ARCHITECTURE MATTERS

Beyond Layered Security Approaches

Every year, record levels of money are spent on new IT security technology – yet major breaches and compromises are more prevalent than ever. The concept of “layered security” – in which an organization supports a wide variety of security technologies in order to discourage attackers – doesn’t seem to be working. It’s time to rethink IT security – not just the technology, but the way it’s approached from a strategic, architectural perspective. There are ways to build a comprehensive set of defenses – a security architecture – that can not only discourage attackers, but actually prevent data breaches. This white paper looks at how the foundational architecture of a next-gen firewall and security platform “matters” in enabling the business and protecting it against a wide variety of attacks, how it enables unique and specific security scenarios, and how it supports a prevention-oriented approach.
# Table of Contents

- Executive Summary ........................................... 3
- Growing Security Risks ..................................... 4
- Changes in Cyberattack Lifecycles ...................... 4
- Addressing Security Requirements ....................... 5
- Evolution of Network Security Architectures ........ 5
- Current State of Network Security Architectures .... 6
  - Layered Approaches via Sequential Point Products 6
  - Integrated Security Architectures .................... 6
- Use Case – File Filtering for Multiple Web Apps .... 7
- Expanding to an Integrated Security Platform ....... 8
  - Prevention Across the Organization ................. 8
- Platform Use Case – Controlling SaaS File Access 9
- Summary ...................................................... 10
**Executive Summary**

This white paper looks at the benefits of an integrated, unified security architecture over the sequential, additive approaches that have evolved in the industry. We'll look at the ability of security architectures to address modern threats while supporting the use of new applications and IT architectures.

IT faces a growing set of security challenges as networks, endpoints, and applications (along with their supporting infrastructures) continue to evolve. At the same time, cyberattacks have become increasingly sophisticated, often unfolding in multiple stages that can bypass uncoordinated layers of security.

The safe enablement of applications and prevention of modern attacks require the careful examination of network traffic across a broad range of contextual information that includes the application, user and content (such as transferred files, URLs and data patterns). The effectiveness of security architectures at detecting and stopping modern cyberattacks is highly dependent on how well they can uncover patterns of behavior spread across multiple concurrent indicators.

To address these threats and, at the same time, support progress, organizations need to implement a security architecture that can:

- Reduce the attack surface across the distributed organization.
- Secure apps everywhere on servers, endpoints, and in the cloud.
- Analyze all threat indicators together in context rather than just individually in isolation.
- Enforce comprehensive, flexible security policies based on full application and threat context.
- Detect and stop ongoing attacks before they result in costly data theft or sabotage.
- Uncover suspicious behavior from unknown threats to stop current and future attacks.
- Integrate with existing systems to simplify operations and enable new forms of IT.
- Continue to evolve to support the organization’s ongoing need for agility and efficiency at an acceptable level of risk.

In general, network security architectures follow either a sequential, layered approach or a holistic, integrated design:

1. **Layered Approaches**: grown piecemeal from layers of point products or functions (e.g., UTM), each of which looks at the traffic’s context or threat factors individually, applying limited sets of security operations in sequential steps. Each layer focuses on specific context and is unable to pass along complete information to subsequent layers, limiting the possible security options.

2. **Integrated Architectures**: unified security designs that classify all traffic into a full context before applying a single set of flexible security rules in one pass.

The limitations of layered security approaches aren’t just theoretical. Common use cases, such as applying distinct file filtering policies to specific web apps, are impossible to achieve using a sequential layered approach to security.

In contrast, integrated security architectures avoid these limitations by first extracting full context and then providing the entire context to a single, unified enforcement model. In addition to more comprehensive security options, this approach allows organizations to easily define and refine security policies for better operational flexibility.

Palo Alto Networks Next-Generation Security Platform extends the integrated architecture approach to provide unique, prevention-oriented capabilities for securing computing environments, reducing attack surfaces, detecting and stopping both known and unknown threats, and enabling organizations to safely deploy increasingly complex applications on evolving IT infrastructures.
Growing Security Risks

IT teams face growing challenges as the applications they need to safely enable, along with their supporting infrastructures, continue to evolve. The users and endpoints accessing these applications have also spread and changed, greatly broadening the scope of what IT must manage and secure. While adapting to these changes is a necessity, it must be done at an acceptable level of risk.

In order for IT to safely take advantage of these changes and advances, security systems must defend the organization from increasingly sophisticated threats and a growing attack surface resulting from:

- **Migration to the Cloud:** Users, data and apps are moving outside the organization and into the cloud, making attack detection and security enforcement more challenging.
- **Shared App Infrastructures:** Movement of apps away from proprietary coding and toward widely used frameworks (e.g., web browsers, LAMP, Java, Office) creates a high-yield attack surface and allows one exploit to be leveraged against a growing set of target apps.
- **Common Ports and Protocols:** Migration of app traffic away from proprietary client-server protocols/ports onto standard HTTP(S) web-based protocols makes application traffic impossible to control at just a port level.
- **Growing User Base:** Employees and end users, both of whom are increasingly mobile, often connect to IT resources from outside the organization rather than internally.
- **Diversification of Endpoints:** Not only desktops but also an ever-more-diverse range of mobile, BYOD, and Internet of Things (IoT) endpoints need to be secured.
- **Greater Risks and Costs:** The scope and resulting damage from attacks, especially those ending in large-scale data thefts, has grown significantly.
- **Easier and Faster Attacks:** Attackers benefit from faster news of zero-day exploits and ready access to time-saving malware development frameworks.

At the same time, for organizations to remain productive and competitive, security must enable many of the same trends that are also driving risk (e.g., cloud, mobility). Secure IT systems and uninterrupted connections to the Internet and other external locations are an absolute necessity for the successful, day-to-day operation of organizations.

Changes in Cyberattack Lifecycles

Cyberattacks continue to grow in complexity and sophistication. The full lifecycle of an attack can extend over weeks or even months, moving through a series of stages:

1. **Gather Intelligence:** This is the initial stage, consisting of probing and intelligence gathering, to detect weaknesses and exploits to be used later in the attack.
2. **Leverage Exploit:** One or more of the discovered exploits and weaknesses are used for an initial infection with malware.
3. **Execute Malware:** The malware runs within the organization’s network, performing further intelligence gathering and building a beachhead to leverage additional exploits.
4. **Control Channel:** Communications out to the attacker are established as a command and control channel to covertly send back new intelligence and receive ongoing attack instructions.
5. **Steal Data:** The final stage of an attack typically culminates in a data breach or theft, system disruption, or even the encryption and ransoming of critical business data.

![Figure 1: Cyberattack lifecycle](image-url)
Detecting cyberattacks during their lifecycle requires a careful examination of network traffic across a broad range of contextual information or factors including applications, users, and even the traffic’s content (such as transferred files, URLs and data patterns). Security architectures need to be able to develop full context for the attack’s traffic as it moves through the stages of this lifecycle in order to detect and stop the attack before it achieves its end goal.

Addressing Security Requirements
How can you counter these growing security risks and safely enable new classes of apps and their supporting infrastructures in the face of increasingly sophisticated cyberattacks? The simplest approach of just prohibiting all new apps, endpoints and IT infrastructures isn’t feasible – security must enable the organization’s productivity and growth, not limit it.

Instead, IT needs to implement a planned and integrated security architecture that can:

- Reduce the attack surface across the distributed organization.
- Secure apps everywhere on servers, endpoints, and in the cloud.
- Analyze all threat indicators together in context rather than just individually in isolation.
- Enforce comprehensive, flexible security policies based on any or all application and threat information.
- Detect and stop ongoing attacks before they can culminate in costly data thefts.
- Uncover suspicious behavior from unknown threats to stop current and future attacks.
- Integrate with existing systems to simplify operations and enable new forms of IT.
- Continue to evolve to support the organization’s ongoing need for agility and efficiency at an acceptable level of risk.

Evolution of Network Security Architectures
Examining how most current security architectures have evolved over time can help reveal their limitations, which are often the result of an unplanned design that has grown via the addition of sequential layers as the security challenges and attacks they face have become increasingly sophisticated.

As shown in the illustration below, legacy security approaches have evolved over the last twenty years from simple port-based perimeter firewalls to a sequence of point products strung end to end.

6. Addition of Sequential Point Products: That basic firewall security then grew via accretion of additional filtering and enforcement point products, like proxies, URL and email filters, and antivirus scanning, that were added one on top of another over the years as new approaches were used in attacks. However, these layers weren’t integrated, as they were added one at a time and operated in a stand-alone fashion.

7. Consolidation into UTMs: The next stage attempted to address this lack of coordination by consolidating these multiple products into a unified threat management (UTM) system. There was some value in consolidation; but, typically, it didn’t include any significant increase in coordination or information sharing between the security functions consolidated within. Functions often have separate rule bases and management requirements, making the deployment and subsequent modification of security postures difficult and prone to errors or gaps.

Figure 2: Evolution of security from firewall to layered
This layering of point products over time, and even their consolidation into UTMs, was never based on any deliberate, planned architecture. Instead, it is an accidental patchwork that was not designed with new applications and their environments in mind.

**Current State of Network Security Architectures**

Current network security architectures can be divided into two fundamentally different approaches, as shown in Figure 3 below:

- Legacy layered approaches that evolved from sequential additions of point products, each typically focusing on a single threat approach.
- Integrated architectures that first develop full context for all traffic, followed by enforcement of a unified set of rules, all in a single pass.

**Layered Approaches via Sequential Point Functions**

As discussed earlier, when examining how security architectures evolved over time, sequential layered approaches have grown by accretion rather than by design, starting from simple port-based firewalls and then adding successive layers of point products, each focused on one threat approach. Even when deployed as a consolidated UTM, the individual layers don’t have access to the full context of application and user information.

As a result, layered security approaches have a number of significant limitations:

- The range and specificity of security policies are constrained by the limited contextual information passed between layers.
- Lack of a rich enforcement model across different filters limits the control that each filter can have on the traffic.
- Inefficiencies are introduced as each layer potentially repeats the work of previous layers to derive limited context.
- Significantly more complex management (even in UTMs) resulting in lost IT productivity, potential misconfiguration, security gaps, and needlessly restrictive policies.

Because of these limitations, layered approaches lack the flexibility that organizations need to effectively manage risk.

**Integrated Security Architectures**

Integrated network security architectures, in contrast to layered approaches, follow a deliberate approach to efficiently classify and enable flexible control over all traffic.
The Palo Alto Networks Single-Pass Architecture is an example of an integrated security architecture, and is the basis for Palo Alto Networks Next-Generation Firewalls. The architecture:

- Initially classifies all traffic through the application and application function level. This even includes classification of encrypted traffic, which is important since it’s estimated to account for 30 to 40 percent of all traffic within typical organizations.

- Next, it identifies the users behind application traffic in a way that makes it simple to understand and control traffic in the organization. For example, rather than specifying IP numbers, the security rules can instead specify user identities and group memberships.

- Finally, it continually updates this understanding by inspecting the traffic's content. This continuing inspection is needed as apps can change activities throughout their session lifetimes, and detecting and responding to these shifts can be significant in keeping an environment secure.

The full context described above is provided as input to a unified set of security rules, and these security rules can define their actions based on any combination of the context provided.

Benefits from this integrated, single-pass architecture include:

- Safe enablement of new apps and supporting infrastructures since comprehensive, precise security policies can be based on more complete context than is possible with a layered approach.

- Simpler management, including straightforward translation of business policies and practices into a single shared set of security rules, reducing the potential for errors or gaps.

- Greatly reduced attack surface across the organization by only letting authorized apps (for authorized users) run, and detecting and blocking threats across all allowed traffic.

- Insight into uncontrolled traffic, allowing it to be studied and added to security rules as appropriate.

The benefits listed enable organizations to move toward a Positive Enforcement Model (PEM). A PEM specifies what is allowed to run on an organization’s network, and traffic that does not match what is allowed is denied by default. While fully adopting a PEM is often aspirational, the single-pass architecture allows rules to be progressively refined based on meaningful application and user characteristics. Over time, the amount of uncontrolled and unknown traffic is reduced to the point where it can be denied without disabling the business.

Use Case – File Filtering for Multiple Web Apps

To highlight the benefits of an integrated security architecture, we’ll look at one of the most common and widespread changes in app infrastructures – the movement of both apps and system tools out of proprietary client-server code and into web apps and Software-as-a-Service (SaaS).

In this use case, three distinct classes of web apps each need to have different security policies applied to limit which files can be uploaded and downloaded by users. In order to balance business productivity with business risk, the following use case might need to be supported:

- Web Browsing: Block all file downloads except for PDFs, as well as all file uploads, preventing both malware infections and data exfiltration.

![Figure 4: Use case of file filtering for web apps](Image)
• **Cloud Backup:** Allow both uploading and downloading of all file types to allow the app to function as a complete backup service.

• **SharePoint Online:** In general, allow uploading and downloading of files to support corporate data-sharing objectives. However, to limit the risk of malware infection, transferring of executables is blocked.

The integrated, Palo Alto Networks single-pass architecture can easily support the set of security policies to implement this use case. That’s because all the relevant traffic context (app name, function, file type, etc.) is available and can be precisely controlled.

In contrast, layered or sequential approaches cannot support this increasingly common use case since the filters implementing app classification and file filtering are in two separate components, with no one layer having a complete knowledge of the entire context (in this case, the filter controlling file blocking has no knowledge of the application). In the past, the unique port numbers and protocols used by proprietary apps could have been used to simulate app-specificity for these types of security policies. However, since these web apps all use a common set of ports (i.e., 80 for HTTP, 443 for HTTPS), it is impossible for a layered file filtering policy to be applied to just a specific web app because application context is not shared with all places that apply control (e.g., file blocking).

**Expanding to an Integrated Security Platform**

The integrated, single-pass architecture we have described is the basis for Palo Alto Networks Next-Generation Firewall (NGFW). Palo Alto Networks Next-Generation Security Platform extends this integrated architecture approach to provide unique, preventive capabilities across a distributed organization.

The platform does this by providing visibility and control across all locations where an organization’s users, applications and data exist. Elements in the platform (which includes the next-generation firewall) also coordinate as needed to share and correlate threat information that can be used automatically for prevention or to provide actionable insight to security practitioners.

**Prevention Across the Organization**

These benefits don’t come just from the NGFW’s single-pass architecture. To protect all of the areas where security risks can arise, the platform includes technologies to capture, analyze, share and leverage intelligence on potential threats.

This threat intelligence, along with the platform’s distributed system and device management components, helps
to reduce the potential attack surface and prevent threats across the organization. Unlike traditional approaches that focus on reactive responses and remediation, the platform protects every part of the organization's global footprint, proactively detecting and blocking unauthorized apps and threats across endpoints, mobile devices, data center servers, and in the cloud.

Supporting components in Palo Alto Networks Next-Generation Security Platform include:

- **NGFW** – based on the integrated, single-pass architecture previously discussed, Palo Alto Networks Next-Generation Firewall provides visibility and enforcement across all on-premises locations, as well as cloud locations via a combination of physical and virtual form factors.

- **WildFire™** – the industry's largest network sandboxing service for rapid cloud-based malware analysis, providing visibility into unknown threats (e.g., files, URLs) within all traffic – WildFire allows the platform to recognize and stop attacks for all customers using the service.

- **Aperture** – advanced, sanctioned SaaS cloud application support and threat prevention, allowing for security postures that include off-premises SaaS apps.

- **Panorama™** – simple at-scale network security management for operational efficiency.

- **GlobalProtect™** – for secure endpoint communication (both mobile and on-premises), posture, and policy enforcement in conjunction with the next-generation firewall.

- **Traps™** – advanced endpoint protection, using a highly scalable, lightweight, device-based agent that prevents exploits from being leveraged by malware (including unknown zero-day vulnerabilities).

- **AutoFocus™** – providing the intelligence, analytics, and context on threats that help to distinguish commodity threats from highly targeted unique ones requiring an immediate response. AutoFocus uses cloud-based intelligence from WildFire as well as a variety of other sources.

**Platform Use Case – Controlling SaaS File Access**

To illustrate how the integrated design of the Palo Alto Networks Next-Generation Security Platform supports security enforcement in a distributed environment, we can look at an increasingly common use case. SaaS apps used for file synchronization and cloud storage, such as Box, have been widely adopted by consumers to store and share both personal and work files. Versions of these services have then been customized and enhanced for corporate deployments, relying on the same web infrastructure and protocols as the personal versions.

The organization wants to roll out the corporate version of the Box app for secure storage and sharing of work files while still allowing users to access their own files in the personal version of Box. To facilitate these information sharing policies, while also controlling the loss of the organization's data and preventing malware infections, security policies need to be enforced to:

1. Allow the sanctioned corporate version of the Box SaaS app to both upload and download files, facilitating legitimate information sharing between employees.

![Figure 6: Controlling SaaS web app file access](image-url)
2. **Allow the personal version of the Box SaaS app to only download files** and block uploading of corporate data to personal accounts. Permitting employees to download files from the personal version of Box allows them to access content shared to their personal Box account by outside vendors.

3. **Block use of unsanctioned and potentially dangerous SaaS apps** to prevent possible malware infections and loss of data.

The next-generation firewall elements of the platform provide the ability to control the file transfer policies desired in this use case. Policies can be set for specific SaaS apps, such as corporate versus personal versions of Box, enforcing security policies based on the direction of transfer, file type, user and other context.

In addition to the control described, the Aperture element of the platform provides the detailed content inspection and analysis of data shared in corporate Box accounts (via integration with Box APIs). With this capability, sensitive data that is transferred to Box can be monitored. This includes the monitoring and enforcement of appropriate sharing privileges for the data.

Files can also be transferred to the WildFire threat analysis service, if they are unknown, to help prevent malware infections from being spread via Box file sharing. Note that these Aperture capabilities augment the control capabilities of the NGFW. Aperture can also provide protection for corporate Box usage even when the service is accessed independent of the organization’s network (and therefore not subject to NGFW enforcement).

The comprehensive security policies supported by security platform’s integrated architecture enable you to control the usage of SaaS apps (including the movement of data) without impeding employee productivity or needlessly restricting choice.

**Summary**

IT faces a growing set of security challenges as applications, along with their supporting infrastructures, continue to evolve. Cyberattacks have become increasingly sophisticated, often unfolding in multiple stages starting with intelligence gathering and culminating in costly data thefts.

Historically, security architectures have evolved from a layering of multiple point products, with each targeting a separate threat approach, requiring traffic to be analyzed in multiple sequential steps. This layered approach to security lacks a unifying architecture and is unable to support the flexible security policies needed as apps and IT infrastructures evolve.

In contrast, integrated security architectures, such as the single-pass architecture, were designed to first develop full context from all traffic and then enforce comprehensive security policies based on that context, allowing both known and unknown threats to be detected and addressed.

**Palo Alto Networks Next-Generation Security Platform** has continued to extend the integrated architecture approach to up-level both visibility and enforcement capabilities across the distributed organization. The platform offers a unique, prevention-oriented approach to securing organizations, enabling the deployment of increasingly capable applications and IT architectures at an acceptable level of risk.

Learn more about why architecture matters at go.paloaltonetworks.com/architecture or go.paloaltonetworks.com/platform.