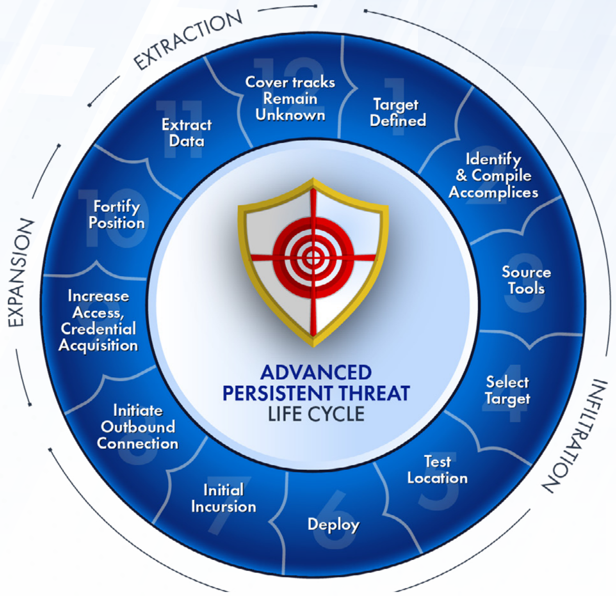
# HOW TO PROTECT YOUR CLIENTS
FROM THE LATEST
ADVANCED PERSISTENT THREATS


EXTRACTION
Cover tracks Remain Unknown
12
Target Defined
1
Identify & Compile Accomplices
2
Source Tools
3
Select Target
4
Test Location
5
Deploy
6
Initial Incursion
7
Initiate Outbound Connection
8
Increase Access, Credential Acquisition
9
Fortify Position
10
Extract Data
11
INFILTRATION
EXPANSION
ADVANCED PERSISTENT THREAT LIFE CYCLE

JUST THE WORDS *"ADVANCED PERSISTENT THREATS"* ARE FRIGHTENING.

Who wants to think about a prolonged and targeted cyberattack where an intruder gains access to your network and remains undetected for an extended period of time?

CELERIUM.com

WELL, HERE'S ONE TO THINK ABOUT.

A Chinese hacking group, Silver Fox APT, has been leveraging trojanized versions of patient medical imaging software (Philips DICOM Viewer) to infiltrate healthcare systems. They gained unauthorized access to healthcare networks where they have compromised sensitive data and disrupted operations.

NEWS
25 FEB 2025
Chinese-Backed Silver Fox Plants Backdoors in Healthcare Networks

Image: Infosecurity Magazine

Researchers at Forescout's Vedere Labs reported that Silver Fox APT exploited Philips DICOM Viewer to deploy a backdoor, a keylogger and a crypto miner on victims' computers.

Once installed, the malware dropped ValleyRAT, a backdoor that gives attackers control of victims' computers and that opened doors into the hospital's networks.

Is this an isolated incident? ANSWER – NO!

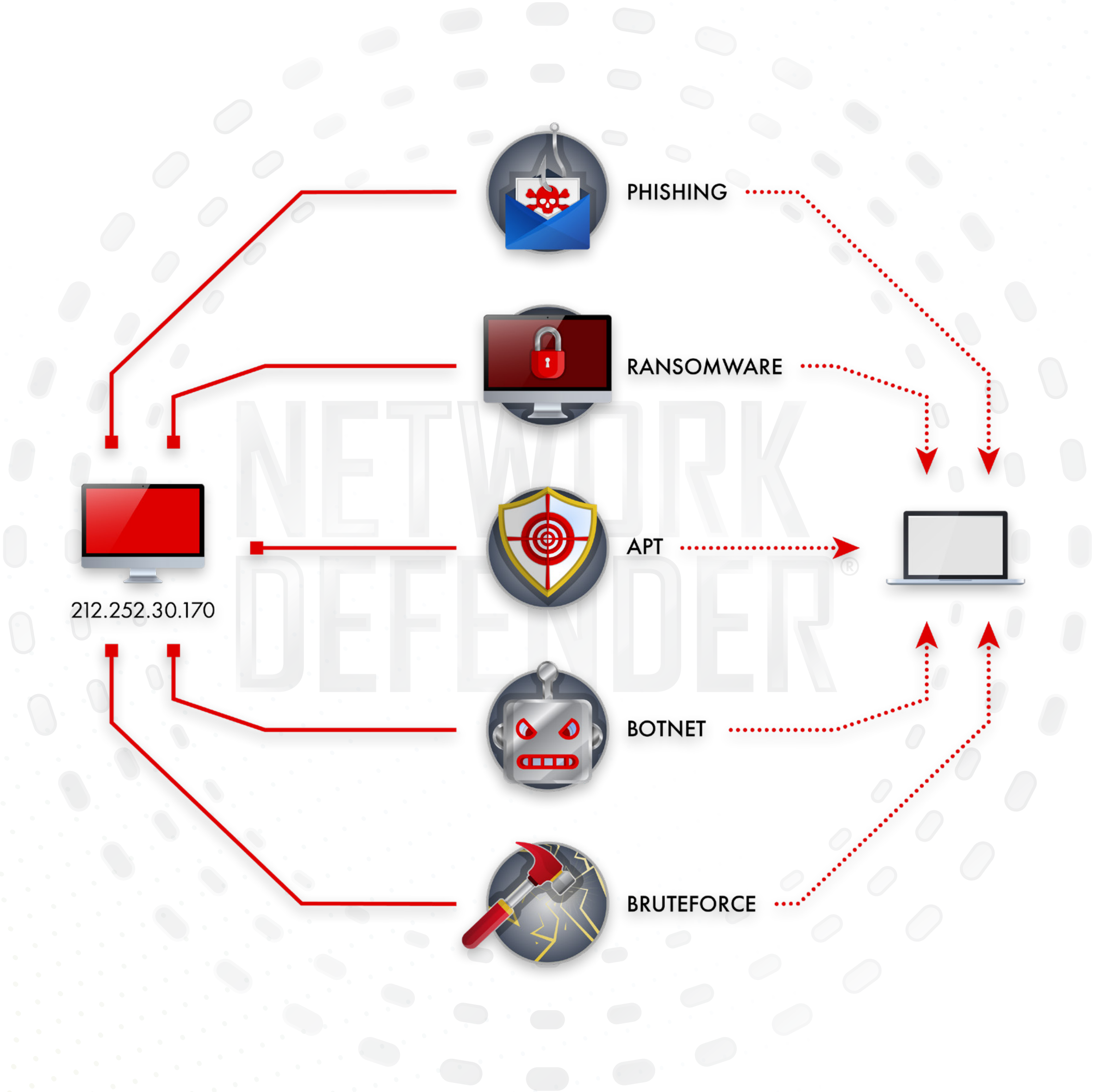
Celerium has identified related Alibaba Cloud buckets hosting additional first-stage malware. This malware mimics more than the Philips DICOM Viewer software, indicating broader **targeting that extends beyond healthcare.**

Celerium has identified possible attempts to download first-stage malware from these Alibaba Cloud buckets on the networks of our clients.

MEET CELERIUM'S
NETWORK DEFENDER®

To help you protect your and your clients IT assets from cyberattacks, including Advanced Persistent Threats, **Celerium invites you to take a good look at Network Defender®**.

