

Protecting today's complex networks from the ever changing landscape of malicious threats and targeted attacks is critical for organizations that rely heavily on their networks. Without detailed intelligence of the threat landscape, organizations place their business operations, intellectual property and customer data at unnecessary risk. Unfortunately, monitoring the changing threats in the wild, and being able to analyze the data and implement necessary security policy changes isn't something most organizations are equipped to do. To address this security challenge, TippingPoint's ThreatLinQ security intelligence portal is an easy-to-use, real-time threat monitoring console that provides a means to evaluate the changing threat landscape and connect that to specific intrusion prevention system (IPS) policy changes. ThreatLinQ gives organizations the ability to proactively optimize their network security in order to reduce unnecessary business risks based on a detailed real-time analysis of today's threat landscape.



"ThreatLinQ provides us valuable intelligence about the threat landscape and how the IPS filters we depend on are used by our peers and colleagues to protect their data."

Justin Bell

Security Architect
Cincinnati Bell
Technology Solutions

Real Time Threat Intelligence

Network security requires an understanding of what is happening outside the network "in the wild." Consequently, TippingPoint maintains an extensive, worldwide network of "Lighthouse" installations to monitor and collect rich data sets on malicious threats and attacks – also known as the "Threat Landscape." This threat landscape data is available in a clear and concise format through the TippingPoint ThreatLinQ console to allow security administrators to quickly review the current and evolving threat landscape.

Monitor the Current State of the Global Threat Landscape

ThreatLinQ provides organizations the ability to view aggregate and detailed attack statistics from around the globe.

Inspect Recent Changes in the Global Threat Landscape for New and Evolving Threats

In addition to monitoring the current status of global threats, ThreatLinQ also tracks, identifies and

provides details on those attacks that have seen the greatest recent growth. These details allow network security administrators to proactively anticipate threats and quickly take protective measures for their networks.

View Top Attack Types Locally by Country

ThreatLinQ gives organizations the ability to drill-down to view local threats. By selecting a country on the world map which is of interest, ThreatLinQ provides a listing of the top attacks within that country. Using this data, organizations can prioritize security policy changes based on both the global and local threat landscape.

Identify Additional Threat Details

ThreatLinQ provides much more than just a simple listing of the top attacks recorded worldwide. ThreatLinQ provides source and destination details for each monitored attack type. This rich attack data allows administrators to make more informed and quicker security decisions to address new security threats.

“The presentation of ThreatLinQ and its content is excellent. The user interface is simple and easy to navigate.”

David Neild

Network Development
Service Leader
University of Leeds

View_Top_Attacks_by_Category

As a general overview of the global threat landscape, ThreatLinQ provides all of the attack data grouped into key attack categories.

IPS_Filter_Intelligence

Network security necessitates that IPS filter profiles protect against the threat landscape. ThreatLinQ IPS filter intelligence data provides organizations with the information needed to “connect the dots” or map the specific threat landscape attacks to specific IPS protection filters.

Review_IPS_Filter_Usage_Statistics

ThreatLinQ provides a simple view of all TippingPoint IPS filter categories and users can easily drill-down into each category to see which IPS filters are automatically enabled with TippingPoint’s recommended settings. In addition, ThreatLinQ collects information on the percentage of reported IPS filter profiles worldwide from participating TippingPoint customers that are enabled, and whether that setting differs from the recommended settings (all data is anonymous).

Compare_Against_Other_Companies’_Enabled_IPS_Filter_Configurations

ThreatLinQ collects information on how enabled IPS filters are configured from participating TippingPoint customers. Users can quickly view all IPS filter deployment statistics by category and drill-down to view individual IPS filter configurations. For each IPS filter, users can view the percent of reported IPS filter profiles that have that specific filter enabled, and whether it is configured to block or rate-limit traffic.

View_Additional_IPS_Filter_Details

In addition to providing additional source and destination data for each specific attack type in the threat landscape, ThreatLinQ also provides the same information as it relates to the specific IPS filters that protect networks from the corresponding attack type.



ThreatLinQ also provides the CVE ID(s) and BugTraq ID(s) associated with each IPS filter where applicable to allow security administrators to conduct additional vulnerability research.

Proactively_Optimize_IPS_Network_Security_Protection

Network security requires maximizing IPS protection. ThreatLinQ helps organizations make proactive changes to their IPS protection profiles based on a quick review of the changing threat landscape and IPS Filter Intelligence data.

