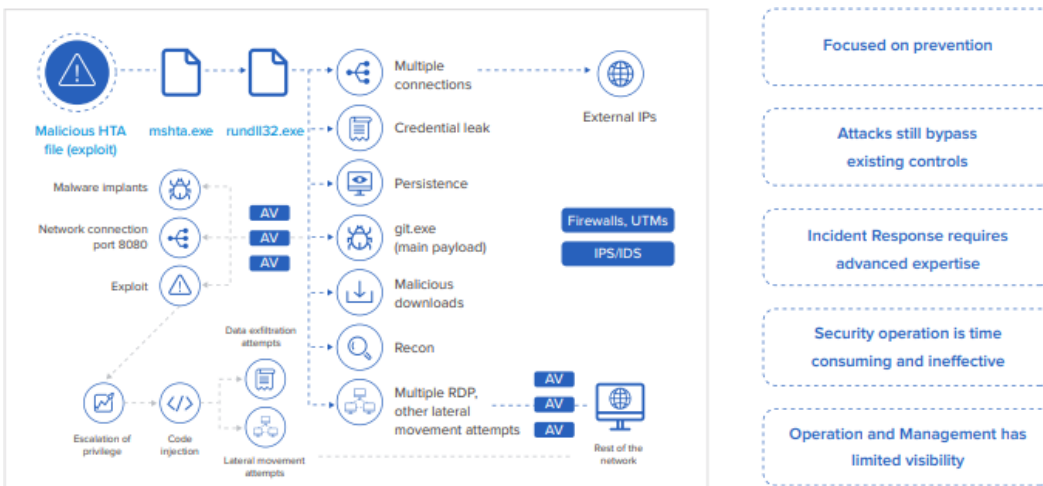


ForeNova NovaCommand

NovaCommand: Intelligent
Threat Detection and
Response Platform

Typical Cyber Security Approach