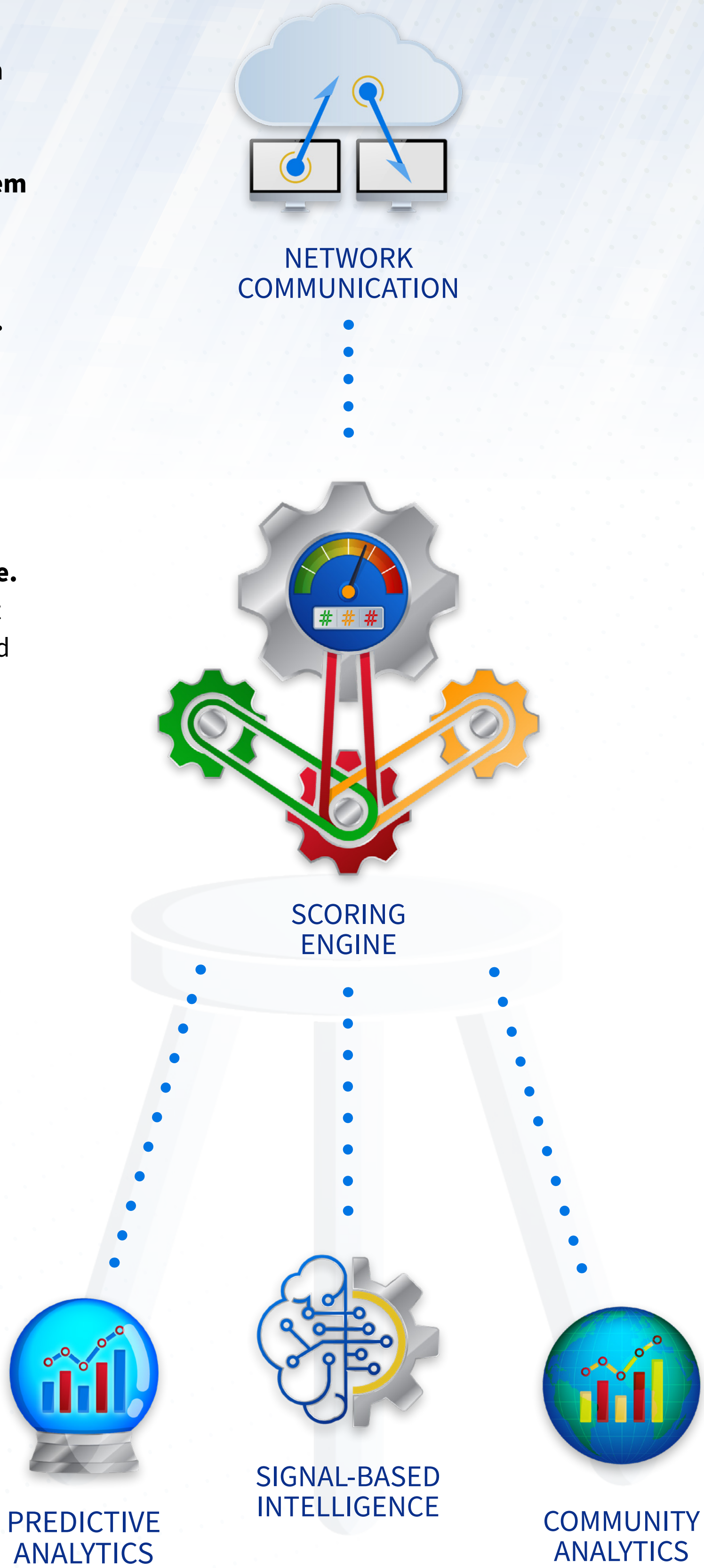
Network Defender is the right-sized weapon to fight against just the kinds of attacks targeting you and your clients. It is built from the ground up, focused on supporting small- and medium- sized companies and distributed large enterprises.



Network Defender uses a combination of distinct, yet complementary, automated approaches to identify known or likely attackers and stop them in their tracks.

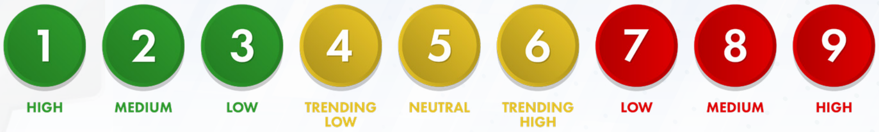
Every attack must come from a source IP address to a destination IP Address. So cyberattacks can be detected or stopped by using IP addresses as the source of truth.

With every inbound or outbound network communication, we evaluate each via our automated scoring engine. Is there a recent score generated for that IP address? If not, we kick our automated analytics in gear using our proprietary three-legged stool of analytics.



SIGNAL-BASED INTELLIGENCE

We created a new approach that we call – Signal-Based Threat Intelligence. We avoid thinking about the information collected from threat intelligence sources in terms of malware command and control, phishing, or ransomware hosts. **Rather, we treat the appearance of an IP on a threat intelligence source as a signal of bad activity.**



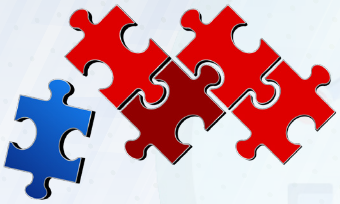
We can then look across time and sources to determine how strong that signal might be at any moment in time. **The combination of signals and their strength affects our calculation of a Threat Score.**

	SCORE = 6	**SCORE - 9**
Number of Times Observed	Seen on 4 Lists	Seen on 2 Lists
Age of Target	3 months old in all 4 cases and is no longer on any of the 4 lists	**NEW** IP address was added to both lists today
Quality of Lists	**LOW** Historically, the lists have not been reliable indicators of compromise	**HIGH** Historically, the lists have been reliable indicators of compromise
Correlation of Lists	**HIGH** the same IP addresses appear on all lists	**LOW** the IP addresses do not appear on all lists

For Advanced Persistent Threats, any attempts to download files or communicate with the infrastructure hosting the malicious executables and multi-part, first-stage downloads, **will be scored “9” and will be blocked**.

PREDICTIVE ANALYTICS

Our robust collection of threat intelligence sources allows us to use Predictive Analytics to determine if an IP address not in our Threat Intelligence Library shares attributes with risky IP addresses in our library. **The number of shared attributes allows us to predict whether this IP address is likely to be malicious.**



COMMUNITY ANALYTICS

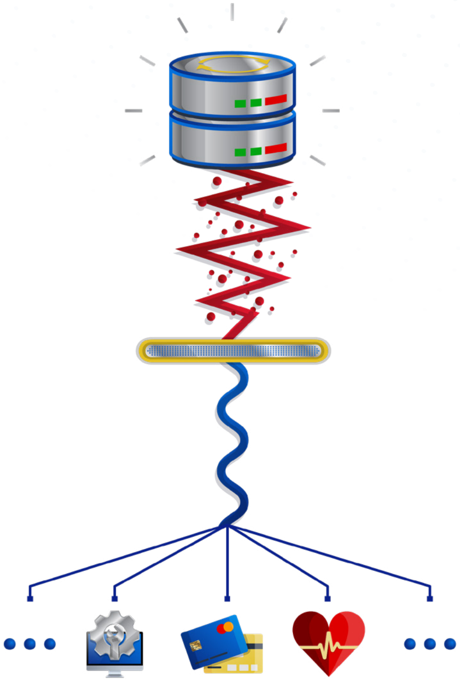
In 2020, Celerium was granted a patent for our unique approach to anonymizing our customers' data in a real-time data set.

With a real-time data set of anonymizing customer data, we can do very interesting things to improve the accuracy of our scoring and to remove false positive from the data set.

Further, because we categorize our customers into size (small, medium and large) and sector (financial services, healthcare, IT, etc.), we are able to identify and research abnormal behavior in the community.

With respect to false positives, we created a noise filter using our community data. This noise filter allows us to compare scoring we get from Signal-Based Threat Intelligence and Predictive Analytics against real-time network traffic.

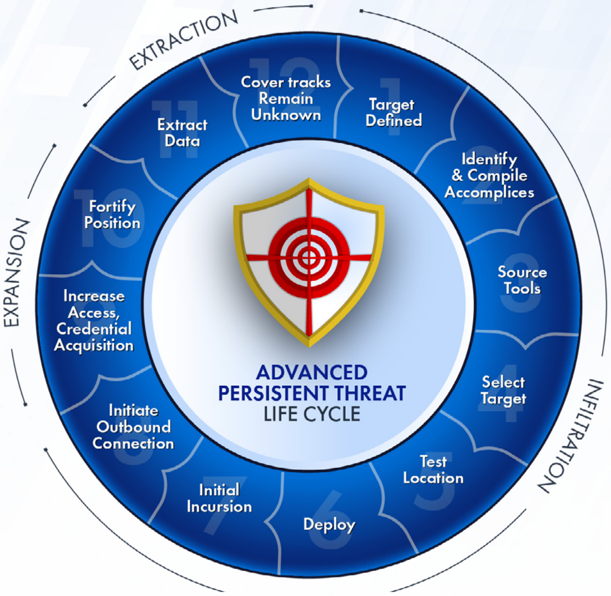
You don't want to lose sleep over **a prolonged and targeted cyberattack** where an intruder gains access to your network and remains undetected for an extended period of time. And you don't want to lose sleep over any other type of cyberattack on your or your client's IT assets.



VISIT CELERIUM.com

to Schedule a Demo of Network Defender,
& See the Cyber Defense It Provides!

HOW TO PROTECT YOUR CLIENTS
FROM THE LATEST
ADVANCED PERSISTENT THREATS


EXTRACTION
Cover tracks Remain Unknown
Target Defined
Identify & Compile Accomplices
Source Tools
Select Target
INFILTRATION
Test Location
Deploy
Initial Incursion
Initiate Outbound Connection
Increase Access, Credential Acquisition
EXPANSION
Fortify Position
Extract Data
ADVANCED PERSISTENT THREAT LIFE CYCLE

JUST THE WORDS *"ADVANCED PERSISTENT THREATS"* ARE FRIGHTENING.

Who wants to think about a prolonged and targeted cyberattack where an intruder gains access to your network and remains undetected for an extended period of time?

CELERIUM.com

WELL, HERE'S ONE TO THINK ABOUT.

A Chinese hacking group, Silver Fox APT, has been leveraging trojanized versions of patient medical imaging software (Philips DICOM Viewer) to infiltrate healthcare systems. They gained unauthorized access to healthcare networks where they have compromised sensitive data and disrupted operations.

NEWS
25 FEB 2025
Chinese-Backed Silver Fox Plants Backdoors in Healthcare Networks

Image: Infosecurity Magazine

Researchers at Forescout's Vedere Labs reported that Silver Fox APT exploited Philips DICOM Viewer to deploy a backdoor, a keylogger and a crypto miner on victims' computers.

Once installed, the malware dropped ValleyRAT, a backdoor that gives attackers control of victims' computers and that opened doors into the hospital's networks.

Is this an isolated incident? ANSWER – NO!

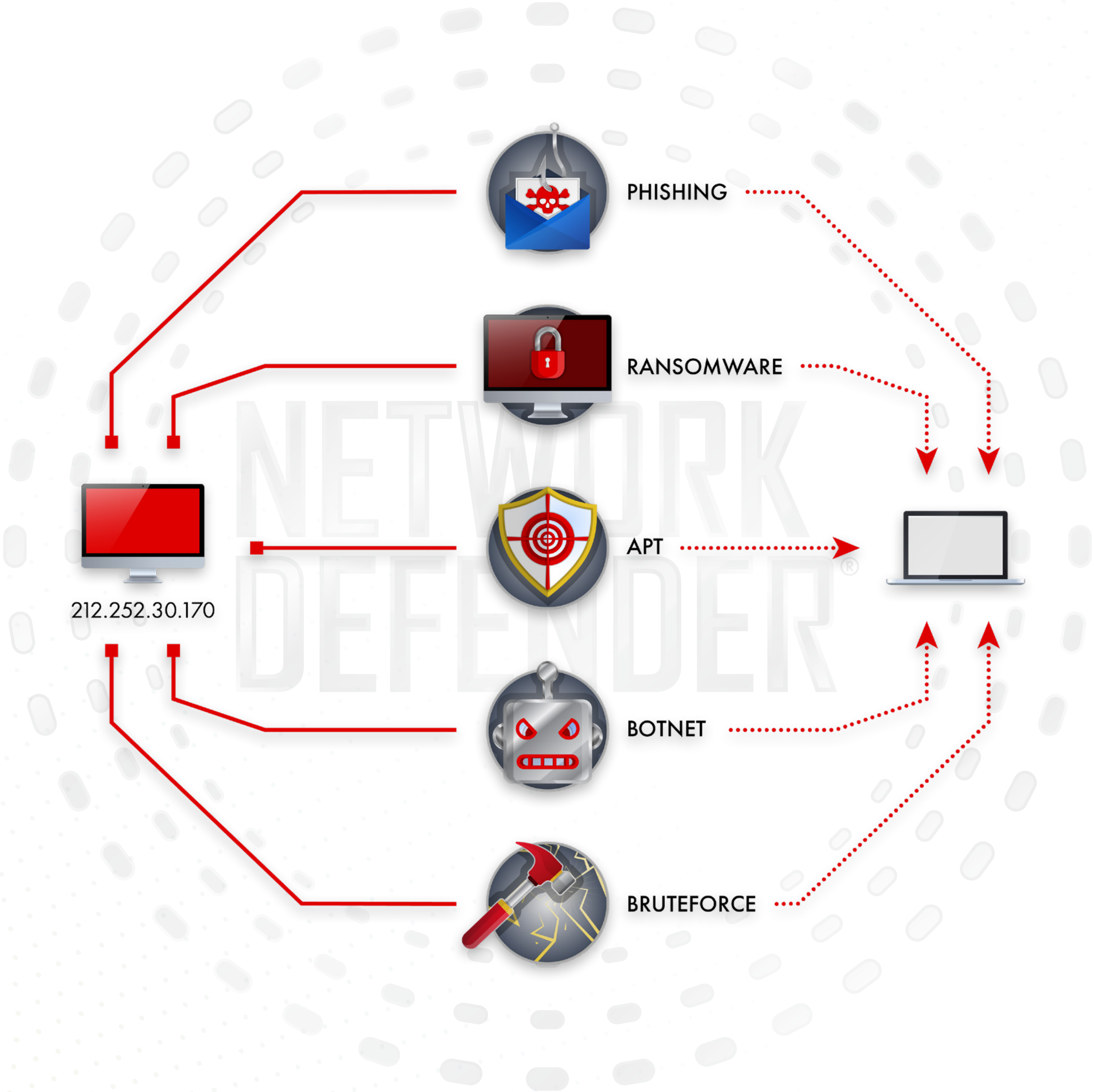
Celerium has identified related Alibaba Cloud buckets hosting additional first-stage malware. This malware mimics more than the Philips DICOM Viewer software, indicating broader **targeting that extends beyond healthcare.**

Celerium has identified possible attempts to download first-stage malware from these Alibaba Cloud buckets on the networks of our clients.

MEET CELERIUM'S NETWORK DEFENDER®

To help you protect your and your clients IT assets from cyberattacks, including Advanced Persistent Threats, **Celerium invites you to take a good look at** **Network Defender®**.

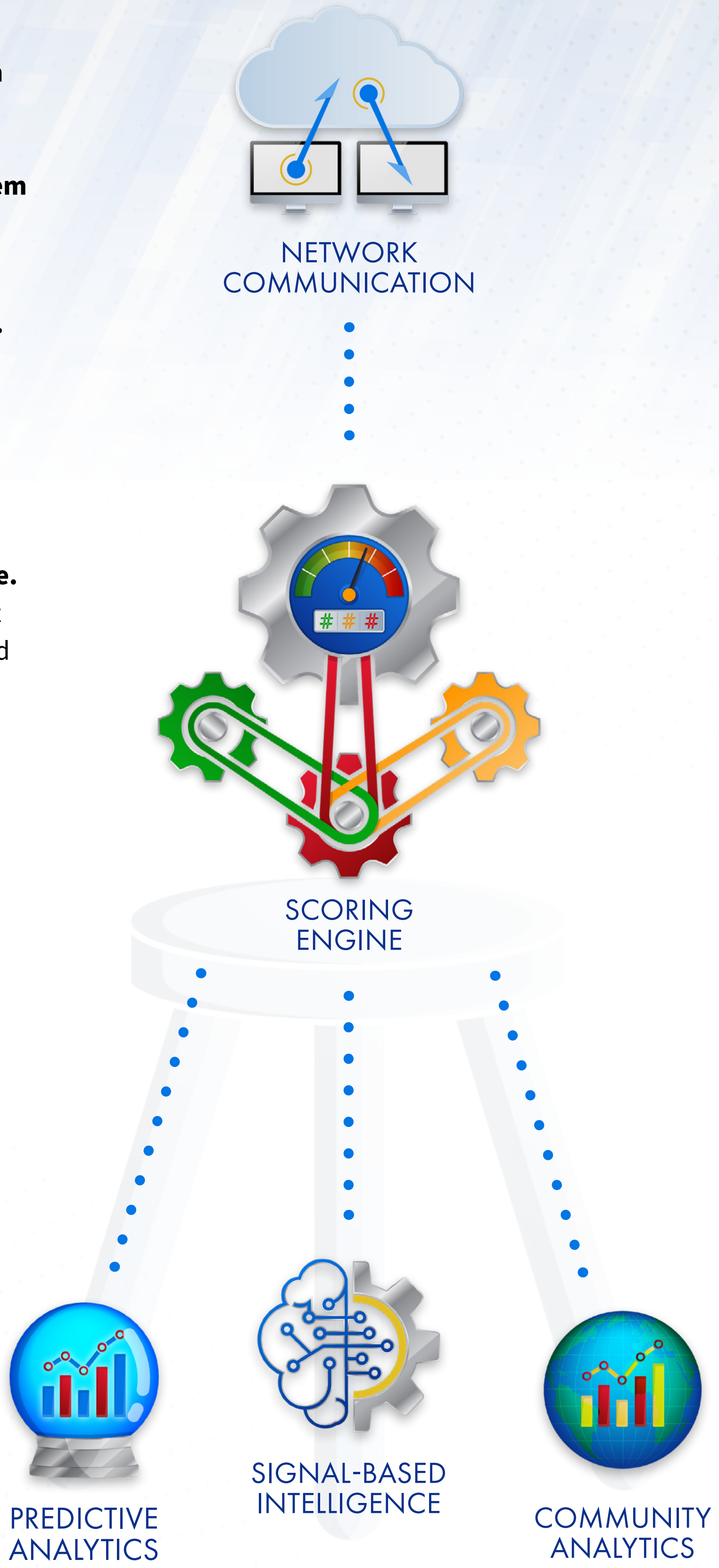
Network Defender is the right-sized weapon to fight against just the kinds of attacks targeting you and your clients. It is built from the ground up, focused on supporting small- and medium- sized companies and distributed large enterprises.



Network Defender uses a combination of distinct, yet complementary, automated approaches to identify known or likely attackers and stop them in their tracks.

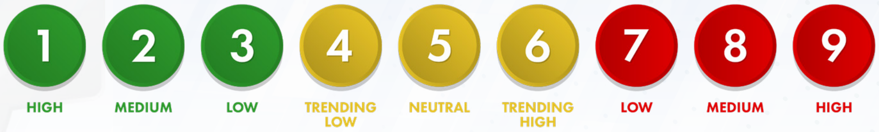
Every attack must come from a source IP address to a destination IP Address. So cyberattacks can be detected or stopped by using IP addresses as the source of truth.

With every inbound or outbound network communication, we evaluate each via our automated scoring engine. Is there a recent score generated for that IP address? If not, we kick our automated analytics in gear using our proprietary three-legged stool of analytics.



SIGNAL-BASED INTELLIGENCE

We created a new approach that we call – Signal-Based Threat Intelligence. We avoid thinking about the information collected from threat intelligence sources in terms of malware command and control, phishing, or ransomware hosts. **Rather, we treat the appearance of an IP on a threat intelligence source as a signal of bad activity.**



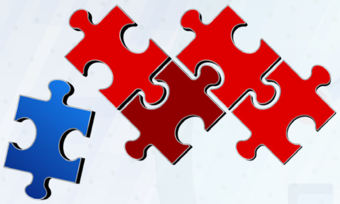
We can then look across time and sources to determine how strong that signal might be at any moment in time. **The combination of signals and their strength affects our calculation of a Threat Score.**

	SCORE = 6	SCORE = 9
Number of Times Observed	Seen on 4 Lists	Seen on 2 Lists
Age of Target	3 months old in all 4 cases and is no longer on any of the 4 lists	**NEW** IP address was added to both lists today
Quality of Lists	**LOW** Historically, the lists have not been reliable indicators of compromise	**HIGH** Historically, the lists have been reliable indicators of compromise
Correlation of Lists	**HIGH** the same IP addresses appear on all lists	**LOW** the IP addresses do not appear on all lists

For Advanced Persistent Threats, any attempts to download files or communicate with the infrastructure hosting the malicious executables and multi-part, first-stage downloads, **will be scored "9" and will be blocked**.

PREDICTIVE ANALYTICS

Our robust collection of threat intelligence sources allows us to use Predictive Analytics to determine if an IP address not in our Threat Intelligence Library shares attributes with risky IP addresses in our library. **The number of shared attributes allows us to predict whether this IP address is likely to be malicious.**



COMMUNITY ANALYTICS

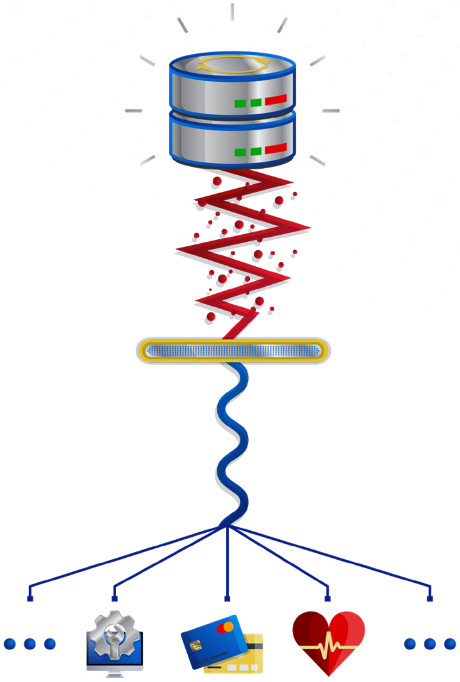
In 2020, Celerium was granted a patent for our unique approach to anonymizing our customers' data in a real-time data set.

With a real-time data set of anonymizing customer data, we can do very interesting things to improve the accuracy of our scoring and to remove false positive from the data set.

Further, because we categorize our customers into size (small, medium and large) and sector (financial services, healthcare, IT, etc.), we are able to identify and research abnormal behavior in the community.

With respect to false positives, we created a noise filter using our community data. This noise filter allows us to compare scoring we get from Signal-Based Threat Intelligence and Predictive Analytics against real-time network traffic.

You don't want to lose sleep over **a prolonged and targeted cyberattack** where an intruder gains access to your network and remains undetected for an extended period of time. And you don't want to lose sleep over any other type of cyberattack on your or your client's IT assets.



VISIT CELERIUM.com

to Schedule a Demo of Network Defender,
& See the Cyber Defense It Provides!