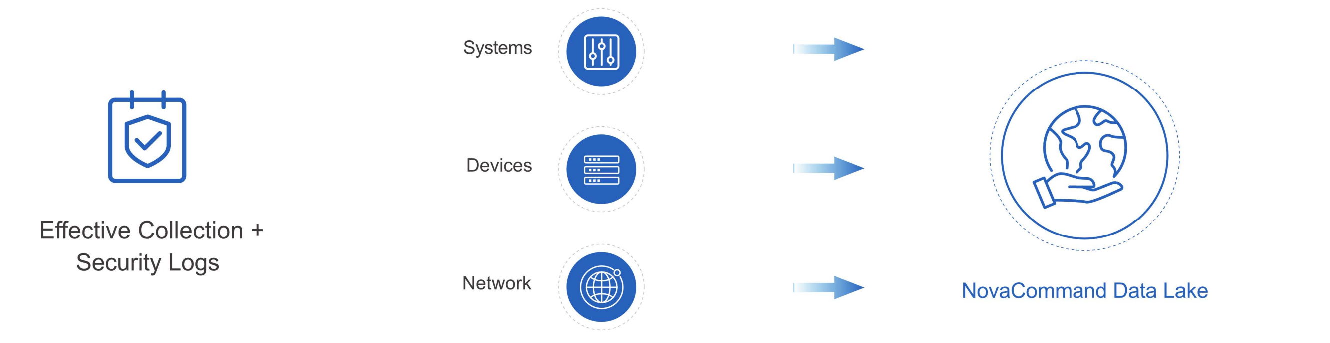
- With security logs being generated from many sources (networks, endpoints, servers, database, applications, authentications), many alerts are also generated, making total security time consuming and difficult to master.
- Security analytics require administrators with security expertise, as average logs and consoles are difficult to read and understand.

03 Poor Visibility Means Poor Threat Detection & Identification

- Without a comprehensive view of any network threats, even the most skilled administrators will struggle and fail to protect the network from what they can’t see.

NovaCommand

NovaCommand platform significantly improves overall security detection and response capabilities by monitoring internal network traffic, correlating existing security events, applying AI and behavior analysis, all aided by global threat intelligence. Unlike other solutions, NovaCommand uncovers breaches of existing security controls while impact analysis identifies hidden threat within the network. Because NovaCommand integrates network and endpoint security solutions,administrator's ability to navigate and understand the overall threat landscape is significantly improved, and response to threat is automated and simplified. NovaCommand can be trusted to improve overall IT security and risk posture.



Effective Collection + Security Logs

Systems

Devices

Network

NovaCommand Data Lake

Sophisticated *Detection*

Detection

Engine zero	AI
UEBA	NTA
TI	Endpoint Secure
NGAF	Others

Simplify Threat *Hunting*

Threat Hunting

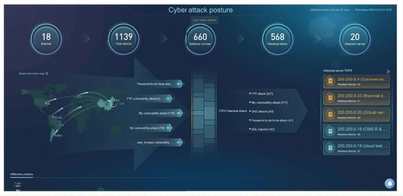
- Attack chain analysis
- Contextual verification
- Attack sorting
- Attack Path
- Security incident alert

Faster and More Efficient*Response*

Response

- Block open ports
- Scan for other malware
- Quarantine
- Stop processes
- Shut down C&C Connections

Comprehensive Visibility



Key Features

1 Sophisticated ***Detection***by closely monitoring every step of the cybersecurity attack chain.

The NovaCommand Analysis Center collects a broad range of network and security data including North-South and East-Westtraffic data, logs from network gateways and EDRs,decodes it using network applications like DNS or mail, and applies AI analysis to uncover undesirable behavior. As NovaCommand is paired with threat intelligence, attacks on all level of the attack chain are detected, meaning faster alerts to exploitation attempts, slow brute force attacks, C&Cactivities, lateral movements, P2P traffic, and data theft.

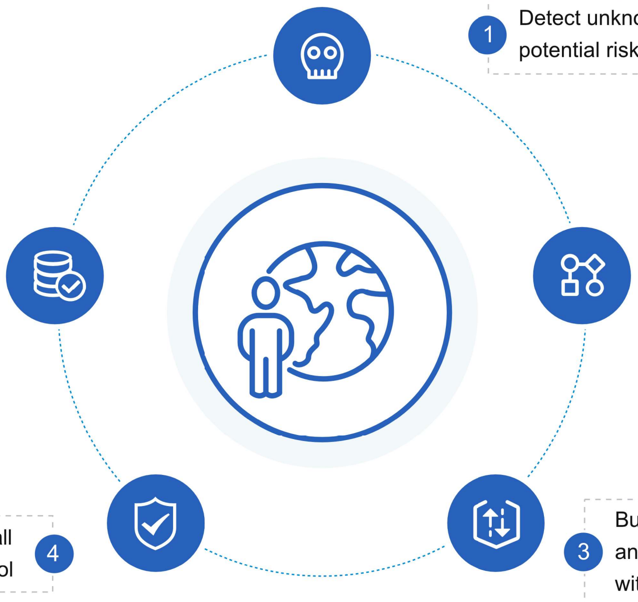
2 Faster and More Efficient ***Response***delivered using incident investigation and tight integration with network and endpoint security solutions.

The NovaCommand Response Center provides a broad range of attack investigation experience, all presented visually within the attack chain. Threat mitigation is prioritized based on the criticality of the at-risk business assets. Combined with EDR and NGFW security solutions, NovaCommand provides flexible and effective mitigation in a timely manner,offering recommendations for policy or patching, endpoint correlation and network correlation.

3 Simplify Threat ***Hunting***

NovaCommand helps security administrators to perform comprehensive impact analysis of known breaches and to track “patient zero,” by evaluating all possible points of entrance. NovaCommand’s unique “Golden Eye” feature studies the behavior of compromised assets like inbound and outbound connections and usage of ports and protocols, and uses this valuable information to strengthen external and internal system defenses.

Solution Benefits



1 Detect unknown threats that pose potential risk to the organization

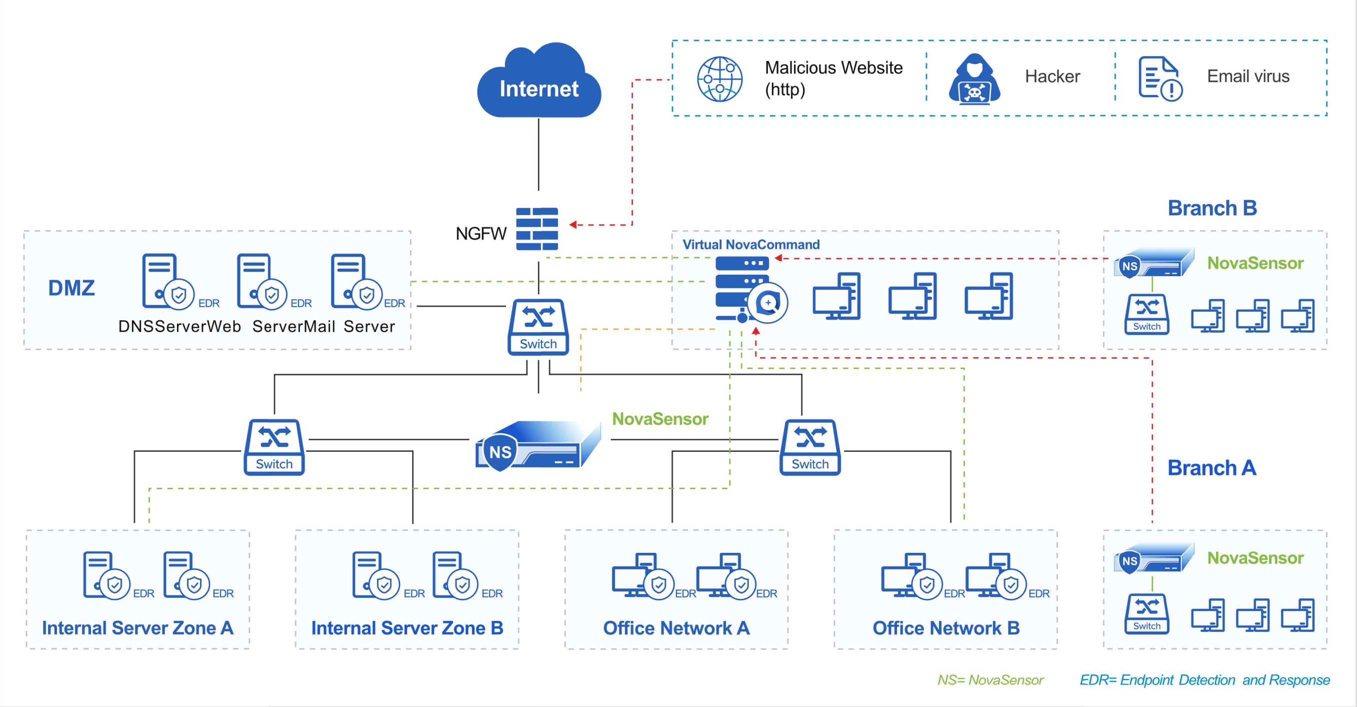
2 Better visibility of infrastructure security posture

3 Business Impact Analysis detects any compromised areas and helps with prioritization of mitigation

4 Faster response improves overall security control

5 More cost effective than other solutions (ex. SIEM)

NovaCommand Deployment



Deployment

NovaCommand is easily deployed within your data centers and branches offices without changes to your network or security settings.

NovaCommand

NovaCommand collects data from NovaSensor sensor and other sources of data origin, normalizes, correlates the data, and presents threat detection, threat hunting and response capabilities.

NovaSensor

NovaSensor is a sensor that collects raw network traffic that is mirrored from switches, extracts security events, detects abnormal behaviors. NovaSensor only forwards less than 1%of the data to NovaCommand.

Neural-X (Threat Intelligence)

Neural-X is a rich source or threat intelligence that contains known IP, URLand files of known attacks. It is also a powerful analytic platform that contains artificial intelligence and sandboxing.

NGFW

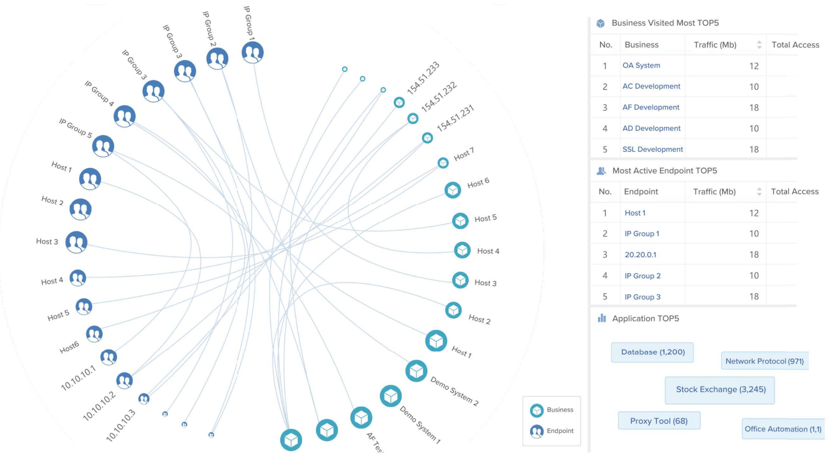
NovaCommand integrates with popular Next Generation Application Firewall to achieve better detection and response, by analyzing logs from NGFWand instructing NGFWto block threats identified by NovaCommand.

EDR

Endpoint Detection and Response (EDR)detects and prevents malware on PCs and servers. NovaCommand integrates with popular EDRs to collect rich sets of evidence for analysis, and quarantine threats identified by NovaCommand.

Simpler Security Visualization

Clear Business and Access Relationship (Access Relationship Chart)



Business Visited Most TOP5

No.	Business	Traffic (Mb)	Total Access
1	OA System	12	
2	AC Development	10	
3	AF Development	18	
4	AD Development	10	
5	SSL Development	18	

Most Active Endpoint TOP5

No.	Endpoint	Traffic (Mb)	Total Access
1	Host 1	12	
2	IP Group 1	10	
3	20.20.0.1	18	
4	IP Group 2	10	
5	IP Group 3	18	

Application TOP5

Database (1,200)

Network Protocol (971)

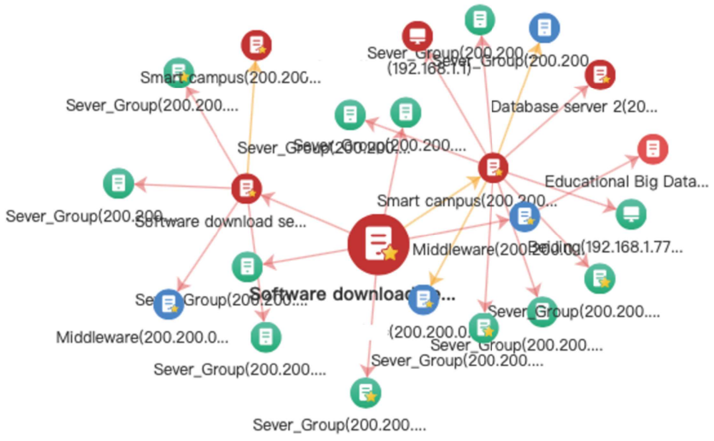
Stock Exchange (3,245)

Proxy Tool (68)

Office Automation (1,1)

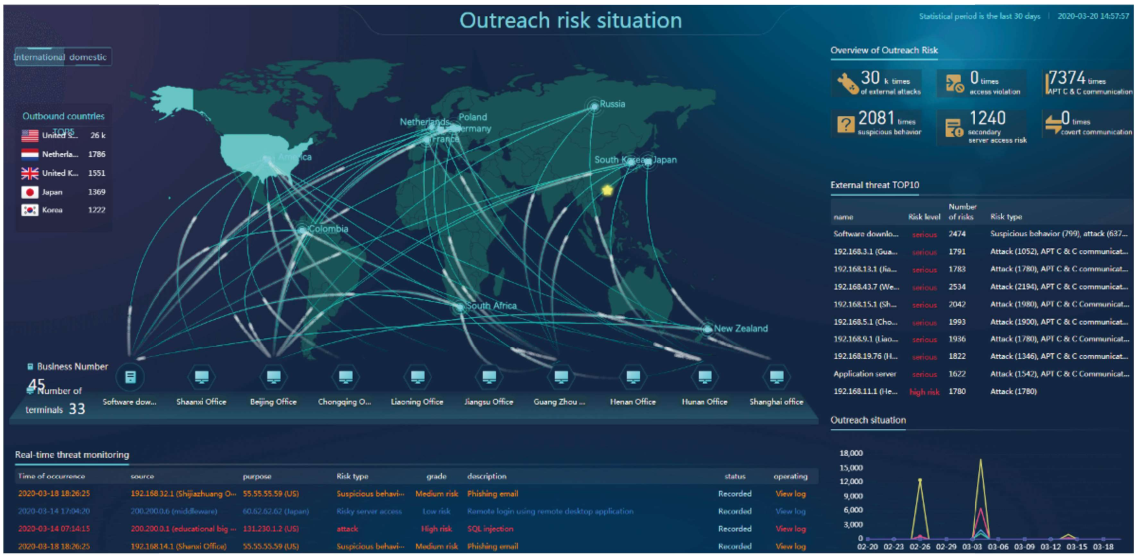
Through automatic identification and asset management, ForeNova NovaCommand enables end to end, effective management and control of the network and all business assets. Based on visualization technology, it clearly displays the access relationships among users, businesses and the Internet, as well as potential risk.

Clear Threat Influence (Latent Threat Golden Eye)



The latent threat detection engine, Golden Eye, evaluates threat influence in multiple dimensions, detecting the "who," "what," "when," "where," and "why" of an attack, and presenting it visually, in an easy to read and understand format.

Global Visualization Aids Decision-Making (Business Outreach Risk Screen)



Outreach risk situation

Statistical period is the last 30 days | 2020-03-20 14:57:57

International domestic

Outbound countries TOP5

United S...	26 k
Netherla...	1786
United K...	1551
Japan	1369
Korea	1222

Business Number 45

Number of terminals 33

Overview of Outreach Risk

30 k times of external attacks

0 times access violation

7374 times APT C & C communication

2081 times suspicious behavior

1240 secondary server access risk

0 times covert communication

External threat TOP10

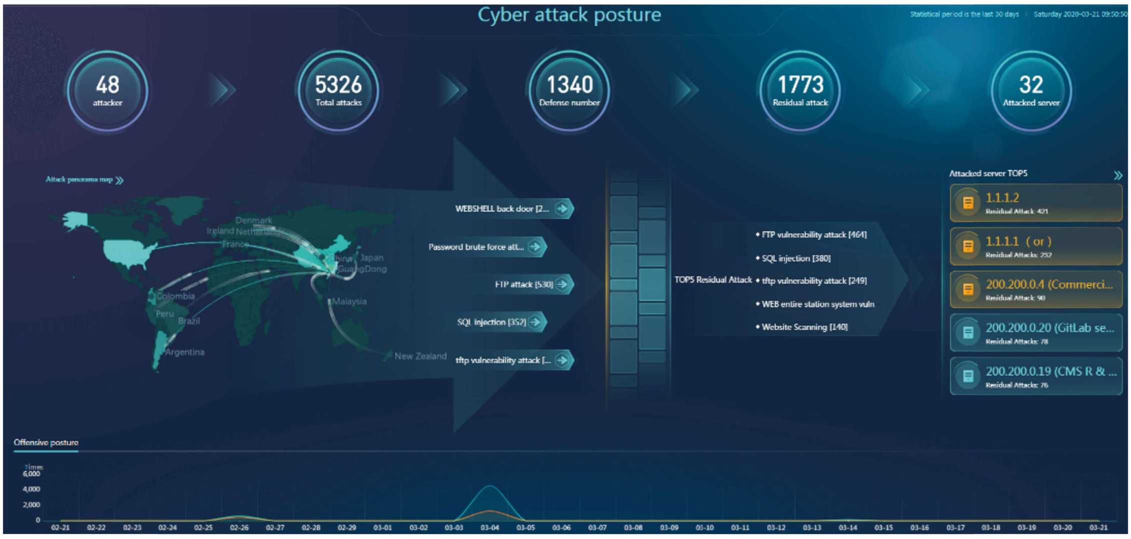
name	Risk level	Number of risks	Risk type
Software downlo...	serious	2474	Suspicious behavior (799), attack (637...
192.168.3.1 (Gua...	serious	1791	Attack (1052), APT C & C communicat...
192.168.13.1 (Jia...	serious	1783	Attack (1780), APT C & C communicat...
192.168.43.7 (We...	serious	2534	Attack (2194), APT C & C communicat...
192.168.15.1 (Sh...	serious	2042	Attack (1980), APT C & C Communicat...
192.168.5.1 (Cho...	serious	1993	Attack (1900), APT C & C communicat...
192.168.9.1 (Liao...	serious	1936	Attack (1780), APT C & C Communicat...
192.168.19.76 (H...	serious	1822	Attack (1346), APT C & C communicat...
Application server	serious	1622	Attack (1542), APT C & C Communicat...
192.168.11.1 (He...	high risk	1780	Attack (1780)

Real-time threat monitoring

Time of occurrence	source	purpose	Risk type	grade	description	status	operating
2020-03-18 18:26:25	192.168.32.1 (Shijiazhuang O...	55.55.55.59 (US)	Suspicious behavi...	Medium risk	Phishing email	Recorded	View log
2020-03-14 17:04:20	200.200.0.6 (middleware)	60.62.62.62 (Japan)	Risky server access	Low risk	Remote login using remote desktop application	Recorded	View log
2020-03-14 07:14:15	200.200.0.1 (educational big ...	131.230.1.2 (US)	attack	High risk	SQL injection	Recorded	View log
2020-03-18 18:26:25	192.168.14.1 (Shanxi Office)	55.55.55.59 (US)	Suspicious behavi...	Medium risk	Phishing email	Recorded	View log

Through real-time monitoring and overall evaluation of the external regions of the network, threat type, and business risk in addition to the latest events and the global threat climate, ForeNova NovaCommand effectively controls both the internal and external security status, enabling all-around security analysis and intelligent decision making.

Global Visualization Aids Decision-Making (External Attack Situation)



Cyber attack posture

Statistical period is the last 30 days | Saturday 2020-03-21 09:50:50

48 attacker

5326 Total attacks

1340 Defense number

1773 Residual attack

32 Attacked server

TOP5 Residual Attack

- FTP vulnerability attack [464]
- SQL injection [380]
- tftp vulnerability attack [249]
- WEB entire station system vuln
- Website Scanning [140]

Attacked server TOP5

1.1.1.2
Residual Attack: 421

1.1.1.1 (or)
Residual Attacks: 232

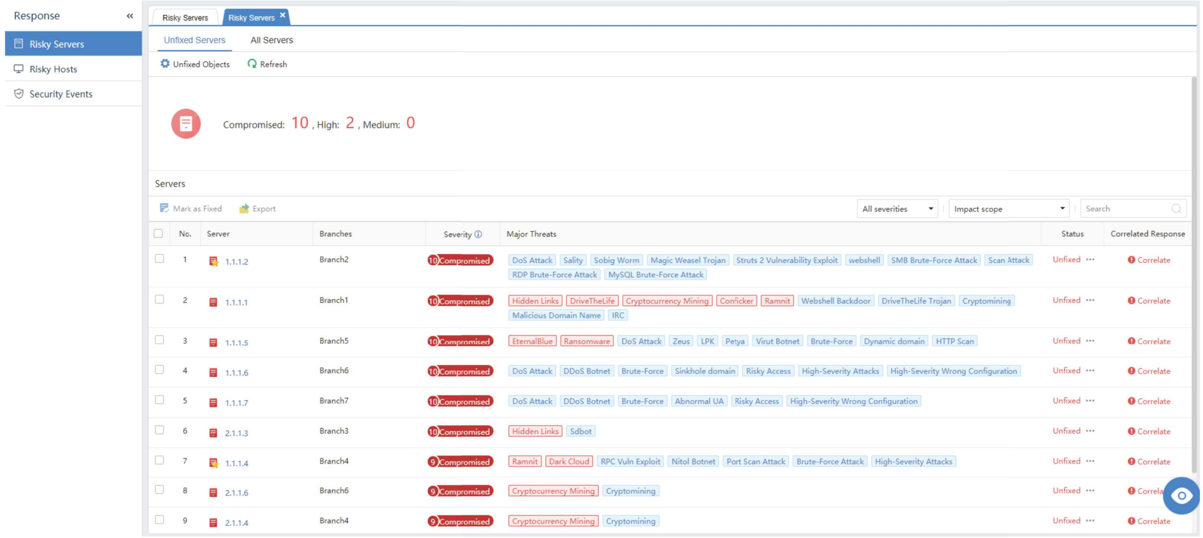
200.200.0.4 (Commerci...
Residual Attack: 90

200.200.0.20 (GitLab se...
Residual Attacks: 78

200.200.0.19 (CMS R & ...
Residual Attacks: 76

Through the real-time monitoring and overall evaluation of external attack times, sources, targets, types and other multi-dimensional information, ForeNova NovaCommand effectively controls external risk to the business and facilitates intelligent security analysis and decision-making.

Micro Visualization Aids Decision Making (Asset Losses)


Response «
Risky Servers
Risky Hosts
Security Events
Risky Servers | Risky Servers ×
Unfixed Servers | All Servers
Unfixed Objects | Refresh

Compromised: 10 , High: 2 , Medium: 0

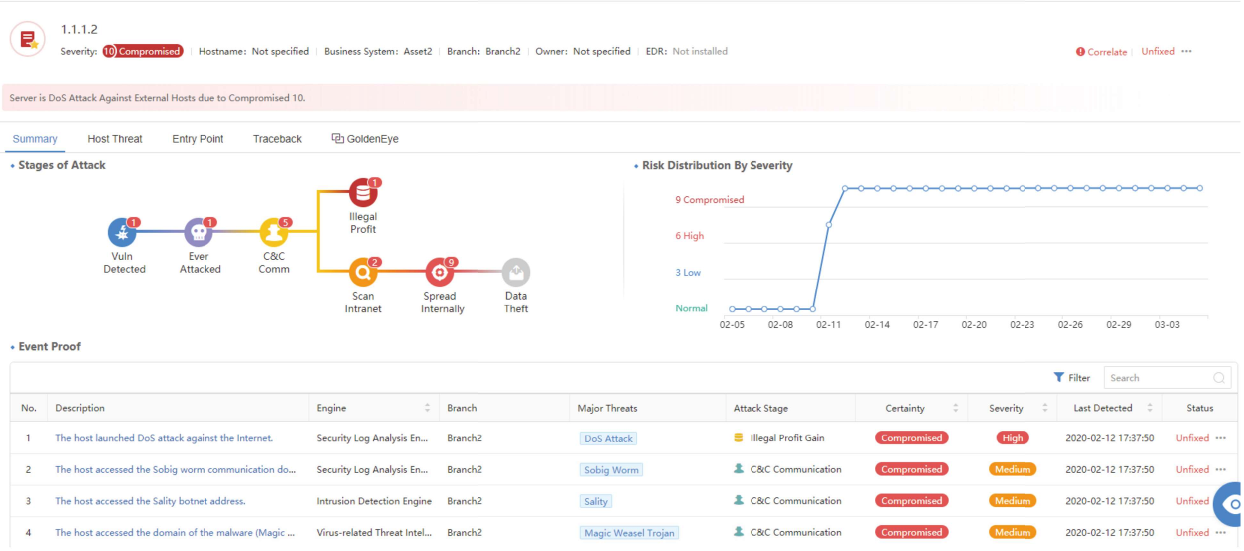
Servers

Mark as Fixed | Export
All severities ▾ | Impact scope ▾ | Search

□	No.	Server	Branches	Severity ⓘ	Major Threats	Status	Correlated Response
□	1	1.1.1.2	Branch2	10 Compromised	DoS Attack, Sality, Sobig Worm, Magic Weasel Trojan, Struts 2 Vulnerability Exploit, webshell, SMB Brute-Force Attack, Scan Attack, RDP Brute-Force Attack, MySQL Brute-Force Attack	Unfixed ···	Correlate
□	2	1.1.1.1	Branch1	10 Compromised	Hidden Links, DriveTheLife, Cryptocurrency Mining, Conficker, Ramnit, Webshell Backdoor, DriveTheLife Trojan, Cryptomining, Malicious Domain Name, IRC	Unfixed ···	Correlate
□	3	1.1.1.5	Branch5	10 Compromised	EternalBlue, Ransomware, DoS Attack, Zeus, LPK, Petya, Virut Botnet, Brute-Force, Dynamic domain, HTTP Scan	Unfixed ···	Correlate
□	4	1.1.1.6	Branch6	10 Compromised	DoS Attack, DDoS Botnet, Brute-Force, Sinkhole domain, Risky Access, High-Severity Attacks, High-Severity Wrong Configuration	Unfixed ···	Correlate
□	5	1.1.1.7	Branch7	10 Compromised	DoS Attack, DDoS Botnet, Brute-Force, Abnormal UA, Risky Access, High-Severity Wrong Configuration	Unfixed ···	Correlate
□	6	2.1.1.3	Branch3	10 Compromised	Hidden Links, Sdbot	Unfixed ···	Correlate
□	7	1.1.1.4	Branch4	9 Compromised	Ramnit, Dark Cloud, RPC Vuln Exploit, Nitol Botnet, Port Scan Attack, Brute-Force Attack, High-Severity Attacks	Unfixed ···	Correlate
□	8	2.1.1.6	Branch6	9 Compromised	Cryptocurrency Mining, Cryptomining	Unfixed ···	Correla
□	9	2.1.1.4	Branch4	9 Compromised	Cryptocurrency Mining, Cryptomining	Unfixed ···	Correlate

Evaluates the overall security posture from a business perspective and visually displays any lost assets, rather than simply listing the number of security incidents.

Micro Visualization Aids Decision Making (Attack Chain Collapse Phase)


1.1.1.2

Severity: 10 Compromised | Hostname: Not specified | Business System: Asset2 | Branch: Branch2 | Owner: Not specified | EDR: Not installed

Correlate | Unfixed ···

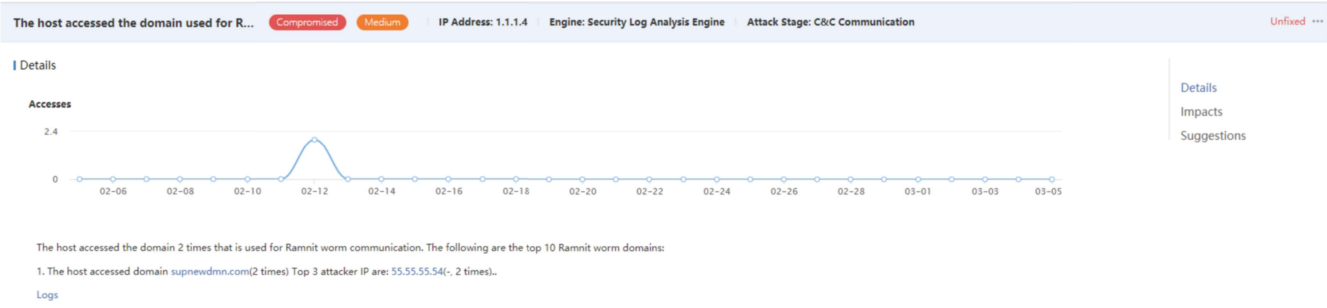
Server is DoS Attack Against External Hosts due to Compromised 10.

Event Proof

No.	Description	Engine	Branch	Major Threats	Attack Stage	Certainty	Severity	Last Detected	Status
1	The host launched DoS attack against the Internet.	Security Log Analysis En...	Branch2	DoS Attack	Illegal Profit Gain	Compromised	High	2020-02-12 17:37:50	Unfixed ···
2	The host accessed the Sobig worm communication do...	Security Log Analysis En...	Branch2	Sobig Worm	C&C Communication	Compromised	Medium	2020-02-12 17:37:50	Unfixed ···
3	The host accessed the Sality botnet address.	Intrusion Detection Engine	Branch2	Sality	C&C Communication	Compromised	Medium	2020-02-12 17:37:50	Unfixed
4	The host accessed the domain of the malware (Magic ...	Virus-related Threat Intel...	Branch2	Magic Weasel Trojan	C&C Communication	Compromised	Medium	2020-02-12 17:37:50	Unfixed ···

Targeting specific lost assets, the attack chain is used to provide proof of the severity of an attack, facilitating easy assessment of any asset loss and showing the attack process and current stage quickly and clearly.

Micro Visualization Aids Decision Making (Detailed Evidence of Lost Assets)



The host accessed the domain used for R... Compromised Medium | IP Address: 1.1.1.4 | Engine: Security Log Analysis Engine | Attack Stage: C&C Communication Unfixed ···

Details

The host accessed the domain 2 times that is used for Ramnit worm communication. The following are the top 10 Ramnit worm domains:

1. The host accessed domain supnewdmn.com(2 times) Top 3 attacker IP are: 55.55.55.54(-, 2 times)..

Logs

Detailed analysis of attacks and abnormal activities are logged and sorted by security incident, and finally clearly displayed, forgoing the more traditional complex logging report method.

Micro Visualization Aids Decision Making (Detailed Suggestions on the Disposal of Lost Assets and Specialized Kill Tools)

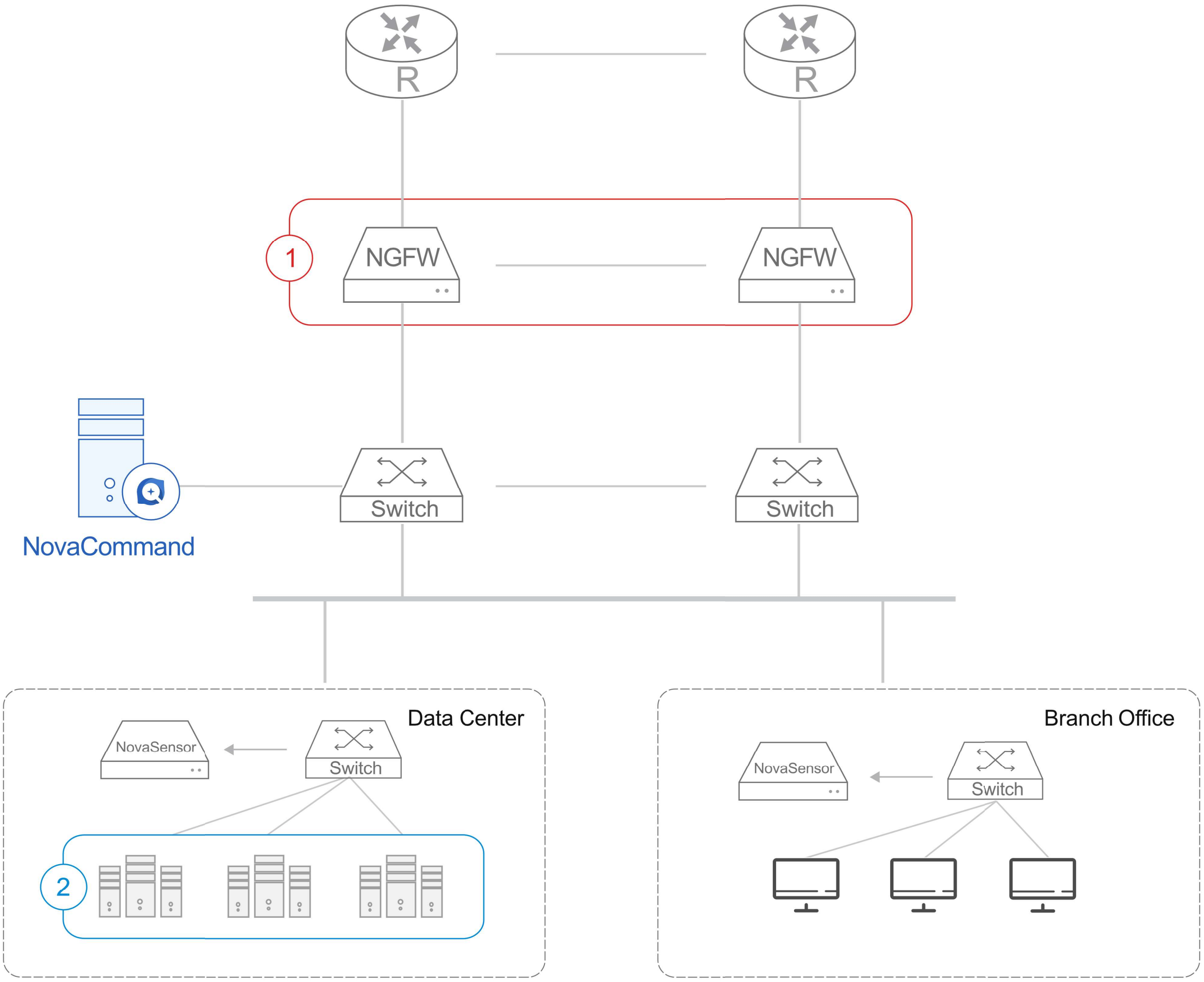
Suggestions

1.Check whether the host is a DNS server or AD domain server (DNS proxy). Of so, add the host IP to compromise scan whitelist.

2. Use Anti Virus or EDR software to scan the hosts.

Displays each security incident in detail and provides disposal suggestions.

Efficient Response



1 NGFW: NGFW provides a rich set of security evidence from either the perimeter or data center to NovaCommand. Once an incident has been confirmed, NovaCommand can instruct NGFW to provide quick responses such as blocking outbound C&C communications with one click.

2 Endpoint Detection and Response (EDR):EDRprovides a rich set of data on PCsand servers to Nova Command to detect and hunt for threats. Nova Command can also instruct EDRto quarantine malware or threat identified.

Typical Success Story

Customer Name	ABC Commission of Economy and Information Technology ** Due to confidentiality issues, we are unable to display the customer name.*
Customer Pain Points	± Web page tampering security incidents are often unavoidable, even with an array of security systems in place. ± Customers are often unable to accurately gauge the affected areas and data after a security incident.
Underlying Issues	± Lack of effective threat detection methods for threats that have already breached border defenses, lying in wait within the internal network. ± Unable to monitor East-Westtraffic between servers.
Deployment Effect	± Located 16 lost zombie hosts, among which 6 are server hosts and 10 are user PC hosts. ± Frequent exchanges of information were discovered between a server attached to the Commission Office, hosted on an external government affairs network, and a French IP address. The threat proved to be a C&C communication address, found to deploying a scan attack on network segments and the whole server, penetrating laterally. All further damage was mitigated through the use of an elimination tool.