Interested in learning more about security?

SANS Institute InfoSec Reading Room

Building the New Network Security Architecture for the Future

With the move to cloud services, software-defined networks and IoT devices, the game has changed in terms of defining an organization's network. Current network security architecture doesn't offer the visibility required for modern-day networks, much less guard against threats roaming within them. This white paper examines key elements of the network of the future and their optimal implementation.

SANS

A SANS Whitepaper

Building the New Network Security Architecture for the Future

Written by **Sonny Sarai**
Advisor: **John Pescatore**

Sponsored by:

NETSCOUT

January 2018

Introduction

Security teams have lost visibility into their networks. As recently as a few years ago, network boundaries were well-defined and data and devices easily identified. But a tsunami of new developments means that not only have we lost the boundaries of the network, but we have lost control over how and what is attached to it as well. With technologies such as IoT, IIoT (Industrial IoT) and cloud impacting network visibility, security controls have become less effective.

This lack of visibility creates gaps in the overall network security of an organization, making it difficult to see attacks, let alone stop them within the company's network boundaries. This makes it imperative to rethink the network security architecture to ensure that the necessary visibility is achieved within an organization's network.

In this paper, we will look at the shortcomings of today's network security architecture, some key technologies to advance it and a new security architecture that supports the evolution to cloud computing and IoT/IIoT.

Enterprise Networks Continue to Morph—But Are Not Yet Future-Proof

The past few years have brought significant changes to companies' network architectures, primarily due to:

- **Enterprise transformation.** Enterprise transformation is "any complex or fundamental organizational change that impacts how its core business is conducted. It can be caused by internal or external factors, but the result is a shift in how the organization relates to its wider economic environment."[1] Businesses want to interact with their customers in ways that were not possible before. Leveraging cloud and IoT technology has allowed them that flexibility.
- **Increased movement to hybrid data centers.** Services such as SaaS and infrastructure-as-a-service (IaaS) have expanded a company's network presence outside of its walls and into the cloud.
- **Improved analytics.** Interconnected smart sensors on a plethora of devices produce mountains of data. This information is used for analytics with the intent of making more informed decisions.

Table 1. How Cloud and IoT Impact Network Security

Technology	Impact on Security and the Network
Cloud (SaaS)	• Company data hosted on an external app, reliant on the cloud vendor's security
Cloud (IaaS)	• Company data and servers hosted on cloud infrastructure; network now extended to this environment • Greater visibility than SaaS • Gaps continue to exist because the customer lacks visibility into the cloud provider's underlying network; attacks at that level are out of the customer's control
IoT	• Network at increased risk of DDoS attacks • Company IoT devices may be compromised and part of a bot network if not properly secured • Insecure devices can launch internal attacks

These factors will continue to pressure security and network administrators to evolve and update their networks to handle the data, devices and security challenges of the near future. Table 1 outlines some of the impacts to network security as a result of cloud and IoT in an organization's network.

Traditional Legacy Networks

In the old network architecture, all systems were contained within the walls of the organization. If network boundaries extended to multiple locations, those locations were typically connected via private WAN link or VPN.

Visibility was easily achieved in the legacy network model, because the organization had control of the entire environment. Security and network teams implemented network packet brokers to manage traffic flows and deliver the packets of interest to the security tools, gaining a deeper understanding of what was occurring in wire data. Security teams implemented SIEM and IDS tools to provide deeper insight into security threats occurring in their environment. These solutions, when deployed effectively and with properly trained analysts, afforded great visibility into the network. Figure 1 shows servers, network gear, user computers and security architecture of a legacy network.

Because all systems were within the organization's control, achieving full visibility into the network was not a significant challenge.

