SOLUTION BRIEF

Creating Resilience within a Security Architecture

Deployment Scenario: Inline and Out-Of-Band

The prevailing wisdom on network security has been to focus on deploying new and more efficient security tools to stop threats from entering the network. While this is clearly an activity that must take place, there also needs to be just as strong an emphasis on remediating threats as fast as possible once they enter the network.

As the plethora of news broadcasts have shown, most enterprise networks will be hacked at some point. In addition, once this happens, the time to notice the intrusion usually takes months, and the time to remediate the problem takes many more months. By adopting a security architecture resilience approach, this time to observance and time to remediation can be reduced.

Solution Components

- Keysight Network Packet Brokers
- AppStack
- SecureStack
- Bypass Switches
- BreakingPoint
- Cyber Range Professional Services
- Traffic Rewind
- ThreatARMOR

Benefits

- Strengthen your capabilities to defend against attacks
- Maximize your ability to rebound from an attack
- Minimize the severity and cost of security breaches

Solution Overview

This solution allows you to:

- Collect better data to analyze security threats in real time and after the event
- Implement better operational response capabilities against attacks
- Apply consistent monitoring and security policies
- Improve operational responses by IT security personnel

KEYSIGHT TECHNOLOGIES

What Is Security Resilience?

According to Dictionary.com, LLC, resilience is the “ability of a system to return to original form, positions, etc., after being bent, compressed, or stretched.” It is also referred to as the capacity to recover from difficulties. Security resilience is your security architecture’s ability to recover and return to a normal state after an attack and/or breach.

There needs to be a fundamental mind shift away from the common thought that network security is a one-time activity or one-size-fits-all. Network security needs to be an ongoing process, not just occasional technology implementations, to create a resilient system.

Network security needs to be an ongoing process, not just occasional technology implementations, to create a resilient system.

Defense Deployment Strategies

Common wisdom for security architectures suggests defense in depth security device solutions that focus on the perimeter, just inside the perimeter, and the core of the network. However, as part of this solution, a best practice is to also integrate your security architecture with a network visibility (monitoring) architecture. Organizations often treat these areas as silos, which starts a cascade of problems, like process failures, blind spots, missed critical data, and delays in problem resolution.

At the Perimeter

All defenses start at the perimeter, typically with a firewall. One of the drawbacks of a firewall-only approach is that updates to the Internet Protocol (IP) address access lists are typically manual processes. By adding a threat prevention gateway, which uses automated updates to known bad IP addresses, you can significantly minimize both incoming and outgoing traffic to bad actors. A threat intelligence gateway has been shown to reduce the amount of data that needs to be screened by an intrusion prevention system (IPS) by up to 30%. Since the threat prevention systems block outgoing traffic, as well, this solution can also reduce, if not eliminate, exfiltration of data from your network, thereby directly limiting the costs of a breach.

Just Inside the Perimeter

Once inside the network, inline security tools are often deployed. When combined with external bypass switches and network packet brokers (NPBs), a very strong and resilient defense can be created. Load balancing, high-availability options, and heartbeat signaling on the NPB and bypass switches can be used to create a self-healing architecture. Other capabilities, like secure sockets layer (SSL) decryption, can be used to strengthen data inspection and the quarantining of suspect data.

At the Core

Once data moves into the core, it can still be inspected. Instead of a real-time analysis, data can be captured and moved to out-of-band security and monitoring tools for deep packet inspection, forensic analysis, log file analysis, NetFlow

The bypass switch and NPB are used to maximize network availability and reliability using high availability, load balancing, and heartbeat messaging. Application intelligence can be added to screen out uninteresting application data that does not need to be inspected.

analysis, regular expression (Regex) searches, etc. This solution uses NPBs and application intelligence to filter out either Layer 2 through Layer 4 data and/or Layer 7 data and send the appropriate data to the corresponding tools, like data loss prevention (DLP) tools, security information and event management (SIEM) tools, log file collection systems, intrusion detection systems (IDS), etc.

Other activities, such as proactive testing of security tools in a lab environment to make sure they protect and defend the network as advertised, can be used as well. If the devices underperform, additional tools can be allocated and processes adjusted. Packet captures of application information can also be replayed and analyzed in the lab to make sure the network is working correctly.

Systemic Processes

Cyber Range training for IT security personnel is another proactive activity. This gives security personnel the ability to experience real attacks (in a controlled environment) so that they can better recognize the symptoms and precursors on a live network. With this knowledge, security personnel not only respond better to attacks, but they can help the systems recover faster to reduce liabilities.

Deploying Inline Security Resilience Solutions

An inline security and visibility architecture solution is designed to maximize the ability to defeat incoming security threats. A threat intelligence gateway (like ThreatARMOR) with a built-in bypass can be used to screen incoming and outgoing data to known bad IP addresses. This reduces the load by up to 30% and helps reduce false positive alerts from an IPS. The threat intelligence gateway can be used in both black listing and white listing security architectures.

The bypass switch and NPB are used to maximize network availability and reliability using high availability, load balancing, and heartbeat messaging.

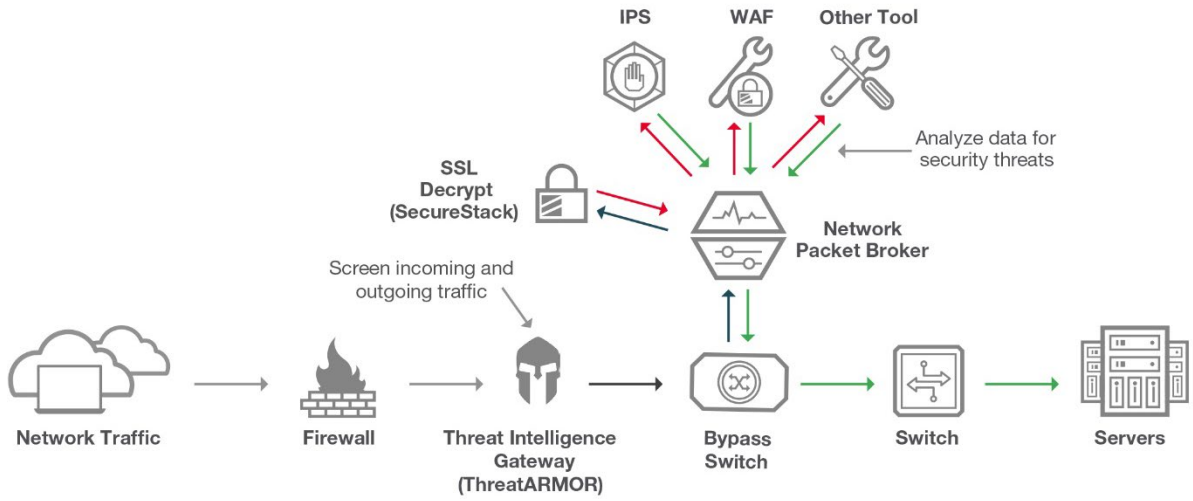

Figure 1. Inline Security Resilience Solution

A new threat is the inclusion of malware within encrypted data payloads. This data can be unencrypted by the NPB, or a purpose-built device, and then passed on to security tools (like an IPS or Web application firewall (WAF)) for examination. Data that is safe is re-encrypted and sent back to the bypass switch to traverse downstream.

Deploying Out-Of-Band Security Resilience Solutions

The out-of-band security and visibility architecture solution is designed to maximize the ability to detect security threats and breaches that have made it into the network. The focus here is to minimize, if not eliminate, the amount of damage that can be done. In this situation, a tap or switched port analyzer (SPAN) feeds the NPB with a copy of all network data. The NPB is then set to filter certain types of data based upon various criteria (IP address, virtual local area network (VLAN), protocol, etc.) and specific data sets are sent to specific types of out-of-band tools (IDS, DLP, SIEM, etc.) for analysis.

This monitoring data can also be filtered by application type. For instance, maybe you only want to see Facebook data or do not want to analyze Netflix data. That data is emphasized in the filtering process. In addition, the application intelligence gateway (AppStack in this case) can generate NetFlow data and additional data (like geolocation, browser type, device type, etc.) that can be used in further analysis of the data. Data masking, Regex searching, and packet capture (PCAP) capabilities are also provided to help analyze specific data natively within that solution or by third-party tools.

A threat intelligence gateway can be used to screen out traffic that either does not need to be analyzed or specifically focus on traffic that does need to be screened. Since the access list in the threat intelligence gateway is constantly updated, this can be used to augment the IP address filtering process within the NPB, as that is often a manual process. The data is then sent on to security tools for analysis of packet and flow data.

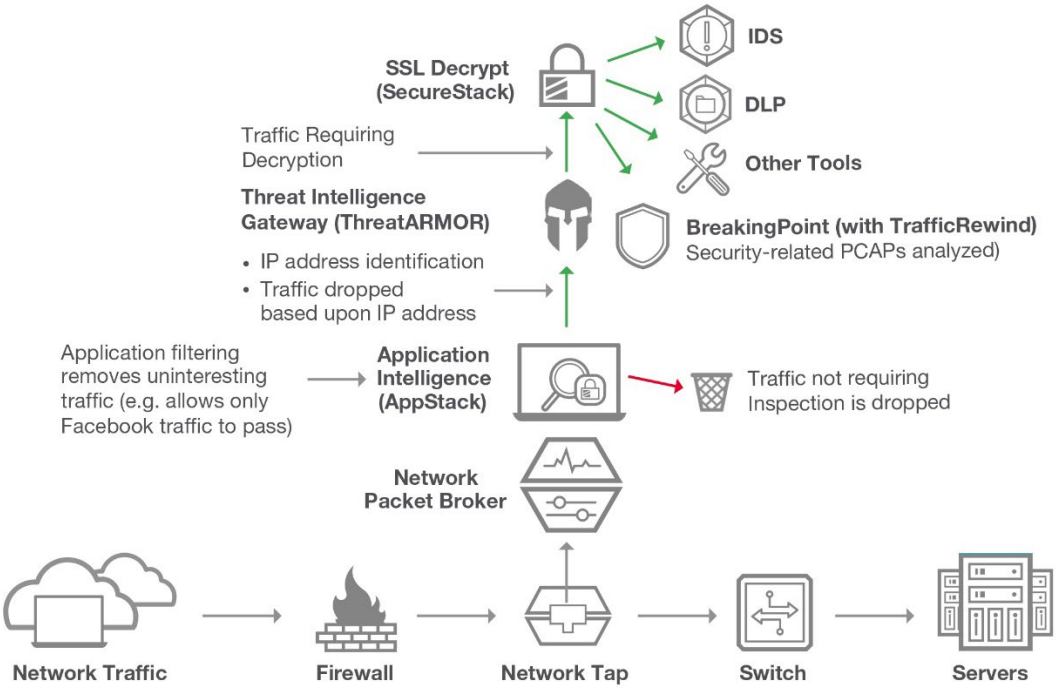

Figure 2. Out-Of-Band Security Resilience Solution

At this point, SSL decryption can also be deployed. Various security and monitoring tools do not support decryption capabilities. If they do, they often consume considerable central processing unit (CPU) resources to perform this function, which ultimately makes the tools less efficient and slower to perform their core analysis functions. The NPB can perform the data decryption before the data is passed on to the various tools. This allows you to decrypt the data only one time and then share across multiple security devices.

Other solutions, like the Keysight BreakingPoint product with TrafficREWIND feature, can take the PCAP information created by AppStack and begin the process to analyze the NetFlow metadata. This reduces the waste of valuable time and resources in trying to replicate production network traffic conditions for fault analysis or to validate architectures and devices before deployment.

Summary

If you cannot protect everything 100%, then security resilience is the next best approach. It allows you to secure as much of the network as you can while building in network visibility and recovery systems to mitigate the effects of a breach as fast you can.

Here are some common elements in a security resilience approach:

- Threat Intelligence Gateways
- Inline tools – FW, IPS, NGFW, SSL decryption, etc.
- NPBs – inline and out-of-band
- External inline bypass switches
- Out-of-band tools – IDS, DLP, SIEM, SSL decryption, flow data analysis
- Application filtering, geolocation information, NetFlow data
- Security device testing
- Network penetration testing
- Cyber Range training Conclusion

Visibility Architecture Solutions from Keysight

Keysight's network visibility solution involves using NPBs in conjunction with application filtering and taps. Learn more about Keysight's Network Packet Brokers, Bypass Switches, AppStack, SecureStack, BreakingPoint, ThreatARMOR, TrafficREWIND, and Cyber Range technology along with our technical partner solutions.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES