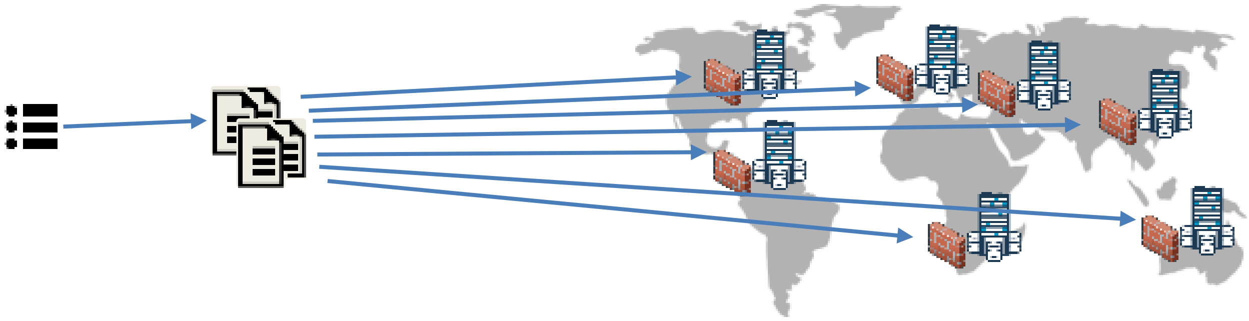
Threat Response: IP Lifecycle Management

IP lifecycle management enables automatic addition and removal of IPs, domains, URLs, and users from blocklists at appropriate times.

Creating or maintaining IP block lists seems like a straightforward task, but there is significant underlying complexity in process design and management of information access. You must factor in the number of enforcement devices, the breadth of devices from the vendors, and the regions where management consoles are accessed. Additionally, each class of device from each vendor may have a separate method of update or integration. This becomes complicated when companies use more than one vendor and need to update tens or possibly hundreds of devices in multiple regions.



The complexity also increases when you have more than one analyst, a steady stream of threats, multiple block list updates, and multiple enforcement devices from multiple vendors.

IP lifecycle management might be manageable if today's threats weren't so complex or sophisticated. Today's attacks include watering holes, malvertising, and strategic web compromises – effectively ephemeral attacks – which means that you not only have to create and update block lists with bad sites, but you must remove sites that are no longer bad. For example, the New York Times has been compromised and used as a watering hole several times in the past few years. Since the New York Times has millions of visitors, it should not be simply blacklisted forever. Instead, it must be blocked when it is bad then unblocked when the threat has been removed.

This is where the complications start. As soon as you have two or more analysts updating the block list simultaneously, who takes precedence? Looking deeper, other questions appear:

- How do you know when the compromised site is cleaned of malware?
- What if you see you a threat at the site again?
- How do you manage those lists across multiple locations, multiple devices, and multiple vendors?

Unfortunately, such a seemingly straightforward task has larger implications:

- Do you require a policy to ensure all updates are done in a timely manner?

- Do you create policy that may introduce a delay for block list updates but ensures analysts are coordinated?
- Do you create a check-in and checkout lock policy on the block list?
- Do you require all team members to create an audit trail for the blocklist changes?
- Do you have a block list owner or manager who insures integrity of the list?
- How do you make sure blocklist updates are synchronized with the network team's operating schedule?

The bigger problem is dealing with end-user access to compromised sites. When you have multiple users updating files for multiple devices, how do you ensure that you remove IPs or domains for compromised sites in a timely manner? Traditional solutions can be extremely manual and cumbersome. Someone maintains an Excel spreadsheet or file with domains and IP addresses and then will manually go to each vendor's device or console to remove individual entries. One risk in this process is that the list updater usually doesn't know if the site that was compromised has been cleaned. All they know is that they should update the list and enforcement devices.

Thousands of sites are water-holed or compromised each year, some of these sites have a high Alexa ranking, such as the New York Times or Department of Labor. These sites eventually need to be removed from block lists as they are cleaned, but managing these block lists will only grow more difficult over time.

This simple task suddenly became complicated, and just the paperwork for tracking each domain and IP for removal for multiple devices from multiple vendors can be a headache. Additionally, this is often a source for human error and internal frustration.

Proofpoint Threat Response and IP lifecycle management

Proofpoint Threat Response comes with built-in IP lifecycle management. This includes the ability to add and remove IP addresses, domains, and URLs from lists which can be applied to enforcement devices. In addition, users can be isolated quarantined or even locked down to prevent identity abuse or privilege escalation.

- Threat Response takes the IP addresses, domains, URLs, and users that an analysts wants blocked, and can automatically set a length of time to place those IP addresses, domains, URLs, and users on one or more block lists. After that length of time has expired, the IP address domains, URLs, or users will be automatically removed from the appropriate list.

- Threat Response can also automatically check for incidents that involve the IP addresses, domains, URLs, or users on those lists and automatically extend the block if an incident is discovered that involves one of them.

IP Lifecycle Management is one of several automation features of Threat Response that enable consistent, repeatable, and rapid incident response.