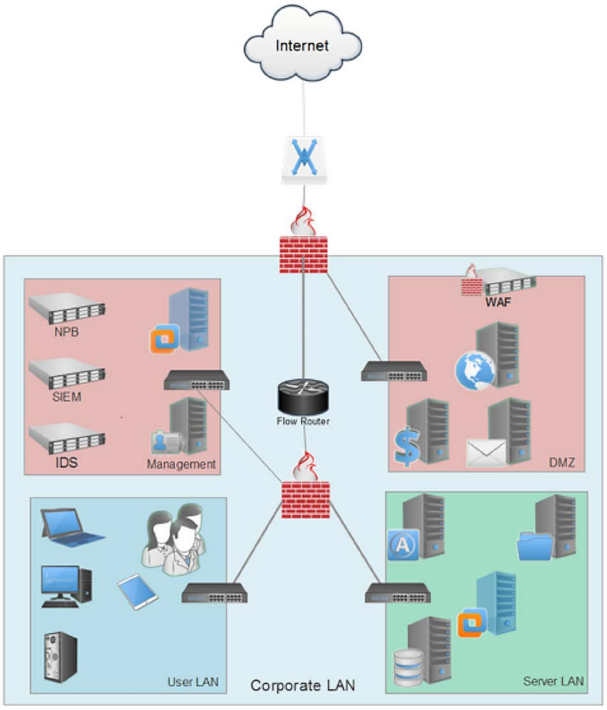

Figure 1. A Typical Legacy Network

[1] KPMG, "Enterprise Transformation Management," https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/Business-transformation-management-factsheet.pdf

Today's Network

Organizations today rely on a network architecture that differs significantly from legacy architectures. Some organizations still use the old network architecture, but it is fading away as organizations continue to adopt cloud services and implement IoT devices.

With the adoption of cloud, some control is lost and, as a result, proper visibility is not achieved. Using an old security architecture on a morphed network limits visibility into the cloud and IoT devices.

Figure 2 shows what networks using a hybrid data center model look like.

The hybrid model contains various cloud service deployments and IoT. Most have environments outside of the network boundaries of the organization such as a SaaS, IaaS or both. The deployment of the security and network monitoring tools in Figure 1 would not achieve the necessary visibility in Figure 2. This is because of the very nature of public/private cloud, which cuts off network visibility—not being able to effectively deploy tools such as a SIEM or IDS in the cloud results in limited visibility at varying degrees, depending on the cloud model being used.

A SaaS model does not allow visibility behind the cloud application, even though the customer's data is flowing through the cloud provider's network. An IaaS model provides more visibility than a SaaS model, but visibility is cut off due to a lack either of access to the cloud provider's network architecture or of tools (such as a cloud SIEM or a network packet broker) that could be employed in the cloud architecture. Private cloud should, in theory, provide the most visibility, because the customer is able to install whatever tools are needed. In reality, the customer might still lack access to the cloud provider's underlying network that the private cloud sits on.

EXPERT ADVICE: Security Analyst Specializing in Incident Response Within an Enterprise

"Implement a Zero Trust model within the organization, as the network perimeter no longer exists. One should build a security architecture with the understanding that assets will get owned (it is only a matter of time)."

Tools to implement in the new network security architecture are:

- Next-gen firewalls, with API or other orchestration features
- Micro-segmentation tools
- Email security solutions

The New Security Architecture

Security and network professionals now must protect not only the information and systems within the walls of the enterprise, but also the data and systems in the cloud and IoT/IIOT that now are an integral part of the security architecture. In essence, there is still the need for a perimeter—but the boundaries have to be extended out to include cloud-based services and devices.

Let's look first at the key issues with securing the network in the brave new world of IOT/IIOT.

The IOT and IIOT are highly vulnerable to becoming sources of large-scale DDoS attacks, and any effective new security architecture must provide strong protection against them. TechRepublic reports that DDoS attacks skyrocketed 91 percent from the first quarter of 2017 to the third quarter due to IoT.[2]