Security Operation Changes

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.

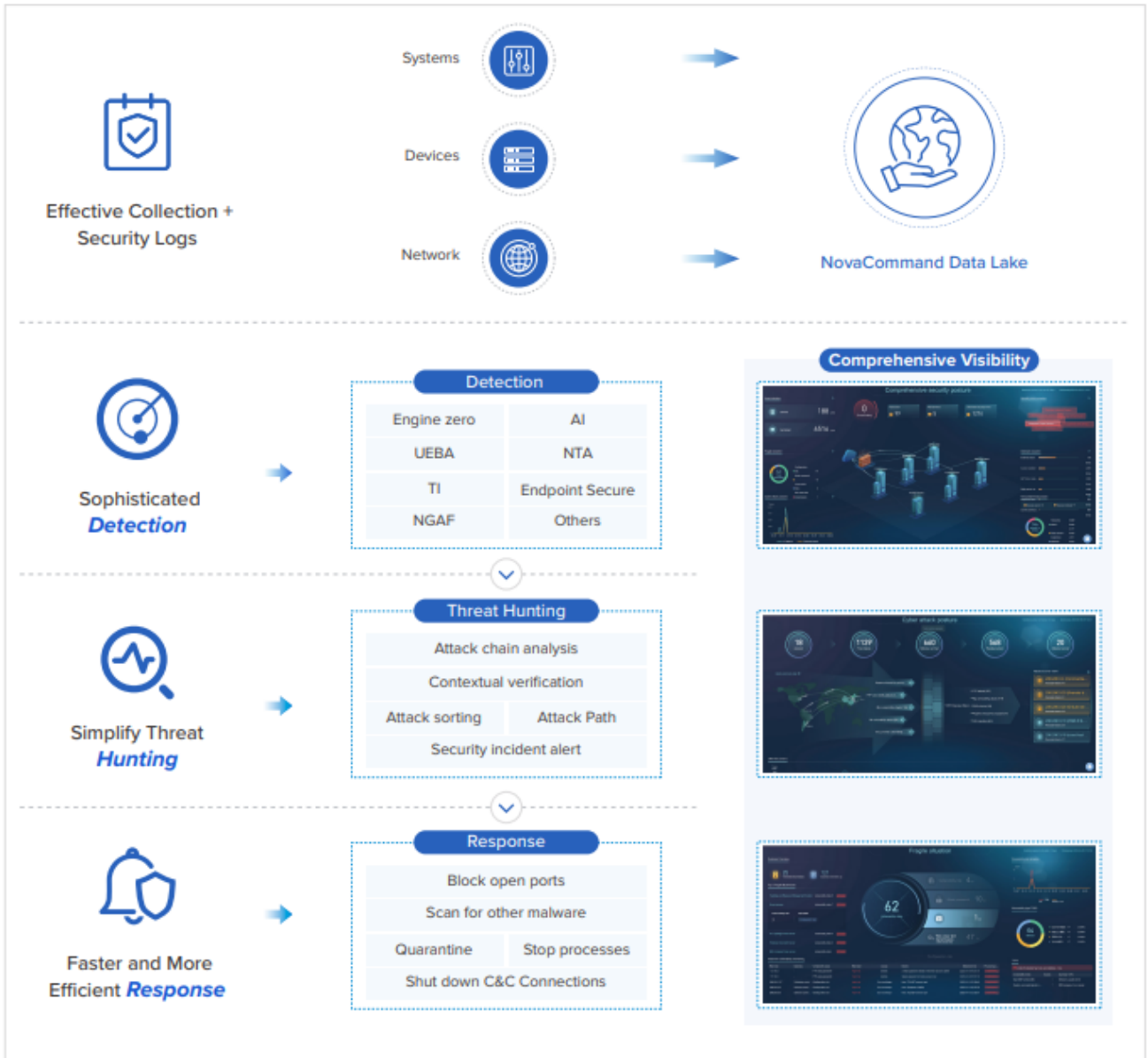
03 Poor Visibility Means Poor Threat Detection & Identification

