WHITE PAPER

Security Resilience – The Paradigm Shift is Here

The CIO and CISO Security Challenge

As daily news stories continue to document, enterprises are struggling with how to prevent security breaches to their networks. Not only do breaches affect the company brand, but economic losses continue to mount, as well.

In the current business climate, it is not a question of if your network will be attacked, but when it will be attacked. And, the real question is how quickly can you respond to the threat and recover. In fact, these are two of the questions that keep chief information officers (CIOs) and chief information security officers (CISOs) up at night:

- Intrusion – Have company networks or systems been infiltrated by malicious actors?
- Breach – Has company data been "exfiltrated" from networks or systems into the hands of malicious actors?

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 recovering the network back to a normal, safe state as quickly as possible. This philosophy is called security resilience.

In the current business climate, it is not a question of if your network will be attacked, but when it will be attacked. And, the real question is how quickly can you respond to the threat and recover.

KEYSIGHT TECHNOLOGIES

What is Security Resilience?

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 the ability of your security architecture to recover and return to a normal state after an attack and/or breach. During attacks and breaches, minutes matter. A business needs this interval to be as short as possible.

Resilience is the ability of a system to return to its original form, positions, etc., after being bent, compressed, or stretched. It is also referred to as the capacity to recover from difficulties.

But, how do you go about creating such an architecture? The solution is to 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.

In addition, there needs to be a fundamental mind shift away from the common thought that network security is a one-time thing or a one-size-fits-all activity. Network security needs to be an ongoing process, not just occasional technology implementations, to create a resilient system. If it is not an ongoing process, enterprises risk exorbitant breach remediation costs that may even threaten company viability.

Once the security resilience shift occurs, a security and visibility architecture can be put into place that will provide three valuable assets to mitigate security threats:

- Better data to analyze security threats
- Better operational response capabilities against attacks
- Consistent monitoring and security policies

The Integration of Security and Visibility Architectures

One of the biggest security challenges for information technology (IT) staff today is to get the proper network information they need, when they need it, so that they can make informed decisions about network security and problem resolution. Proper network visibility is the solution. Without this visibility, how do you know that your network has not been breached? If your network has been breached, what was affected? This visibility gets back to the fundamental concerns that CIOs and CISOs have.

With the proper visibility architecture in place, you will be able to see what is (and what is not) happening on your network. There is a huge value that proper data acquisition can bring to your network security. When you actually integrate your security architecture with your visibility architecture, you will equip yourself with the necessary tools to properly visualize and diagnose the problems on your network.

Once you have the data you need, it can be fed to the security architecture. For instance, in the case of inline deployed security tools, Secure Sockets Layer (SSL) decrypted data can be fed to an intrusion prevention system (IPS), web application firewall (WAF), or data loss prevention (DLP) tool for inspection. Suspicious data can go through further analysis. Security threats can then be killed in real-time or diverted to a honey pot for further analysis.

Out-of-band security solutions can be employed to analyze data to detect breaches and either minimize or eliminate data breaches. Information from the visibility architecture is fed to security tools like a security information and event management (SIEM), DLP, intrusion detection system (IDS), or other analysis device to uncover the threat(s). Remember, the key is that, by integrating the two architectures, you will be able to improve your root cause analysis. This is not just for security problems but for all network anomalies and general issues that you often encounter.

Creating the Resilient Architecture

Consider the 2017 Trustwave Global Security Report, which shows that 57% of compromised victims did not detect the breach themselves. Those companies had to be informed by law enforcement, business partners, or (worse yet) customers that they had been breached. In addition, the 2017 Cost of Cyber Crime Study (from the Ponemon Institute) shows that average length of time from intrusion to identification is 191 days. While a breach may not be preventable, a duration of over 6 months for detection is unacceptable.

The 2017 Trustwave Global Security Report that shows that 57% of compromised victims did not detect the breach themselves. Those companies had to be informed by law enforcement, business partners, or (worse yet) customers that they had been breached.

Part of the problem is that typical network security often focuses on the following concepts:

- Access
- Architecture vulnerability

While these two concepts are definitely part of the solution, the equation to solve the whole problem encompasses more variables and includes the following:

- Access
- Policies and Procedures
- Architecture Performance (vulnerability and resilience)
- Monitoring and Auditing

For instance, IT professionals work to protect their networks. Conventional wisdom says to invest in securing access and architecture vulnerabilities. And, these are the main tools that you are probably using, correct?

- Firewalls and NGFWs
- IDSs and IPSs
- SIEM and DLP
- Penetration testing
- Forensic recorders

These devices are a good start, but it's not just about installing equipment. The philosophy of the security architecture is important, as well. There are typically four different approaches you can take towards network security:

- A best effort approach
- A design centered around regulatory compliance
- A defensive architecture
- A resilient architecture

Each of these approaches has different attributes and benefits associated with it. The chart in Figure 1, shows you the basic differences between the four approaches.

	Best Effort	Regulatory Compliance	Defensive	Resilient
Basic Security (FW, IDS, Sniffer)	•	•	•	•
Simple Monitoring (tap, crash cart)	•	•	•	•
Meet regulatory compliance (logging, policy)		•	•	•
Advanced Security tools (NGFW, SIEM, IPS, SSL Decrypt)			•	•
Out-of-band visibility (tap, NPB, tools)			•	•
In-line visibility (bypass switch, NPB)			•	•
Resiliency testing, Threat Intelligence			•	•
Security processes in place			•	•
Expose IOC & data exfiltration				•
Automate security responses				•
Cyber Range training				•
Advanced processes (network security life cycle)				•

A best effort approach is merely an attempt to just do something. While it may allow you to prevent an attack or two, it does not achieve real security.

A best effort approach is merely an attempt to just do something. While it may allow you to prevent an attack or two, it does not achieve real security. Basic components like firewalls, IDSs, and sniffers are a good start for security equipment. Visibility components are typically basic, as well (switched port analyzer (SPAN) ports, maybe some taps, and a crash cart for monitoring tools), but they often require Change Board approvals and delays before security and monitoring tools can be connected to the network.

The next level up is about adhering to regulatory compliance initiatives like Payment Card Industry (PCI), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act (GLBA), etc. While some may think this achieves real security, compliance initiatives are typically just guidelines that cannot be blindly followed, as there are too many dependencies like what the chosen security equipment and architecture is, specific business needs, how much and what type of personally identifiable information (PII) you use and store about your customers, the attractiveness of your company as a target, etc. This approach typically allows you to meet your company compliance initiatives but will most probably still leave your company vulnerable.

Do not misunderstand. You want to deploy tools and solutions that adhere to regulatory compliance, but the reality of modern threats means that you need go beyond this strategy.

The defensive approach is where you start to see real value from your security architecture. This comes from the blending of advanced security tools with visibility tools to get true visibility into what is happening and where it is happening on the network. It also begins with the integration of three core fundamental aspects of an effective security architecture—the blending of people, products, and processes to achieve true security. However, you cannot just throw security equipment at the problem and expect the desired results.

While advanced security equipment is part of the equation and includes next generation firewalls (NGFWs), IPSs, SIEM, DLP, forensic tools, etc., the solution also includes visibility products like out-of-band taps and packet brokers, virtual taps, and application monitoring. SSL decryption also removes the risk of concealed malware.

In addition, Keysight's BreakingPoint product allows you test and characterize the resiliency of your security components and security architecture, which often results in component savings of up to 30%, as well as a robust security architecture. Threat intelligence can also be used to reduce incoming threats and improve post-breach forensic analysis with better screening for known bad IP addresses. If you cannot see the threats and problems correctly, you cannot respond correctly. You also need to have proper processes, like continuity plans, escalation plans, etc. With this level of capability, you get a strong security architecture that is integrated with complete network visibility so that you can respond appropriately to security threats and reduce your mean time to repair by up to 80%.

A resilient security approach takes the defensive approach to the ultimate level. The core tenet here is that you probably cannot 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 PII and corporate intellectual property (IP). For instance, application intelligence can be used to expose indicators of compromise once a network has been infiltrated. SSL decryption can be used to expose hidden malware that made it into the network so that a DLP, IDS, or other security tool can still catch it. Cyber range training gives your team the practical experience it needs to be able to see and defend against modern security attacks in the best manner possible.

Lastly, incorporating advanced security processes and techniques (like a life cycle approach) with security resilience components can result not only in the reduction of security breaches, but can also reduce the cost of a successful breach significantly. The exact cost reduction depends on the type and amount of security resilience and visibility architecture components deployed.

A resilient security approach takes the defensive approach to the ultimate level. The core tenet here is that you probably can't 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 PII and corporate intellectual property (IP).

Conclusion

It would be nice to think that we could stop all security attacks, but that just is not the case. Media stories about breaches like Sony, Target, Home Depot, Yahoo, Anthem, and thousands of other companies prove this point. So, if you cannot make your network completely bulletproof, then what can you do? 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.

If you cannot make your network completely bulletproof, then what can you do? 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.

As part of a resilient security approach, you will want to characterize your network. Basically, you want to know that your network is as secure as possible and also how it will respond to a threat. The last thing you want is a self-inflicted outage—like security components that operate at half of their stated capacity or the blocking of all traffic instead of blocking just the bad traffic.

Finally, the network may get compromised, but the true test is how long does it take 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 6 months). This time delay is far too long–bad actors took whatever they wanted long ago.

The benefits of the security resilience approach can be summarized as follows:

- Implement real-time threat defense
- Reduce breach costs significantly
- Maximize network uptime
- Minimize PII record and financial losses
- Document security equipment (firewall, IPS, etc.) underperformance to receive potential equipment discounts from vendors
- Potentially earn cyber insurance discounts due to extensive security protections

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