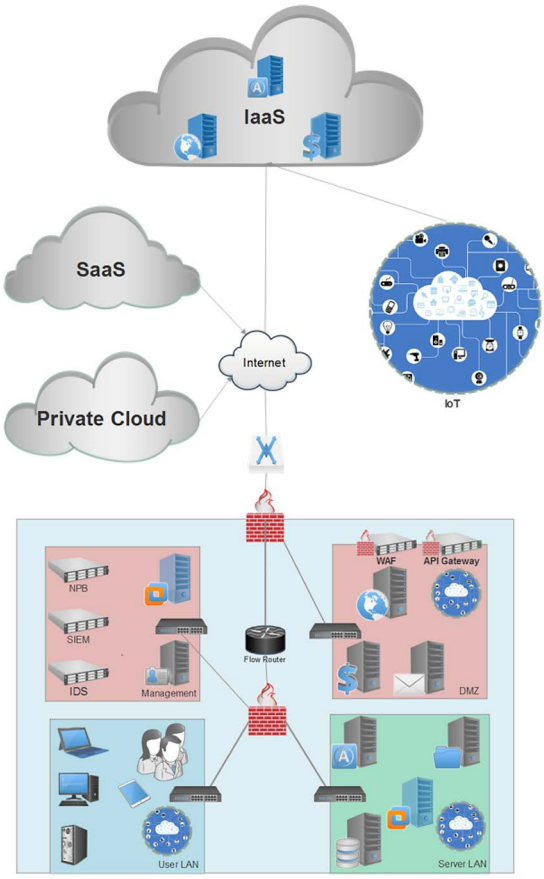

Figure 2. Hybrid Data Center

[2] "DDoS attacks increased 91% in 2017 thanks to IoT," Nov. 20, 2017, www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/

Therefore, it is paramount to ensure that your security design is architected to maximize visibility that extends beyond just traditional devices on internal networks. Take time to ensure that this design is well-thought-out and vetted by other IT teams. Before the design is finalized, determine what the requirements are, what technologies should be used (along with their objectives), and optimal placement of the technology to achieve this ideal architecture.

The Fundamental Need for Wire Data Visibility in the New Architecture

No matter what technology becomes the next big thing or what an organization's network looks like in the future, there will always be a need to have visibility into wire data. Wire data is the traffic highway that sends packets to and from their destinations. Visibility of the wire data is key from a security monitoring perspective. It provides insight into what is occurring on the network.

Examples include port scans, lateral movement, data exfiltration and data access. Malicious activity is very difficult to hide within packet data. A skilled investigator can even hypothesize nefarious activity when analyzing network metadata of encrypted traffic flowing through the wire. This is not a simple task, but with the right architecture and tool sets, it can be achieved.

IoT

The IoT phenomenon exploded onto the scene due to demand for big data and better analytics in a wide range of industries. But organizations must protect their IoT devices and data from being compromised, and to sufficiently protect IoT assets, visibility is required to understand what needs protecting and how to protect it.

IIoT

IIoT devices send telemetry and other types of data to a control system. These devices can be within an organization's network or out in the field. The risk of not reasonably safeguarding an IIoT device goes further than the danger of it being part of a botnet. Worse yet is a threat actor manipulating the data being sent to the controller. Take, for example, sensors used to regulate the temperature of perishable goods in transit being altered to provide inaccurate information. Decisions would be made with the wrong information, which in this case could result in loss of perishable inventory.

Using Packet Brokers in the New Network Architecture

Packet brokers are devices that ingest network traffic and subsequently aggregate, replicate, deduplicate and forward the traffic to network security, analytic and monitoring systems. With the evolution of software-driven packet brokers that decouple packet broker functionality from hardware, this functionality can be deployed cost-effectively and at the scale required for new network architectures. In virtualized environments, virtual taps can work in conjunction with software-driven packet brokers to gain the packet visibility needed in the cloud.

Packets provide visibility into the customer's traffic in the cloud and subsequently send the traffic to the appropriate network and security monitoring tools. This is potentially a game changer in terms of visibility. One of the biggest concerns with the cloud is not having the necessary visibility into wire data to understand what is going on in the network. Software-based packet brokers, if configured correctly, provide this visibility. Ideally, the broker's target systems should be in the customer's location so that any data analysis and network performance monitoring can be performed locally.