1. Compare IPS Filter Profiles to the Threat Landscape

– The first step in making proactive security policy changes is to review the threat landscape data on ThreatLinQ and compare the top threats to an IPS filter profile(s). From this comparison, it is simple to quickly identify where protection gaps might exist. This narrows the threat areas that administrators need to focus their energies on evaluating.

2. Identify the IPS Filters That Cover Any Security Gaps

– The second step in making proactive security policy changes entails directly mapping any security gaps to individual IPS protection filters. ThreatLinQ directly maps the exact IPS filter(s) for each attack identified globally. This correlation makes the ThreatLinQ threat landscape data extremely actionable for security administrators.

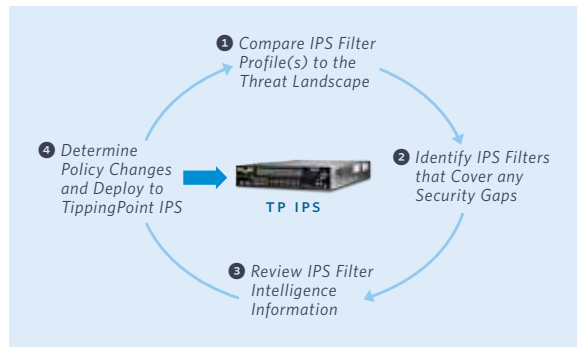
3. Review IPS Filter Intelligence Information – The third step in making proactive security policy changes requires an analysis of the IPS filter intelligence information for the filters needed to protect against new attacks in the threat landscape. A review of the IPS filter usage and configuration information provided shows if and how others are using the specific filters. This additional information on the specific vulnerabilities and IPS filters help organizations make a final determination about what security policy changes are warranted for their unique environment.

4. Determine Any Necessary Policy Changes and Proactively Deploy

– From this simple process, security administrators know exactly which IPS filters protect against the top global and local attacks and any identified security gaps. ThreatLinQ’s real-time threat intelligence data and IPS filter

ThreatLinQ®_ThreatLinQ

IPS-Secured_Networks



intelligence data provide security administrators with the most complete, concise and simple to use information available in the proactive security policy change process.

Easy_to_Use_for_IT_Personnel

The ThreatLinQ interface and data presentation makes it simple for all IT personnel to quickly review IPS security policies.

Simple_Navigation_Through_the_Policy_Review_Process

The ThreatLinQ user interface is simple and intuitive. The navigation “walks” users through reviewing the top global and local attacks; “movers and shakers”

(new and growing global threats); and IPS filter intelligence data. This navigation shows security administrators how to review the global threat landscape, identify possible security gaps and proactively optimize their security profile.

Clear,_Concise_Data_Presentation

The ThreatLinQ data presentation makes it easy for IT personnel to quickly learn how to review the top threats and make proactive decisions on maximizing of IPS protection within minutes.



Features and Benefits

TippingPoint ThreatLinQ

- > Available to all TippingPoint customers
- > Accessible through TippingPoint's Threat Management Center
- > No additional login credentials required
- > Requires only minutes per week to keep IPS protection optimized

Threat Intelligence Data

- > Listing of all attacks in the wild
- > Number of attack hits (individual instances)
- > Charts of daily attack activity with number of hits, unique source IP and destination IP addresses
- > Map of top attack sources worldwide
- > Destination port number for each attack type
- > Destination port name
- > Destination port description
- > Number of monitored attacks per port number

- > Source IP addresses for each attack type
- > Number of monitored attacks per source IP address
- > Reverse DNS information for the source IP address
- > Source countries
- > Number of monitored attacks per source country
- > Source cities if known
- > Source port number for each attack type
- > Source port name
- > Source port description
- > Number of monitored attacks per port number

“Movers and Shakers”

- > Listing of attacks exhibiting the greatest increase in activity
- > Charts of daily attack activity with number of hits; unique source IP and destination IP addresses for these top growing attacks

IPS Filter Intelligence Data

- > IPS filter descriptions
- > IPS filter reference information and links for additional research
- > CVE ID and hit count
- > BugTraq ID and hit count
- > IPS filter “Recommended Settings”
- > IPS filter usage statistics - percentage of reported profiles with filter enabled or disabled, percentage of reported profiles with enabled filters deployed to block or rate limit

Key ThreatLinQ Features

- > Real Time Threat Intelligence
- > IPS Filter Intelligence
- > Proactively Optimize IPS Network Security Protection
- > Easy to Use for IT Personnel

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS

European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450

Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999