- ▶ 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.



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-West traffic 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&C activities, 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.

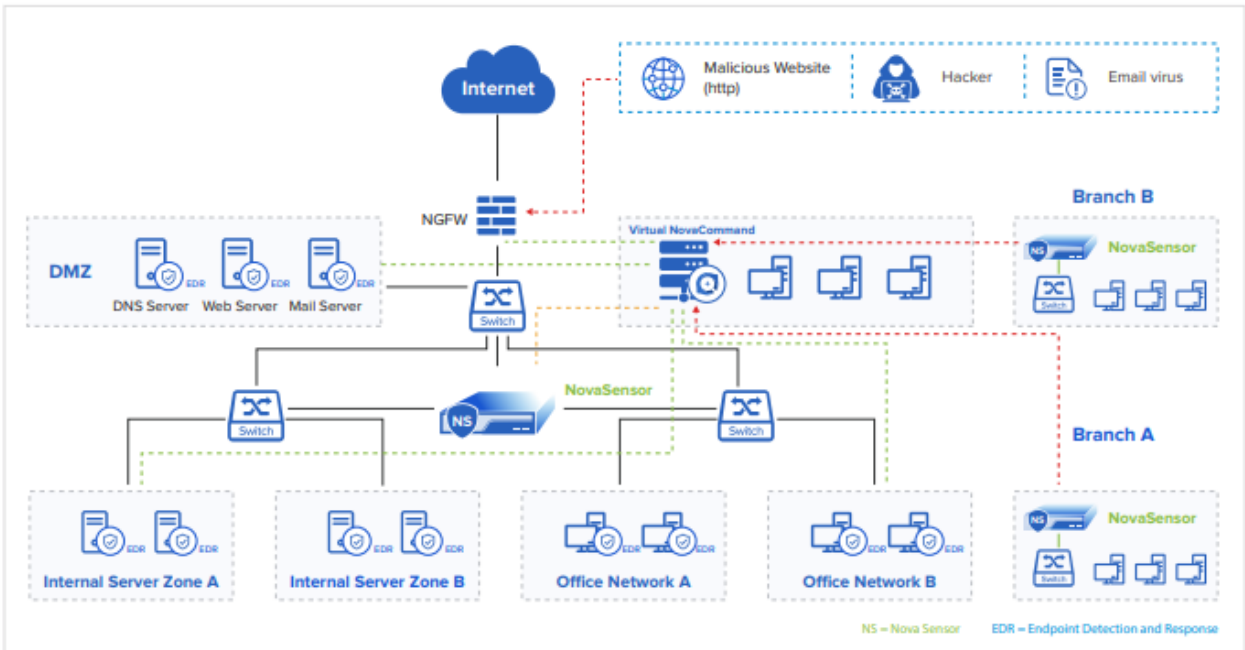
3 Simplify Threat **Hunting**

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



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 of threat intelligence that contains known IP, URL and 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 NGFW and instructing NGFW to block threats identified by NovaCommand.

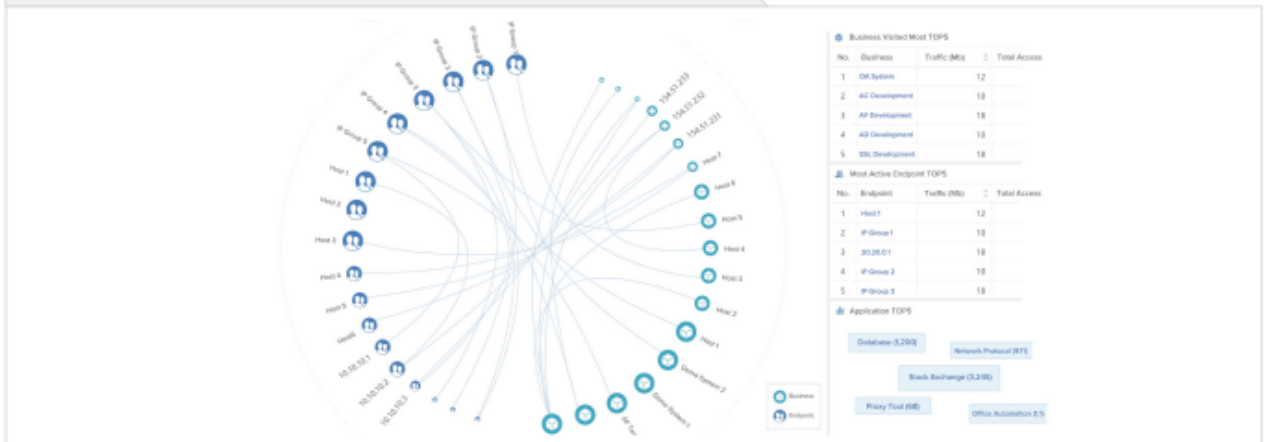
EDR

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)



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)

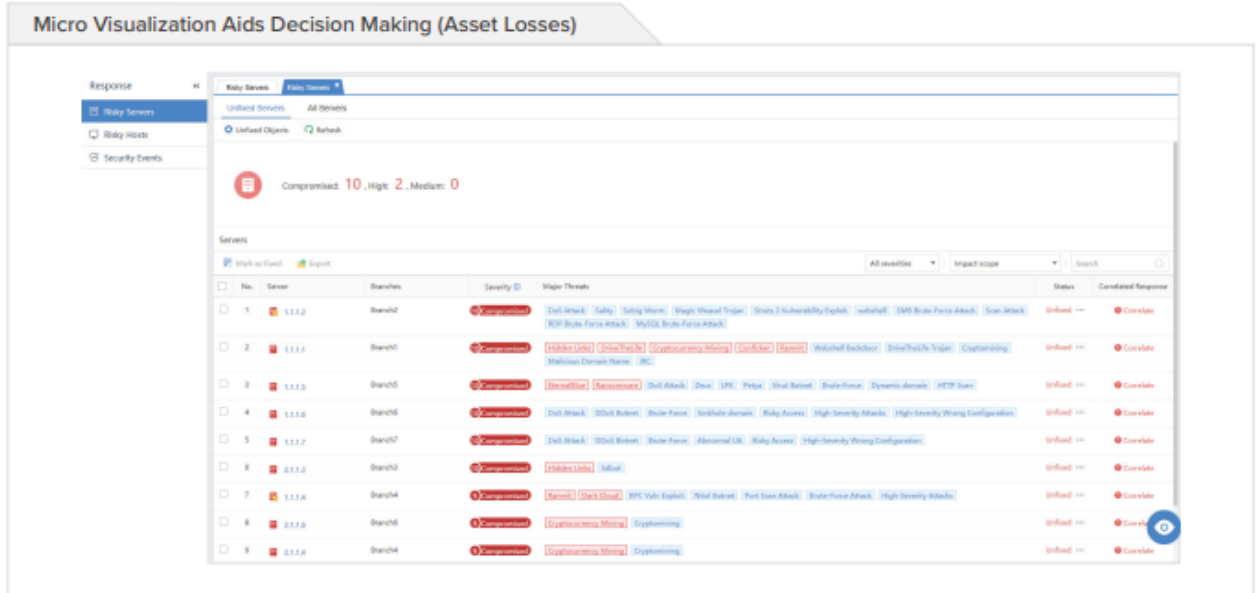


Through real-time monitoring and overall evaluation of the external regions of the network, threat type, and business risk in addition to the latest events and the global threat climate, ForeNova NovaCommand effectively controls both the internal and external security status, enabling all-around security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

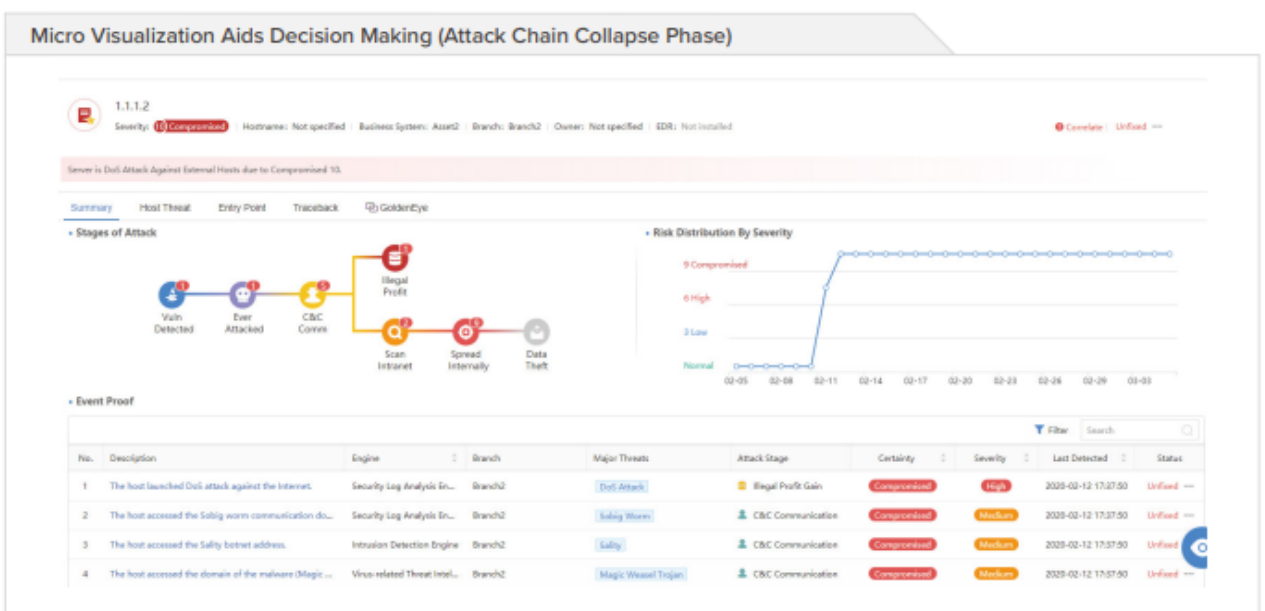
Global Visualization Aids Decision-Making (External Attack Situation)



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.



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



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)



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.

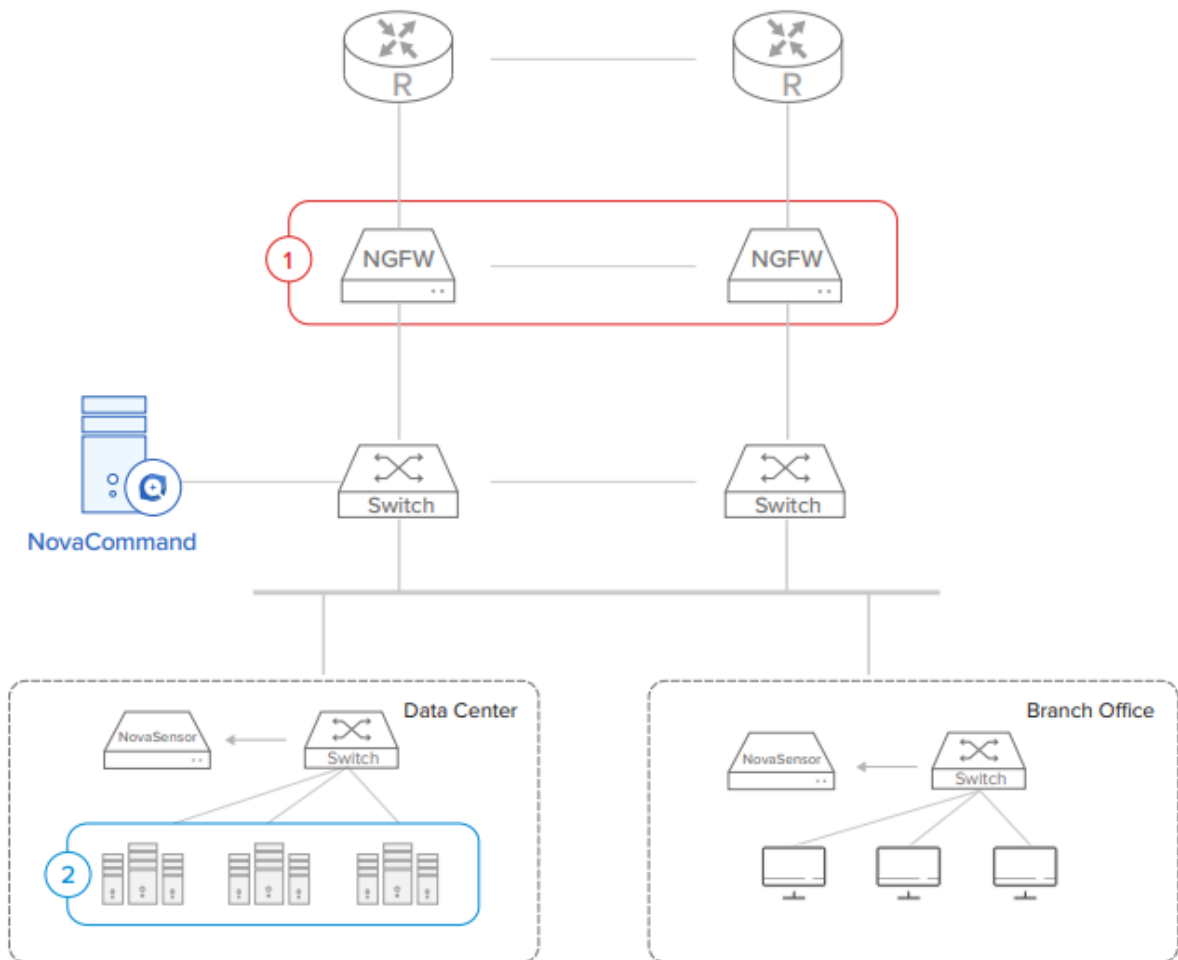
Micro Visualization Aids Decision Making (Detailed Suggestions on the Disposal of Lost Assets and Specialized Kill Tools)

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): EDR provides a rich set of data on PCs and servers to Nova Command to detect and hunt for threats. Nova Command can also instruct EDR to quarantine malware or threat identified.

Typical Success Story



Customer Name	ABC Commission of Economy and Information Technology <small>* Due to confidentiality issues, we are unable to display the customer name.</small>
Customer Pain Points	<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ○ 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-West traffic between servers.
Deployment Effect	<ul style="list-style-type: none"> ○ 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.