Architecture Scenario 1: IIoT devices are within the company's LAN/WAN

This scenario speaks to recommendations in two areas:

1. **Security architecture to help protect against a company's IIoT devices being compromised**
2. **Security architecture to help prevent compromised IIoT devices from infiltrating other areas of the network**
    - **Place a firewall in front of the IIoT devices and ensure they are behind a NAT.**
        - It does not have to be a next-generation firewall; a simple Layer 3/4 firewall will suffice. This is a good example of the use of older security technology making sense.
        - A firewall ensures that the IIoT devices are not directly reachable from the outside. This helps if the firmware is forcing the use of Telnet and has credentials hard-coded. If the devices do not require Internet access, then ensure block rules are in place so traffic originating from it cannot get out.
        - If the device requires Internet access, then allow it to send only outbound traffic to specific IP addresses. No inbound traffic should be allowed unless it is stateful.
    - **Ensure traffic monitoring is configured through some type of network flow information.**
        - This allows visibility into the network, thus enabling baselining of traffic. Now one can identify what is normal traffic within a given period of time.
        - Alerts can be configured for notifying appropriate personnel if traffic deviates from the baseline.
    - **Place network IDS/IPS sensors along the edge of the IIoT network.**
        - This allows the sensor to monitor and alert on any suspicious traffic.
    - **Segment off the IIoT devices from the user community and data center.**
        - This ensures that if an IIoT device gets compromised, it will only affect other devices on the same network segment. Do not let them hop segments.

Architecture Scenario 2: IIoT devices are deployed in the field outside of the company network

Ensuring proper security and visibility for devices out in the field requires a different security strategy than for devices on the company's network, as in Scenario 1. In most

cases, the defenses would be designed on a case-by-case basis, but some actions can be recommended:

- **Place a lightweight, industrial-grade firewall in front of the IIoT device.**
  - Most, if not all, IIoT devices collect and send information to a centralized system, usually in the cloud or in a company's data center. Connecting an industrial-grade firewall router and configuring a VPN connection ensures that communication can go between only the centralized data collector and the IIoT device.
  - Protecting an IIoT device with a lightweight firewall reduces the risk of malicious intrusion.
- **Maintain network segmentation between IIoT devices and information technology systems.**
  - Segment off any IT services from IoT device communication at the corporate level. Most IoT devices should run in a separate segment from critical business systems. They should have little or no communication with information technology services, such as user desktops and data center operations. Follow the practice of implementing a Zero Trust model for the IoT segment. This means implementing strict access control from within the IoT segment and for traffic in and out of the IoT segment. Treat as a hostile environment.

Cloud-Hosted Network Security Devices

In the preceding section, we made some recommendations for addressing the unique security issues presented by IoT and IIOT. Let's now turn to the issue of cloud.

Security teams must ensure that the security posture of their cloud service's infrastructure is at a reasonable level. Network security vendors understand the need to have network security devices in the cloud that are similar to what were historically used on premises, because that increases visibility. Visibility is the key takeaway here, because you cannot protect systems you cannot see. Keep in mind that these devices are there to protect the customer's environment within the cloud, not the cloud vendor's entire environment.

Here are some of the top virtual network security appliances that can be used in IaaS scenarios:

- **Virtual web application firewalls.** These are designed to protect against attacks on websites in the cloud. They work almost identically to the on-premises web application firewalls from the same vendor. Most vendors that have a mature web application firewall solution offer an equivalent virtual edition. For example, vendors would offer the virtual edition in the AWS or Azure Marketplace. The firewall still sits in front of the website to shield it from malicious traffic. The web server, even hosted in the cloud, should be protected the same way it would be protected on premises.
- **Virtual network-based firewalls.** Firewall vendors have also added their solutions to the cloud as virtual appliances. Code base is typically the same. A virtual

EXPERT ADVICE: C-Level Executive, Head of Information Security at an Enterprise

"In my view, any security architecture should be built based on 'defense in depth,' starting from your endpoint, moving up to servers, network and access control. The traditional concept of having all endpoints within a defined physical network is not working anymore. Users need to work from different locations, with different devices over a network that the company has no control of. The new design should be built to accommodate new technology trends such as cloud and IoT."

Candidates to include in the ideal network security architecture:

- Vulnerability management program to include endpoints in the cloud
- Log monitoring and analytics system that monitors assets in the cloud
- Security that is baked into DevOps' day-to-day activities, as per the DevSecOps principle
- Tools that monitor, record and map network traffic, with the objective of gaining visibility across the entire network

network-based firewall would sit at the edge of a customer's cloud network to protect the perimeter, but it could very well be placed in the Internet network to segregate between subnets.

- **Virtual routers.** These solutions allow cloud customers to implement a full-featured router. They can be equipped with firewall and advanced routing capabilities. These routers can be utilized in the cloud environment, just as they would in a customer's own network. Routing, access lists and stateful firewall rules can be configured between subnets in the cloud. Virtual routers can also be used to create site-to-site VPNs between the customer's infrastructure in the cloud and on premises. This is ideal if an organization uses one vendor for all its networking solutions. It can continue with that approach if the vendor's routers are available in the cloud marketplace. This simplifies the environment.

Along with analyzing wire data, logging of network activity should be paramount in the design of the security architecture. Ideally, security-related events should be sent to a centralized logging and analytics system to assist with correlating events of interest. This centralized log collector should be on premises and not in the cloud. A combination of wire data and logs greatly enhances visibility, because packets tell us what's going on in the wire. Logs tell us what is occurring on the endpoints.

Most virtual solutions are deployed in an IaaS model, because customers typically don't have access to the cloud's back-end network infrastructure in SaaS and platform-as-a-service (PaaS) models. The security architecture would be different in these two models, as discussed later in this paper.

Manage and Monitor

The principle of managing and monitoring security events is fundamentally the same in the modern network as it is in legacy networks. With the inclusion of consumer and Industrial IoT, cloud, BYOD and software-defined networking (SDN), the difference comes in how these security tools are placed to provide the most network coverage. This is a big challenge, especially in regards to IoT devices deployed in the field and the cloud. SaaS providers, for example, rarely give customers access to their network infrastructure, so customers are unable to place network and security monitoring tools to alert on any security events in the cloud. However, that does not mean security events should not be managed.

The objective for effectively managing and monitoring is to quickly and effectively detect security events within the organization's environment and to prioritize, manage and respond to those events. The difference between monitoring for security events in legacy networks versus the modern network is coming up with the additional use cases from which to build your monitoring capabilities. Some of the key areas in preparation of effectively managing and monitoring for security events include:

- Having visibility into wire traffic
- Knowing what is normal traffic in terms of network traffic

This must be done in all areas of the company's network. Once this is in place, then configure monitoring for deviations from what is normal.

EXPERT ADVICE: Information Security Consultant Specializing in Risk Management

"A successful security architecture is one that is baked into the initial design of the supporting components. Security concepts that are recognized as best practice or a minimum starting point are applicable (e.g., detection/monitoring, segregation, access controls, prevention/blocking controls, etc.), but must be tailored to the environment they are being installed within and accommodate for current and future dependencies."

Technologies important for the ideal security architecture are:

- Honey pots—A strategic way to uncover malicious activity and identify possible behaviors to monitor for
- Web application firewalls—Additional protection and visibility for external-facing web servers
- IDS—A system that provides visibility into odd activity and a strategic way to identify lateral movement within a network
- Firewalls or special-purpose unidirectional gateways—A way to achieve physical control of information flow (in one direction), where segregation of environments exists (e.g., an IIoT environment)
- Zero Trust networks—Technologies to establish encryption of network communication paths within internal networks; to require authentication of users, devices and applications to cross-segmented network boundaries; and to inspect all network traffic

Internal Network

Monitoring the internal network is vital for effective visibility. The primary focus of monitoring used to be prevention, but a few years back it moved to detection. This is no different in the modern network. Operation technology (OT) environments that house IIoT devices must be monitored the same as the IT environment. Cloud environments, especially IaaS, must be monitored the same as the on-premises environment. A customer's infrastructure in the cloud should be viewed as an extension of an organization's internal network and, as a result, monitored the same as on-premises. Therefore, the role of monitoring internal network traffic has expanded to more areas of the customer's network or boundary. The principles of monitoring the network are the same, but the scope is larger.

Because the network boundaries have expanded due to hybrid data centers and IoT, these monitoring devices must be well-placed to ensure proper visibility. Start by understanding where all your systems and data reside, both in the cloud and on premises. Then learn where you have gaps in your existing security architecture in terms of visibility to all your data and systems. From there, build your requirements to address those gaps and apply the necessary security architecture appropriately.

An area where there is not historically sufficient visibility is the cloud—in both IaaS and SaaS models, with each model having different requirements. For example, visibility as to whom, when and where connections are being made to SaaS services can be achieved using a cloud access security broker. CASB is a solution that proxies the connection between the client and the SaaS application. It provides logging, auditing, access control and, with some vendors, encryption capabilities. The logs can then be sent off-box to a SIEM or another log analytics tool. Logs can then be correlated to detect anomalous behavior.

IaaS, on the other hand, has more options available in terms of security architecture. For example, many network vendors have made virtual security appliances—such as next-gen firewalls, web application firewalls and many others—available in cloud marketplaces.

Cloud Configuration

Careful thought must be taken when designing the security architecture in a cloud environment. Designs differ depending on the cloud service model being used. Ideally, the security architecture should be planned during the design phase of the project. This way, security does not have to be added in after the fact, which has the propensity to cause certain issues or delay implementation. There is greater flexibility to implement more security tools in an IaaS model. A SaaS model, however, significantly reduces the security architectural options that can be implemented. Table 2 lists the ideal network security architecture for each cloud service model, focusing on network-related security owned by the customer.

EXPERT ADVICE: Head of Network at an Enterprise-Level Organization

"One of the bigger risks is lack of security with IoT devices. It is like the Wild West in terms of insufficient oversight and governance. The SaaS model of network security in the cloud is very limiting for customers and offers little to no control. The IaaS model provides much more flexibility, as the customer is building up the network infrastructure within the cloud and then building up the system stack to the application layer."

Key network security technologies he feels are important:

- 802.1x and NAC (not just for corporate assets such as desktops and laptops, but also for mobile devices including BYOD)
- Security tags (traffic policy created based on tags injected into each packet)
- NGFW (next-generation firewall) implemented in various parts of the data center, with a focus on monitoring and protecting against unauthorized east-west traffic)
- Secure tunnel between corporate data center and cloud IaaS environment
- Virtual firewall and flow data in the cloud
- Signature- and behavior-based IDS/IPS with machine learning (next-gen IDS)

Identifying Blind Spots in the New Network

Legacy network architectures can leave gaps in a company's security posture, with blind spots in the network due to lack of visibility in the cloud and IOT/IIOT. This reduced visibility can render existing security controls useless or ineffective.

As we consider architecting a new and improved network, what existing technologies can be implemented in new ways to help secure today's—and tomorrow's—networks? While some tools have potential shortcomings, they can be utilized in different ways in a new security architecture for protecting data, devices and the network. Some recommendations:

Table 2. Ideal Network Security Architecture for Cloud Service Models

Cloud Service Model	Applicable Network Security Architecture Owned by Customer
IaaS	Software-based packet brokers IDS/IPS SIEM (D)DoS attack prevention Virtual security appliances (WAF, router, NGFW) Network segmentation
PaaS	***(Limited from a network security perspective when implemented by customer)*** SIEM Logging IP restrictions (if applicable) (D)DoS protection API gateways Cloud access security broker
SaaS	***(Limited from a network security perspective when implemented by customer)*** SIEM (D)DoS attack prevention Logging IP restrictions (if applicable) API gateways Cloud access security broker

1. **Signature-based antivirus: What is the role of traditional antivirus tools?**
   - **Shortcomings**
     - Insufficient to detect unknown threats or zero-day attacks because they can only detect malware for which it has a signature
     - Easy to evade by simply modifying the binary or re-encoding the payload to make it undetectable to most antivirus software

   Recommendation: Do not rely on signature-based antivirus solutions alone. Most reputable solutions implement a behavior- and heuristic-based approach while still incorporating signatures to detect viruses. They still have a place within the security architecture as long as they are not the only method to detect viruses. Having a multilayered strategy for your antivirus will ensure the greatest coverage. Make sure AV placement on virtualized servers does not degrade resources.

2. **Layer 3/4 firewalls: Do these firewalls offer anything useful to a re-imagined network?**
   - **Shortcomings**
     - Unable to deny or allow traffic based on application
     - Cannot detect malicious traffic outbound on standard ports such as HTTP/HTTPS and DNS
     - Lack effective built-in web content filtering

   Recommendation: Legacy Layer 3/4 firewalls continue to have a place in security architectures—they just need to be deployed differently. For example, a next-gen firewall can guard the perimeter as well as guarding between the user network

segments and the IT data center. But stateful Layer 3/4 firewalls should be placed in segments where there is not much traffic, such as between the IoT segment and the IT data center.

Alternatively, the firewalls could be used instead of a Layer 3 switch to configure multiple subnets and apply security policies. This is especially useful in network segments where systems do not communicate much with each other.

3. **Signature-based IDS: How can IDS be used in the new network that faces new kinds of attacks?**

   - **Shortcomings**
     - Mainly detects known bad as opposed to unknowns
     - Has time gaps between the discovery of a new vulnerability or exploit and the creation of a signature, which must then be pushed down to the IDS; the network is at risk of attack during this window

   Recommendation: Similar to the signature-based antivirus approach, look for IDSes that incorporate both behavior-based detection and signatures for the detection of anomalous behavior. Criminals inside a network use common behaviors and tools when moving laterally, such as PSEXEC or password-spraying domain controllers. Signature-based IDS systems should detect this behavior if tuned correctly.

   One can place the signature-based IDSes in less sensitive areas of the network. As an example, network segments dedicated to quality assurance or user acceptance testing might not have a lot of traffic. Utilizing these older IDSes could help reduce the cost of buying a modern-day IDS that has behavior-detection capabilities, while still ensuring that visibility is maintained.

4. **Descriptive analytic tools: What role will data analytics have in the new network?**

   - **Shortcomings**
     - Uses data that describes past events
     - Lacks capability to conduct predictive and prescriptive outcomes

   Recommendation: When conducting an investigation, we will always need to know what happened. Descriptive analytic tools help us understand just that. They also assist with summarizing datasets, such as how often brute-force attacks were conducted against a web server or where attacks against the e-commerce application are coming from geographically. This can help us make informed decisions on how to improve security on these systems. While descriptive analytic tools should still be part of the security arsenal, they are best packaged in another tool such as a SIEM or IDS. This way, the analytics is done on the tool that alerted on the event.

Although these older security technologies have limitations, they should not be replaced altogether, because they still can support a stronger security posture when used appropriately in the new network. It is also important to not rely on these tools alone.

Conclusion

The network has evolved significantly from a few years back, when it was better defined and network and security practitioners had a solid idea of their network's boundaries. The emergence of digital transformation, IoT and cloud has caused the network architecture to continue to expand and morph. With the capabilities offered by this newer technology come increased security risks caused by blind spots in the network.

Defending against attackers in this modern network calls for a different way of thinking. The old network security architecture is no longer sufficient; combating today's threats requires updating to a security architecture that leverages evolved security technology. This does not mean that older technologies must be replaced. Instead, they need to be utilized or placed differently on the network to ensure effective security.

About the Authoring Team

Sonny Sarai, SANS GIAC Advisor, has more than 10 years' IT experience, 8 of them in an information security capacity. He now works in the Canadian retail space as a senior information security analyst, responsible for data governance, compliance, penetration testing, digital forensics and incident response. Sonny holds a degree in forensic investigation, specializing in computer crime. He holds a CISSP and industry-leading certifications from SANS in advanced digital forensics (GCFA), network intrusion detection (GCIA) and security essentials (GSEC). Sonny has an extensive lab dedicated to research, development and analysis, where he continually hones his skills and enhances his capabilities.

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTE, and service with both the National Security Administration, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems "and the occasional ballistic armor installation." John has testified before Congress about cyber security, was named one of the 15 most-influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this paper's sponsor:

NETSCOUT®

Last Updated: February 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VAUS	Mar 17, 2018 - Mar 24, 2018	Live Event
ICS Security Summit & Training 2018	Orlando, FLUS	Mar 18, 2018 - Mar 26, 2018	Live Event
SANS Munich March 2018	Munich, DE	Mar 19, 2018 - Mar 24, 2018	Live Event
SEC487: Open-Source Intel Beta One	McLean, VAUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TXUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, AU	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Boston Spring 2018	Boston, MAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS New York City Winter 2018	OnlineNYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced