WHITE PAPER

Best Practices for Security Resilience

The Reality of Today's Security Architecture

News broadcasts for the last several years have shown that most enterprise networks will be hacked at some point. It is not a question of if, but when. In addition, the time it takes for most IT departments to notice the intrusion usually lasts about 191 days, according to the 2017 Ponemon Institute Cost of Cyber Crime Study. This gives hackers plenty of time to find what they want and exfiltrate that information.

Enterprise networks will be hacked at some point. It is not a question of if, but when.

What if there was a better way? By adopting a resilient security architecture approach, this time to observance and time to remediation can be reduced. Resilience is the ability of a system to return to its original form, position, etc., after being bent, compressed, or stretched. It is also referred to as the capability of a system to recover from difficulties. Extrapolating this concept to a security architecture, security resilience is the ability of your architecture to recover and return to a normal state after an attack and/or breach.

Because of these realities, a new paradigm shift in network security is needed. While security defenses still need to be maintained, there has to be at least equal, if not greater, effort placed on returning the network back to a normal, safe state as quickly as possible. During attacks and breaches, minutes matter, so a business needs this interval to be as short as possible.

KEYSIGHT TECHNOLOGIES

A security resilience approach is about deploying functionality to:

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

Implementing Security Resilience

Besides the typical security threats caused by malware and denial of service, new threats abound in the modern age. According to Ron Ross at NIST, "Complexity is an adversary's most effective weapon in the 21st century. One organization's IT product feature is another organization's attack surface." The Internet of Things (IoT) approach to network architectures also provides a plethora of attack surfaces and potential security holes.

You will not be able to prevent every security attack. So, you need to have an architecture that is as resilient as possible to minimize downtime, costs, and potential losses of personally identifiable information (PII) and corporate intellectual property (IP).

A resilient security approach goes beyond the defensive security architecture approach. The core tenet here is that you will not be able to prevent every security attack. So, you need to have an architecture that is as resilient as possible to minimize downtime, costs, and potential losses of personally identifiable information (PII) and corporate intellectual property (IP). The primary goal of security resilience is to reduce data breach costs by decreasing the discovery time and limiting (if not eliminating) data exfiltration to limit costs (fines and lawsuits), which are often based upon the number of records stolen.

An average of 191 days before discovery and remediation is far too long to be acceptable. Here are some ways to potentially reduce that time:

- Deploy threat intelligence gateways to prevent the exfiltration of data to known bad IP addresses
- Implement inline NPBs to support serial tool chaining
- Use application intelligence to find indicators of compromise
- Decrypt SSL-based monitoring data once with an out-of-band NPB, and distribute to forensic tools for faster analysis
- Install a security attack replay capability to capture security data, and view it in the lab to acquire a tactical analysis of how breaches took place
- Conduct cyber range training to recognize threats faster and practice responding to them properly
- Use threat simulation in your security lab to understand better how new threats behave
- Capture and filter monitoring data, and then send that data to a purpose-built device to look at traffic patterns

Deploy Threat Intelligence Gateways

One of the first things to do is to deploy threat intelligence gateways to limit, if not prevent, the exfiltration of data to known bad Internet Protocol (IP) addresses. Threat intelligence gateways are a common defensive technique but they are also relevant to a resilient approach, as well. The threat intelligence gateway should hopefully block all incoming traffic from known bad IP addresses. However, the IP address may not be known as bad at the time of the attack, thus allowing an attack to succeed.

While the malware may have made it into the network, frequent new definition updates may be able to stop some of the data loss. Even if a new rap sheet of bad IP addresses does not capture the known bad IP address for 30 days, this is still a reduction by half in the typical duration of a breach. Should such an update occur within 15 days or less after the attack, then the breach interval could be reduced by 75% or more.

According to a 2016 Ponemon Institute study, organizations follow up on only 29% of security alerts issued by their tools. Ever wonder what is in the other 71%? If so, try automating the inspection process to increase alert inspection and follow up.

Perform Inline Serial Tool Chaining

According to a 2016 Ponemon Institute study, organizations follow up on only 29% of security alerts issued by their tools. Ever wonder what is in the other 71%? If so, try automating the inspection process to increase alert inspection and follow up. This can be accomplished by tool chaining.

Tool chaining is a powerful solution for automating the movement of data packets in security monitoring solutions. An Keysight Vision-series network packet broker (NPB) can be used to capture suspect data and then pass that data serially to multiple security tools for additional security inspections and analysis. Based upon that analysis, the data can be killed, it could be deemed non-threatening and passed on into the network, or it could require further analysis/quarantining.

Use Application Intelligence to Capture Indicators of Compromise

Security breaches almost always leave behind some indication of the intrusion, whether it is malware, suspicious activity, some sign of other exploit, or the IP addresses of the malware controller. Application intelligence can be used to expose indicators of compromise (IOC) once a network has been compromised. IOC is the ability to detect application signatures and monitor your network so that you know what is and what is not happening on your network. Once this is coupled with other metadata, you have actionable intelligence that allows you to see rogue applications and aberrant behavior on your network.

SSL decryption can be used to expose hidden malware that made it into the network so that a DLP, IDS, or another security device can catch it.

Some examples of IOC include:

- Unusual levels of outbound traffic
- Outbound traffic to unusual IP addresses and geographies
- Unusual increases in application bandwidth flows
- Increases in read volume size
- Unusual increases in SAN access volume
- Applications using unusual ports
- Mobile device profile changes
- Large amounts of data being stored in the wrong places

One way to discover these IOCs is to look at metadata via enhanced NetFlow records. This metadata enables you to detect and investigate the footprint left behind. Keysight's Vision-series NPB with application intelligence (AppStack), allows you to generate NetFlow data based upon: application signature (and granular application actions), email addresses, credit card numbers, Domain Name System (DNS) traffic, and Web traffic (encrypted or not).

Deploy an NPB with SSL Decryption

While Secure Sockets Layer (SSL) decryption may have been performed when the data entered the network, if there is a breach, then something was obviously missed, and a DLP or other security tool will be needed for deep packet inspection to locate the threat. Unfortunately, many monitoring tools cannot handle SSL-encrypted traffic. Traffic with encrypted payloads sent to these tools is discarded, either immediately or after the central processing unit (CPU) has spent valuable processing capabilities and time on the traffic just to determine that it cannot, in fact, process the traffic. This not only decreases productivity, but it results in a higher security risk for the company due

to potential missed security threats. SSL decryption can be used to expose hidden malware that made it into the network so that a DLP, Intrusion Detection System (IDS), or other security device can catch it.

By deploying an Keysight Vision-series NPB with SecureStack (the SSL decryption capability), you have a fast and efficient way to decrypt the monitoring data once and then distribute it to multiple tools. Offloading the decryption function to the Keysight NPB allows you to improve tool performance, which can decrease the data analysis time. In some cases, security and monitoring tools can process encrypted data. Unfortunately, this is usually a costly feature upgrade, or the SSL inspection generates a significant performance overhead on security tools. In other cases, network monitoring mechanisms for SSL decryption involve using a special appliance to capture data packets, decrypt them, and then forward those packets on to special-purpose tools for analysis. However, unless you have a high volume of traffic that needs to be decrypted, the use case just mentioned can end up being a slower, more costly solution than using an NPB with integrated decryption capabilities.

Data captures and analysis must happen as close to real-time as possible. Automating workflows to create an adaptive monitoring environment is the only way to address the new needs.

An Keysight NPB equipped with integrated SSL/Transport Layer Security (TLS) decryption capability provides these value-added functions:

- Capture of the requisite data packets
- Decryption of the payload data with passive decryption
- Passing of the data on to the appropriate tool(s)

In an out-of-band solution, the decryption methodology works such that the decrypted data is just a copy of the network data, not the original data. So it does not need to be re-encrypted after being analyzed. It can also be discarded if not needed. For example, this capability can be used to decrypt Simple Mail Transport Protocol (SMTP) mail traffic and hand it off to an antiviral tool for virus and malware inspection. Other data can be decrypted and sent off to a DLP device for deep packet inspection.

Deploy an NPB for Automated Responses

With the myriad of changing security threats and the need for maximum network uptime, information technology (IT) personnel cannot accept the time limitations of a static programming process anymore. Data captures and analysis must happen as close to real-time as possible. Automating workflows to create an adaptive monitoring environment is the only way to address the new needs.

The automation of network monitoring allows you to align your security and monitoring tools with dynamic network changes to increase operational efficiencies. This creates an adaptive monitoring environment. The automation capability does this by creating an integration between a network controller device (like an SIEM) and an Keysight Vision series NPB.

A typical use case is for a SIEM to analyze data to detect any anomalies. SIEMs use log data to provide a wide view of the network and have powerful correlation capabilities. However, SIEMs themselves do not have packet-level visibility to analyze anomalies in detail.

Once the SIEM finds an anomaly, it can send a command through a representational state transfer (REST) interface to the Keysight NPB. Incident remediation can begin the instant an anomaly occurs, because the security tools and engineers have all the information they need. This type of solution speeds up root cause analysis, eliminates time-consuming manual steps, and
simplifies compliance.

Review Security Data Captures to Improve Forensic Analysis

When a network fault occurs, determining the exact resolution can be an art instead of a science. Common questions include: What exactly triggered the fault? What pre-event traffic was occurring? Is this fix the correct solution? Etc. IT teams need to be able to react quickly and accurately when the network is impaired, as a fast repair time is critical.

These IT teams need to quickly identify the root cause of a service outage and validate the fix in a lab environment. Replaying the traffic capture is not feasible as the volume of traffic is too high. Also, generating a predefined mix of constant traffic does not often reveal the issue. NetFlow-based security data captures can be created and viewed in the lab for tactical analysis of how a breach took place. This allows the security team to rebuild, in detail, how the attack was carried and what signs (IOC) were left as the breach progressed.

A product from Keysight called TrafficREWIND is the answer. It holds the records history of the traffic characteristics preceding the service outage. Keysight's BreakingPoint product can then regenerate the TrafficREWIND-exported traffic profile, allowing the response team to first reproduce and then identify the root cause and validate potential solutions.

This solution can also be used to validate the reliability of the production network when software patches and security policy updates are applied. As the mix of traffic varies during the day, multiple tests have to be conducted with individual most-relevant traffic mix snapshots. Keysight's AppStack capability continuously analyzes the production traffic and generates NetFlow data. TrafficREWIND records and synthesizes the NetFlow data, allowing users to visualize the traffic mix in 15 minute intervals and select the desired time window.

Once a breach has occurred and a solution defined, that solution can then be tested with a professional security tester, like Keysight's BreakingPoint solution, that can stress the equipment and network to its breaking point. You can see the real performance impact of decisions with various "what if" simulations (like SSL key and cipher impacts, latency due to SSL, how application intelligence would look with different geographies and traffic mixes, how DDOS mitigation would affect your network performance, etc.).

Conduct Cyber Range Training to Improve Threat Recognition

Organizations worldwide face a dangerous shortage of network security personnel with the skills required to defend against cyber attacks. This urgent situation is made worse by the weaknesses and vulnerabilities that continue to pervade critical IT infrastructures—despite billions of dollars invested in cyber security measures. Addressing these problems requires Internet-scale simulation environments, along with a comprehensive training curriculum and proven methodologies, to develop the skills necessary to defend and recover from attacks on the IT infrastructure.

A cyber range gives your team the practical experience it needs to be able to see and defend against modern security attacks in the best manner possible. It is one thing to read a driver's manual on how to operate a car, it is a completely different situation to successfully drive the car after only reading the drivers manual. You need practice to really understand how the components operate and how to recognize situations before and as they start to happen in real-time.

Cyber range training provides a safe environment for personnel to:

- Recognize patterns for security threats and compromise
- Recognize threats faster and practice responding to them properly
- Simulate critical infrastructure components, including computer servers and clients
- Simulate and conduct offensive operations against enemy targets
- Simulate and conduct defensive operations to protect critical infrastructure components

Perform Better Network Security Testing and Simulation

Many organizations rely upon penetration testing. Unfortunately, while penetration testing may have some benefits, conducting penetration testing will not help you once the bad actor has broken into your network. What is needed is a way to observe how a specific attack works and analyze the specific attack pattern to understand better how specific threats behave and how to defeat them.

Once a breach has occurred and a solution defined, that solution can then be tested with a professional security tester, like Keysight's BreakingPoint solution, that can stress the equipment and network to its breaking point. You can see the real performance impact of decisions with various "what if" simulations (like SSL key and cipher impacts, latency due to SSL, how application intelligence would look with different geographies and traffic mixes, how DDOS mitigation would affect your network performance, etc.). Running these types of simulations is important, because you cannot just cut services to your customers to correct a problem. You can also deploy additional tools like IxNetwork and IxLoad to see the performance impact on realistic video and voice streams when changes to encryption and other security measures are implemented. This data is critical for network and device dimensioning.

Capture Monitoring Data to Analyze Traffic Patterns

There are additional ways to create resilience in your security and network architectures. This includes segmenting the network to slow down network penetration by attackers. Network segmentation is a classical technique deployed in modern networks. For instance, an older but common IT policy used to give users access to network shares or File Transfer Protocol (FTP) folders. Now with software as a service (SaaS) collaboration (like SharePoint) the users do not have access to the underlying network layer, but data repositories are still segregated by the applications. Monitoring data can be captured an analyzed on the application level to look for IOC and IT policy compliance.

A second activity is to look at traffic patterns. This is where an Keysight NPB can be used to capture and filter either specific or general network monitoring data packets. This data is then sent to a purpose-built device for packet inspection to look at traffic patterns and other IOC.

Conclusion

If your enterprise network is like most others in existence, you have a security risk somewhere that someone can exploit. A strong security architecture is the best defense. Unfortunately, this will not be enough. Security architecture resilience is the next best approach—secure as much as you can, but build in network visibility and recovery systems to mitigate the effects of a breach as fast you can.

The network may get compromised, but the true test is how long it takes to recover. This time interval will directly determine the amount of intellectual property and financial loss that your organization will incur. This includes the amount of time a network is down (for instance during a denial of service (DoS) attack) to the amount of time it takes to realize that you have been breached and to stop the breach (which averages over 2 months). This is far too long—bad actors took whatever they wanted long ago. The exact cost reduction depends on the type and amount of security resilience and visibility architecture components deployed.

Keysight network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. For more information on network monitoring solutions, visit www.keysight.com/solutions/unleash-network-visibility.

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