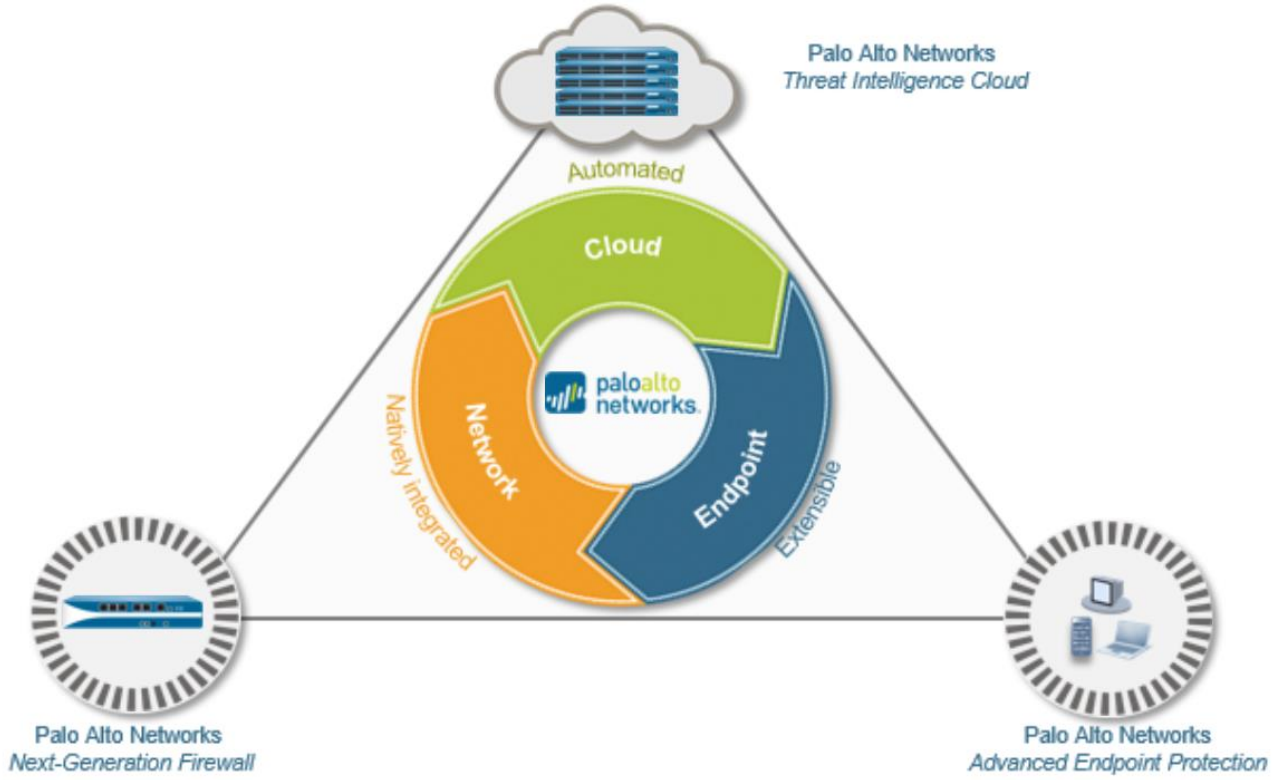
# Modern Prevention to Disrupt the Cyber Attack Chain

***(The Case for a Purpose-Built Enterprise Security Platform)***




By Palo Alto Networks

## Table of Contents





**Palo Alto Networks** 4401 Great America Parkway Santa Clara, CA 95054 **Main:** 408.753.4000 **Sales:** 866.320.4788 **Fax:** 408.753.4001 **paloaltonetworks.com**

## Preamble

Palo Alto Networks created a purpose-built platform from the ground-up to assure quality IT services and include unmatched protection. Our teams succeeded in delivering a vision that helps organizations get control of evolving networks to protect critical assets. The discussions in this document are a reality, not hypothetical. The paper explains problems with existing cyber security culture and approaches. Then, the paper introduces modern approaches that create transformational pivots to make prevention, action and control organic and fundamental to an enterprise security strategy. The disruption introduced through our technology reinvigorates a responsibility to innovate and achieve the Confidentiality, Integrity and Availability expected for operating interconnected systems.

Because of our innovation and hard work, Palo Alto Networks is the fastest growing cyber security company in history. Our Enterprise Security Platform provides superior capabilities for visualization, protection and control of all network traffic, applications, users and endpoints – this includes shared commercial data centers and mobile devices. In addition, Palo Alto Networks customer support exceeds industry averages, maintaining 9 out of 10 customer satisfaction ratings consistently. With more than 19,000 customers in over 120 countries across multiple industries, more than 75 of the Fortune 100 and the most advanced governments and militaries rely on Palo Alto Networks to improve their cyber security posture. We help organizations make prevention a champion and vital part of their security and protection strategy. Over 4,000 customers and growing rely on Palo Alto Networks for their Advanced Threat protection.

## Prevention and Resiliency Challenge

Effective cyber defense must withstand changes to adversary tactics and tools that traditional non-integrated "best of breed" approaches cannot address. It must address advanced unknown threats as well as known threats. Resiliency and defense across the Cyber Attack Chain comes from protecting and defending systems at all places in the network, across all network traffic on endpoints, in data centers, in remote locations and at major Internet gateways.

To improve prevention and resilience, it is important to:

- Prevent new attacks and automatically block follow-on attacks.
- Provide physical and virtual devices that are agile and scalable enough to integrate with and protect data at all locations on the enterprise: data centers, mobile devices, internet gateways, internal networks and endpoints.
- Automatically control and block unwanted applications and activity everywhere on the enterprise.
- Create cohesion between IT, cyber security and intelligence professionals to coordinate actions on the enterprise.
- Prevent the ability for attackers to use known tactics to attack an enterprise.
- Ensure Immediate and automatic sharing and distribution of intelligence signatures across the globe.

## Problems with Existing Legacy Approaches

The reactive nature of cyber security culture and approaches continues to impede our ability to prevent attacks. If we take a little time to discuss cyber security culture, we realize that the emphasis is overwhelmingly on detection and response. Unfortunately, the culture and emphasis inhibits prevention innovation and fails to address problems we can solve to prevent attacks. Instead, the culture leads to the idea of a security gap.



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

This section discusses the problems with current practices from a prevention perspective. The hope is to create a more meaningful discussion around prevention as a counter to the reactive detect and respond discussion that currently dominates the IT and cyber security community. As we walk through each problem, keep in mind that IT operations and defense are two sides of the same coin. Any gaps in protection evolved from segmenting IT operations and defense the way the industry does today. A modern prevention approach enables IT systems to maintain business continuity and provide prevention at the same time.

## Legacy Port Based Security Practices

If you look at every successful and major attack, you will see that the compromised organization used port based firewalls for security at their perimeter. Port based firewalls are no longer effective for protecting an organization or controlling applications and users. It is important for IT leaders and practitioners to change their practice from relying on port based security. It does not work. This is common knowledge in the cyber security community and we must have a discussion around evolving beyond this practice and changing architecture design.

## Proliferation of Advanced Tactics to Average Attackers

One of the most prominent and advanced threats to critical networks is delivery and execution of malware against unprotected known and unknown vulnerabilities. The adversary has effectively utilized technology and enhanced their ability to create and deliver highly effective unknown or zero-day malware that can disrupt business continuity and increase risk. Unfortunately, the enemy's ability to create tactics and disseminate them outpaces the cyber security community's ability to mitigate the tactics. As a result, average attackers have the ability to easily access controlled networks. This problem creates confusion around what is an advanced attack or a less sophisticated attack that used an advanced tactic to gain initial access. A contribution to the confusion comes from the cyber security community's reliance on logging to identify advanced tactics. The reliance on logs creates unsustainable manual effort as new IT technologies become required to support business needs. As a result, the proliferation of known advanced tactics provides attackers an overwhelming advantage against an organization. We must eliminate the ability for attackers to use known advanced tactics to gain enterprise access.

## Limited Visibility and Control of all Applications, Users and Network Traffic

A cardinal rule in defending an enterprise includes knowing everything happening on the enterprise at all times. This enables an organization to provide robust IT service and availability for authorized activity while eliminating unauthorized activity. Today, limited visibility and control of all activity by applications and users creates significant challenges for IT and cyber security professionals. Without full visibility and control, all traffic and activity is treated the same. As a result, cyber security professionals are unable to discern authorized activity from unauthorized activity.

Most architectures today resemble what you see in **Figure 1**. They consist of silo vendor appliances, processes, and infrastructure assembled like a best-of-breed manufacturing production line. The IT operations and defense professionals take logs from events that roll down the production line of individual non-integrated point products. The IT operations and defense team members perform their individual duties and spend time when possible to try and makes sense of all these logged events. This is ineffective from a prevention perspective for three reasons:

1. **Limited visibility**:
   You cannot secure what you cannot see. Your IT and security architecture must be fully integrated to provide the ability to **see all applications, users and the individual devices operating on the network** at all times. Full visibility at all times is the first step to prevent attacks that might utilize non-standard ports, protocols, or SSL encryption for evasion. Your IT and security architecture must



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

have the ability to see and prevent new targeted attacks that are utilizing threats (unknown malware and zero day vulnerability exploits) that have never been seen before. Current best of breed approaches are unable to provide full visibility of everything happening on your enterprise. As a result, blind spots litter enterprises and increase the attack surface. **Full visibility and control is required to eliminate all blind spots.**

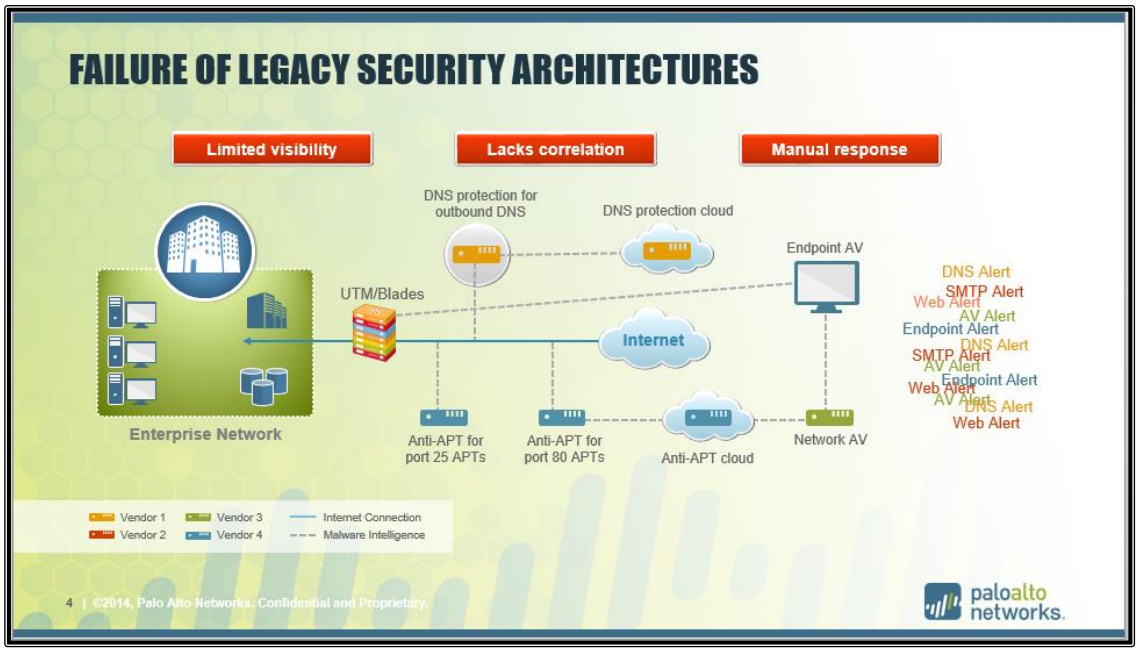



*Figure 1: Failure of Existing Cyber Security Legacy Approaches*

2. **Lacks correlation**:
   The IT operations and defense teams today lack the ability to defend against multi-dimensional attacks. The primary reason is the lack of correlation between IT and cyber security events on the enterprise. Correlation techniques continue to require too much overhead without protecting or preventing unwanted activity or attacks. To improve, architecture **must act like a system of systems** where integrated technologies work together in a coordinated manner to prevent attacks. In this way, correlation makes each element within the system of systems smarter providing the ability to make immediate decisions about whether activity is malicious, authorized, or unwanted.
3. **Manual response**:
   Attacks and business technologies continue to evolve at a rapid pace. Yet, the approaches to security fail to keep up. As a result, existing efforts are overly manual, and rely on unsustainable manual response processes to protect mainstream and leading edge business technologies required for growth. Your security architecture must employ **automation that is constantly learning and applying new defenses** without a need for manual intervention. It must **weed out the congestion**, automatically preventing unwanted, suspicious and unknown activity. The automation is required to ensure your teams can focus on performing in-depth analysis to oversee a controlled and protected environment.

It is time to evolve beyond the limited visibility and control holding back IT operations and security professionals. We must provide the ability to immediately control authorized versus unauthorized activity everywhere the enterprise exists at all times.



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

### Limited Threat Vector Coverage

Many commercial companies created point-product tools that can detect and determine if a file or an executable is actually malware, but these tools have limited ability to stop the malware. This is also true for malicious activity that indicates attacker tactics. As a result, attackers maintain a significant advantage with a combination of unknown malware and tactics. Ultimately, targets receive malware despite detection. This creates a high level of burden for cyber security and incident response personnel to investigate compromises and lateral movement.

The current approach is unmanageable, continues to fail and leads to dangerous dwell time advantages for adversaries. Prevention requires the ability to prevent attacks across all threat vectors, not just a handful. Organization leaders need to understand that deploying detection across a few threat vectors, such as web traffic or e-mail, based on legacy port-based technology fails to reduce risk. At most, the practice provides limited protection across a handful of threat vectors. To make prevention relevant in an enterprise, companies must reduce their attack surface and implement protection across all threat vectors.

### Complex Non-Integrated Systems and Manual Burden for Professionals

The cyber security community spends considerable resources and energy segmenting technologies in a "quadrant" or "best of breed" category. Although this practice intends to help differentiate technologies, it leads to serious segmentation of cyber security systems and continued isolation from IT operations. The result creates an overwhelming manual burden for IT and cyber security professionals. The most talented IT and cybersecurity professionals spend most of their time trying to integrate segmented technologies rather than analyzing unwanted and malicious activity. Over the years, this manual burden and segmentation took a front seat to prevention innovation and helped create the excuse of a "security gap". The cyber security community fueled the excuse by a continued reliance on legacy security technologies that did not keep up with evolving IT technologies.

To complicate problems, the bulk of cyber security effort is on detect, respond and remediation practices that remain unable to prevent attacks or reduce the ability for attackers to access enterprises. While some detect and remediate technologies can detect zero-day malware, they require a significant human resource investment and multiple non-integrated appliances positioned at edge, data center and internal traffic locations. This approach makes scalability very difficult and very expensive with limited reduction in an enterprise's attack surface. The approach creates coverage gaps inherent to network and endpoint appliance silos that create blind spots on the enterprise. In addition, the approach lacks the ability to defeat vulnerability exploitation. The detect and remediate technologies only detect zero-days without automatically preventing the attacks. The adversary will attack with new unknown malware, and will do significant damage in a very short period, sometimes less than 24 hours. Existing detect and remediate methodologies fall well short of covering all threat vectors and increase risk to business continuity and growth.

These problems are systemic throughout the IT and cyber security industry. The problems create overwhelming risk for organizations and countries that we must address. In the next section, the paper explains how Palo Alto Networks delivers a modern approach to solve these problems. It clarifies the modern prevention approach we created through our innovation and determination to be relevant to business enablement and growth.

## Prevention Delivered through a Modern Approach

Palo Alto Networks delivers a novel way to address each of the problems identified in the earlier section. To set the stage, we want to make a few observations about cyber security culture. Historically, we place a



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

cyber security technology or product in a "quadrant" to differentiate "best of breed", but let's reflect on this practice with some questions.

- Is the concept of a "security gap" real or a myth? No doubt, there will always be some sort of security gap based on the speed of evolving technology. However, this gap is small and not as large as many respond and remediate technology companies explain in the market. Any gap that exists for mainstream established technology is an excuse for a lack of innovation. That is, the company or technology is unable to prevent the attack – thus, a security gap.

- Is "best of breed" a good practice from a prevention perspective? Prevention is, and always has been, a significant part of protecting an enterprise. Yet, most "best of breed" offerings deal with reactive detect and response technologies that have limited prevention aspects. They may prevent a limited number of attacks, but they leave a significant attack surface after installation. Thus, companies have to choose what types of attacks they will try to prevent. In the end, it becomes an overwhelming practice in manual integration. The most talented team members spend the bulk of their time trying to make non-integrated technologies work together while the attacker is maneuvering around them using unprotected threat vectors.

- Is it "best practice" to separate IT operations from defense? We know today that IT operations and defense cohesion is critical to protecting an enterprise and preventing attacks. In addition, we realize that separation tends to lean toward compliance confirmation rather than preventing attacks and providing protection on the enterprise. We must do a better job of building cohesion between IT and defense operations.

The three reflections are some core reasons that the cyber security culture fails to prevent attacks. At Palo Alto Networks, our innovation and hard work is changing these cultural reflections for the better. We delivered on a vision to create better cohesion between IT and cyber security professionals so prevention is an embedded component of an enterprise architecture. As a result, the idea of a security gap is a myth for established mainstream technologies. We evolved beyond reactive "best of breed" approaches and provided an entirely new way for IT and cyber security professionals to defend their enterprises from attacks.

Prevention is relevant to protection and business growth, Palo Alto Networks makes prevention a reality by solving problems and enabling organizations to adopt emerging technologies securely at reduced risk. The rest of this section is dedicated to discuss how we solved the problems explained earlier in this paper.

## Decode All Traffic Regardless of Port, Including SSL

We moved beyond legacy port-based security practices by creating a technological approach that decodes all network traffic everywhere our enterprise security platform devices exist in the network. The approach transformed the cyber security industry and provided customers full visibility into all their network traffic. To achieve this required and entirely new definition and approach to decoding network traffic. Our engineers used extreme creativeness to introduce a modern means to decode all ingress and egress traffic. In addition, we ensured this was standard on every appliance and virtual system out of the box.

When you see a box sitting in an internal position on your enterprise, or in your data center, or on an internet access point, you will see a machine decoding all traffic independent of port. This is a significant differentiator in how we operate and fundamental reason that we continue to disrupt the cyber security industry. We are modern.



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

Peel back the onion of any of our physical or virtual appliances and you will find the same thing. There is no legacy port-based security technology found. Instead, over 150 decoders working in synchronized fashion as part of what we call a single pass architecture to identify, control and protect applications, users and content. Welcome to the future of IT operations and defense. Palo Alto Networks achieved something completely new in traffic that redefines what it means to control and protect network traffic everywhere an enterprise exists in the world.

## Eliminate Average Attackers' Success with Advanced Tactics

Not all attackers are equal. Unfortunately, all attackers have access to advanced tactics that give them a significant advantage against IT operations and defense teams. Detect and respond organizations are unable to prevent average attackers since they have limited visibility and protection across all threat vectors. As a result, they place their emphasis on unsustainable manual and complex approaches to detect average attackers and then respond after the event occurred. That is, if the event received the right level of priority and was not lost in the inundation of alerts. The Palo Alto Networks approach to prevention takes ground back from average attackers that use known tactics created by advanced attackers. We do this through our unique control, visibility and protection for all network traffic, everywhere in the enterprise.

**Figure 2** shows the modern extensibility our purpose-built prevention platform and approach brings to the IT operations and defense scene. From left to right, you see all the locations our modern and unique design controls out of the box. You do not need multiple blades or bolt on parts to control and protect the enterprise. Since all of our devices are the same except throughput size, we decode all traffic everywhere. Thus, we automatically eliminate unwanted activity while allowing wanted activity supporting business. As a result, advanced attack techniques in the hands of average attackers lose their power and get defeated. This reduces your attack surface and introduces automated prevention throughout your enterprise. In addition, extensibility enables your organization to focus on growing business rather than reacting to an inundation of alerts.

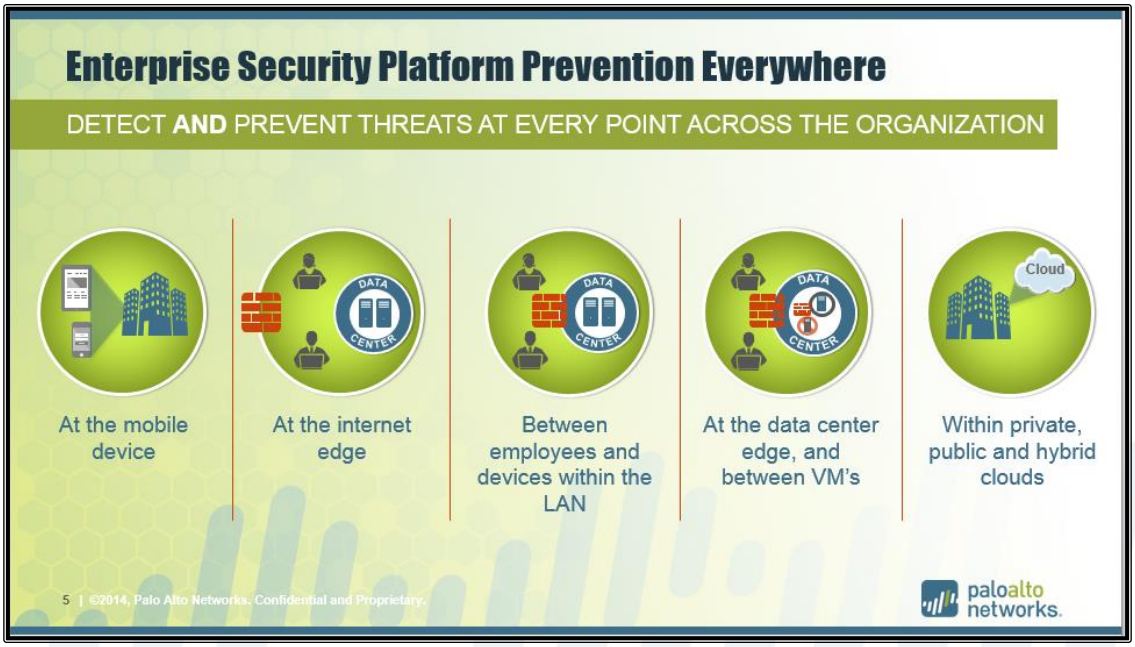



***Figure 2: Eliminate Average Attacker's from Using Advanced Tactics***

Our Enterprise Security Platform protects and controls users, applications and activity everywhere in the enterprise, not just on the perimeter. As a result, attackers lose the advantage they currently have using proliferated known advanced tactics. We eliminated their ability to move freely in an enterprise after



**Palo Alto Networks** 4401 Great America Parkway Santa Clara, CA 95054 **Main:** 408.753.4000 **Sales:** 866.320.4788 **Fax:** 408.753.4001 **paloaltonetworks.com**

gaining access and credentials by controlling all activities on the network, everywhere the enterprise exists. This includes internet gateways, smartphones, tablets, laptops, servers, desktops, virtual machines, data centers, etc.

## Full Visibility and Control of All Applications, Users and Network Traffic

An additional advantage of decoding all ingress and egress data is the granular control you get for all applications, users and network traffic. Again, this is standard on every Palo Alto Networks physical and virtual appliance. The modern approach extends creative ways to operate and defend networks that we are only scratching the surface of today. Yet, we already see some tremendous advantages.

The Zero Trust model created by John Kindervag of Forrester Research provides a great way to explain of how our modern innovation achieves full visibility and control. The model continues to gain ground as a standard practice to prevent evolving modern threats and ease the burden of operations and defense costs.

There are three foundational concepts[1] of the Zero Trust model. The table below explains how our technology organically delivers the three concepts natively, out of the box:

| # | Concept Description | How Palo Alto Networks Delivers |
|---|---|---|
| 1 | Ensure that all resources are accessed securely regardless of location. | The granular visibility and control of applications and users that comes standard in all our physical and virtual appliances creates some interesting scalability to control access to resources securely from any location.<br><br>First, our technology controls all traffic and access to resources by user, not IP address. As a result, it doesn't matter what device or location a user connects from. They get access to the resources they need to perform their job.<br><br>Second, our appliances control all ingress and egress traffic using a fully integrated VPN created by our engineers. This ensures all traffic communicates securely no matter where they exist.<br><br>Third, the fully integrated VPN extends all threat prevention and cloud intelligence services to devices everywhere they exist or roam.<br><br>Fourth, not only do we control access to applications and resources by user, we control traffic access based on user. In addition, we provide the ability to create multiple virtual networks where specific users have access while others do not. This organic ability provides a new form of segmentation everywhere across the enterprise. It doesn't matter what IP a user accesses the enterprise from. Users only get access to resources and the portion of the enterprise required by their associated user group. This is very important and provides a new form of flexible secure access independent of location on the globe. |
| 2 | Adopt a least privilege strategy | Because we control all network traffic and application activity by user through full integration with authentication systems, we have the |

[1] John Kindervag, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security", September 14, 2010



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

| | | |
|---|---|---|
| | and strictly enforce access control. | organic ability to adopt least privilege and automatically enforce strict access control.<br><br>This extends to applications and resources for all users, everywhere. It is a native capability on all our appliances. In fact, the only difference between our physical and virtual appliances is throughput. So, the control extends everywhere across an enterprise at all times. |
| 3 | Inspect and log all traffic. | Because we decode all ingress and egress traffic, everywhere in the enterprise, we deep packet inspect all traffic everywhere one of our appliances exist.<br><br>If you point to a Palo Alto Networks device in your architecture, you don't have to look at the model number to confirm that all traffic is inspected. This aspect creates a tremendous ability to know everything happening on your enterprise at all times. In addition, if you don't know what an activity is, or you don't want an activity to happen, you can automatically deny the activity from traversing on the enterprise. The activity just won't go anywhere.<br><br>By the way, we log all traffic, application and user activity at all times. To help reduce complexity and improve automation, we developed a free Splunk application to consume our logs. All Palo Alto Networks Enterprise Security Platform physical and virtual appliances easily point to Splunk to eliminate the need for complicated log indexing and aggregation design and integration drills. |

***Table 1: Zero Trust Fundamental Components***

The Enterprise Security Platform's ability to cover all three Zero Trust fundamental concepts out of the box is novel. Seriously, can you think of anyone that can plug in their device and meet these three criteria organically when you connect the appliance? Interestingly, this modern aspect of our platform gives you the full visibility all users, applications and network traffic everywhere your enterprise exists on the globe.

## Full Threat Vector Coverage Everywhere (Network and Endpoint)

In today's overly complicated cyber security market, one thing is certain. If an attacker installs malicious evil on an endpoint you lose. You lose business continuity, business growth and valuable resources because your smart personnel are in a state of continuous response. In fact, in its existing state, cyber security is irrelevant to business growth or protection. Our Enterprise Security Platform changes everything, and makes prevention a fundamental component of your IT operations and defense strategy. There are two simple reasons for this:

1. The Enterprise Security Platform is purpose-built and integrated to provide full threat vector coverage everywhere on your enterprise.
2. The Enterprise Security Platform defeats attackers before they can exploit vulnerabilities on endpoints.



**Palo Alto Networks** 4401 Great America Parkway Santa Clara, CA 95054 **Main:** 408.753.4000 **Sales:** 866.320.4788 **Fax:** 408.753.4001 **paloaltonetworks.com**

To explain the two reasons, we will reflect on the Cyber Kill Chain®[2] and the Cyber Attack Chain[3]. Many IT and defense professionals use the two chains for post attack analysis. In our case, we want to use them for pre-attack full coverage of all threat vectors. It is not enough to keep attackers out, you also have to control the applications, users and activity everywhere in the enterprise.

For this paper, we use the Cyber Attack Chain to focus on specific areas of attacks. However, we want to give a shout out to the Lockheed Martin team for their chain as well. If you want to learn more about the Lockheed Martin version, they provide a great description **here** on their website.

A closer look at the Cyber Attack Chain reveals six stages. Gartner introduced the model in a blog post **here**. The six stages include:

1. Delivery
2. Exploit and/or Install
3. Command and Control
4. Privileged Operations
5. Resource Access
6. Exfiltration

In this paper, we combine stages four and five to combine Privileged Operations and Resource Access together. **Figure 3** provides a representation of the stages. We organized the stages around the outside the diagram starting with Delivery and ending with Exfiltration. Lines on the drawing point in both directions to show all traffic in both directions and the multiple Palo Alto Networks devices shown in the diagram show the extensibility of inspecting full packets and decoding all traffic everywhere in the enterprise.

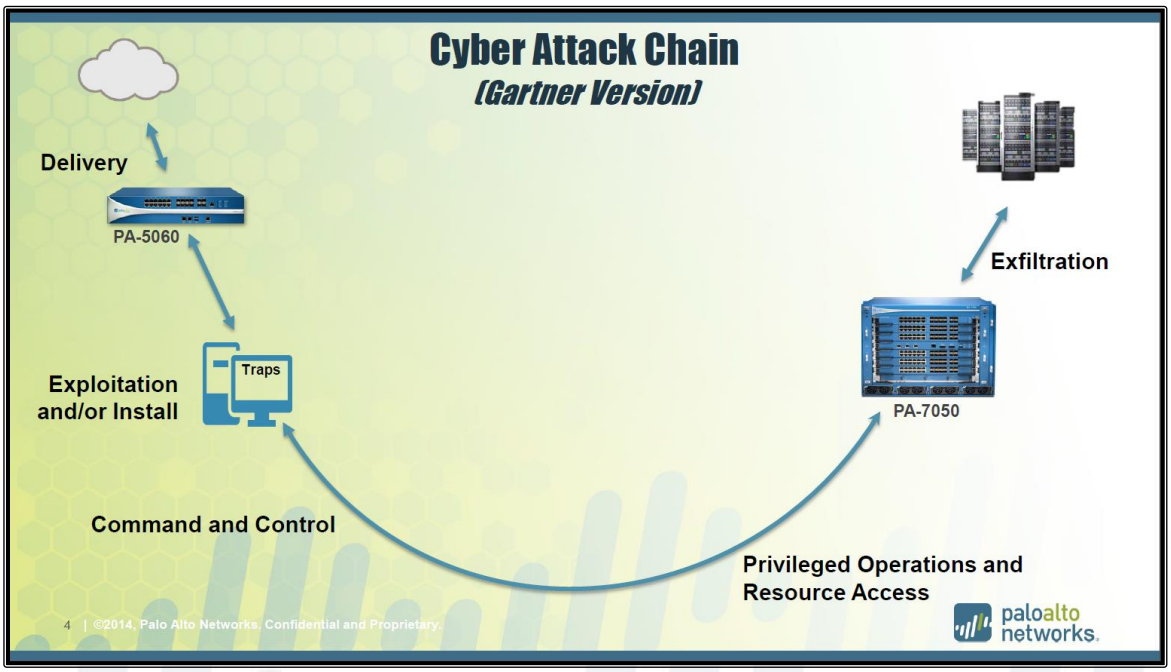



*Figure 3: Cyber Attack Chain*

[2] Lockheed Martin
[3] Gartner



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

As mentioned earlier, if an attacker or someone malicious gets to install (Stage 2), you lose. You missed the fight. Our platform keeps you ahead of the fight by defeating attackers before they can exploit a vulnerability and by controlling applications, users and content everywhere the enterprise exists. Defeating the exploit and controlling the enterprise is a powerful combination and fundamental to what drives our innovation as a company. We realize that stopping the attacker at exploitation takes significant ground back from attackers. We do this elegantly, without disrupting business continuity or introducing additional operational and security risk.

**Figure 4** shows the organic platform capabilities that protect the entire enterprise everywhere the enterprise extends or operates.

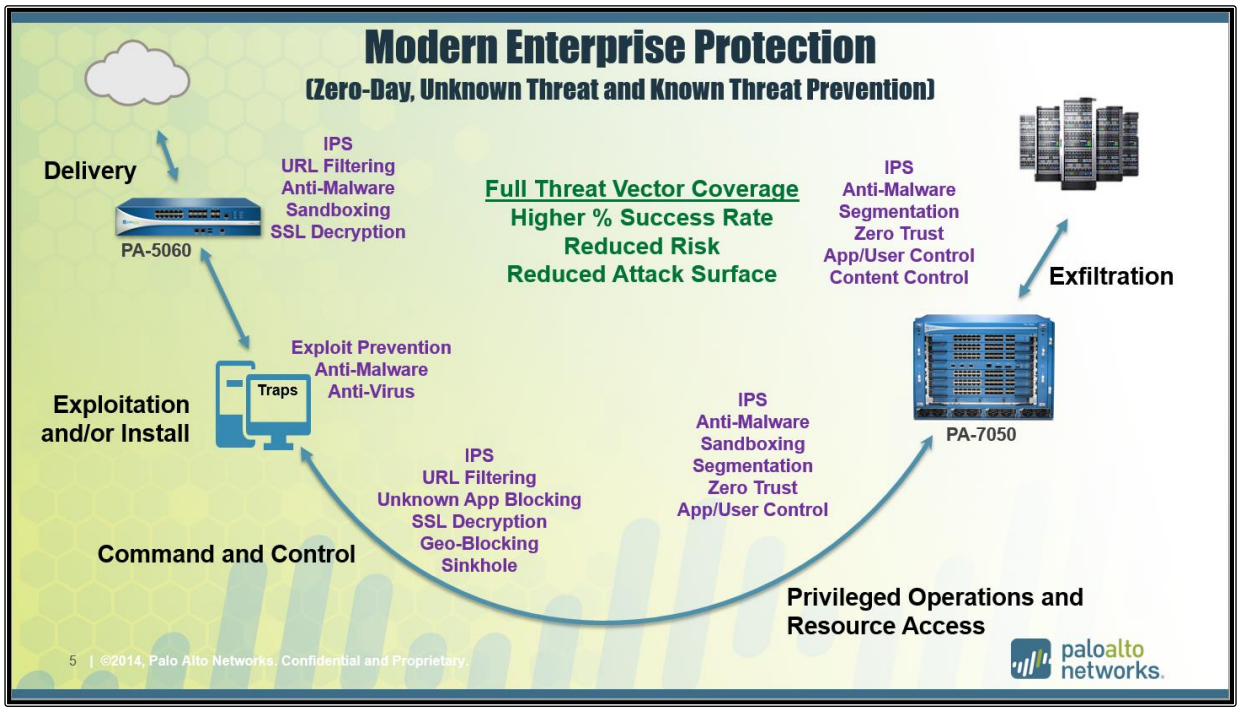



*Figure 4: Enterprise Security Platform Full Threat Vector Coverage*

Defeating attacks at every stage of the attack chain is important since attacks come in different forms and can arrive via multiple vectors including web, e-mail, and external storage. For instance, key in on Stage 2, Exploitation and/or Install. Most traditional endpoint security products protect endpoints from malicious executable files, which are the least sophisticated form of delivery. The most advanced and targeted attacks arrive in the form of seemingly harmless data files opened by legitimate applications. For example, attackers often implant malicious code in a Microsoft Word or PDF document. Once a user opens the file, the malicious code takes advantage of a vulnerability in the application, allowing it to execute code and take full control of the endpoint.

Our platform protects endpoints by preventing exploitation of vulnerabilities and install, both malware in the form of executables and in the form of data files. This is one clear example of how our purpose-built platform provides automated and integrated protection across the full threat spectrum. Our approach is both modern and novel to prevent attacks against organizations. We do not give attackers the opportunity to install malicious code on the endpoint and our integrated capabilities protect across every stage of the attack chain for additional preventative measures.



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

This is a significant difference from best-of-breed practices and bolt-on approaches that encompass the reactive detect and respond cybersecurity community today. Point products lack the ability to protect organizations against all threat vectors. As a result, point products have the ability to detect malicious files or activity, but lack the ability to prevent malicious compromise immediately. In addition, point products are unable to defeat attackers at the exploitation stage. As a result, IT operations and defense teams have a significant dis-advantage against all threats, including advanced threats. The way we provide full threat vector coverage is an entirely new approach capable of protecting organizations from evolving threats.

Inside the line on **Figure 4**, you see the protection capabilities integrated within platform devices and endpoint agents. As an adversary attacks a target, our platform uses the integrated capabilities to deny the attacker access or movement at every stage of the attack. This approach raises the bar for prevention since it provides the only fully integrated system of systems environment that is purpose-built to prevent attackers' access to an enterprise. Our modern approach to prevention directly combats the ability for an adversary to gain a foothold and maintain persistence. In addition, it reduces the overall attack surface area on an enterprise.

Delivering prevention and control capabilities at every stage of the attack chain through our Enterprise Security Platform reduces complexity, the attack surface and risk. Covering all threat vectors with one integrated platform automates prevention and control. It inherently improves prevention and protection against attackers. In addition, the integrated platform limits the impact of vulnerabilities that exist across the enterprise. In this way, the manual burden of risk mitigation because unpatched systems are required to support business continuity is no longer an issue.

Prevention now takes a center stage to business continuity, enabling growth and protecting organizations. Welcome to the 21st century, things are moving fast. Our innovation, passion and drive deliver on a prevention vision by fielding capabilities across all stages of the attack chain to provide full threat vector coverage. This is how we defeat Zero-Day, Known and Unknown attacks.

## Fully Automated and Integrated Network, Intelligence and Endpoint Protection

In the previous section, we mentioned that the Enterprise Security Platform is a system-of-systems. This is an added advantage since the Enterprise Security Platform is purpose built and fully integrated. At each stage, the protection not only achieves full threat coverage through extensibility, it also introduces novel automation.

**Figure 5** helps highlight how the system of systems integration automates prevention and control on an enterprise. Building on the previous figure, a triangle in the middle shows the three main components of our platform. They include, **Next-Generation Firewall**, **Advanced Endpoint Protection**, **and Threat Intelligence Cloud**. The line between each component indicates that these systems are all purpose-built to perform control and prevention purposes in an extensible manner throughout the enterprise.

Our engineers designed the three components to extend the capabilities that cover each stage of the attack chain. Here is a description of each.

**Next Generation Firewall:**
The Next-Generation Firewall is responsible for executing the capabilities in all network traffic everywhere the enterprise exists. This includes all network traffic going to and from mobile smart devices or laptops. Everywhere network traffic exists, our control and protection holds because of the extensible nature of the design. In fact, the only difference between our low-end



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

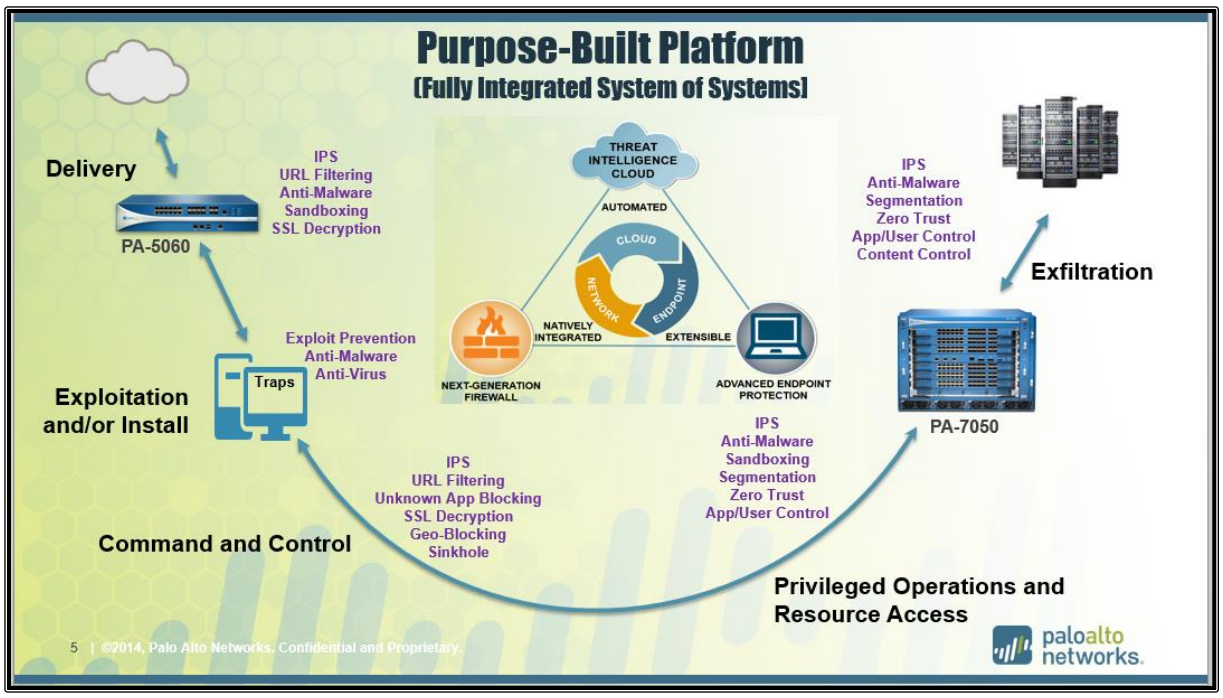



***Figure 5: Integrated Purpose-Built Platform***

and high-end models is the throughput. We build the appliances on the same operating system to control and protect enterprises natively with no additional blades or hardware. In addition, we virtualized everything so it scales everywhere. It is the Next-Generation Firewall that provides an unprecedented vantage point across all network traffic to control and protection all applications, users and content at all times

**Advanced Endpoint Protection:**
The Advance Endpoint Protection provides unprecedented protection of endpoints. The exploit prevention it introduces takes ground back from attackers. Even if an endpoint is unpatched, the exploitation prevention holds. It removes the attackers' ability to access enterprises with proliferated advanced tactics that best of breed and point products cannot prevent. This is the key to defeating attackers before they install malicious code on a system with known or unknown malware. Do not let attackers take advantage of known and unknown vulnerabilities.

**Threat Intelligence Cloud:**
The Threat Intelligence Cloud provides an unprecedented over watch for all our customers across the globe. All deployed platform devices automatically push suspicious file artifacts from any location on all customer enterprises. The Threat Intelligence Cloud detonates these file artifacts to determine malicious and gather threat indicators. At the same time, it automatically converts the intelligence indicators to signatures and deploys them to all platform devices in network traffic and agents on endpoints. This process is really fast and getting faster all the time. Today, we gather the intelligence indicators for file artifacts in 5 minutes and deploy signatures across the globe within 15 minutes.

Together, the three platform components change the game for prevention and protection of global enterprises. Just imagine the tight automation gained from our agent defeating an unknown piece of malicious malware on a user's endpoint. At the same time, we extracted the malicious malware from network traffic and detonated it in the cloud for automated signature dissemination in 15 minutes. Keep in

mind; this happens no matter what port or application the attacker used as a threat vector. Your IT operations and defense professionals gain essential time, automation and efficiency. Your company reduces the attack surface, reduces risk, gains protection and makes prevention relevant to growing your business.

The **Appendix**: The Enterprise Security Platform provided at the end of this paper provides a full description of the Enterprise Security Platform technologies. In the next section, we will discuss the platform's impact on Global operations.

## Global Enterprise Prevention – IT Operations and Defense Cohesion

The Palo Alto Networks Enterprise Security Platform provides transformational pivots to lead the way defeating adversaries at every attack stage. **Figure 6** introduces a visual of how a true purpose-built and integrated platform changes the game for global IT operations and defense professionals. As the emphasis of the diagram shows, there are four operational pivots introduced when our prevention approach disrupts the Cyber Attack Chain. All four of the pivot transformations overlap in a way that is consistent with covering threat vectors. This overlapping of operational pivots along with capabilities identified in the last section bolster the platform's ability to defeat Privileged Operations and Resource Access. Our approach provides defenders an advantage to extend vigilance and prevention everywhere to defeat attackers.

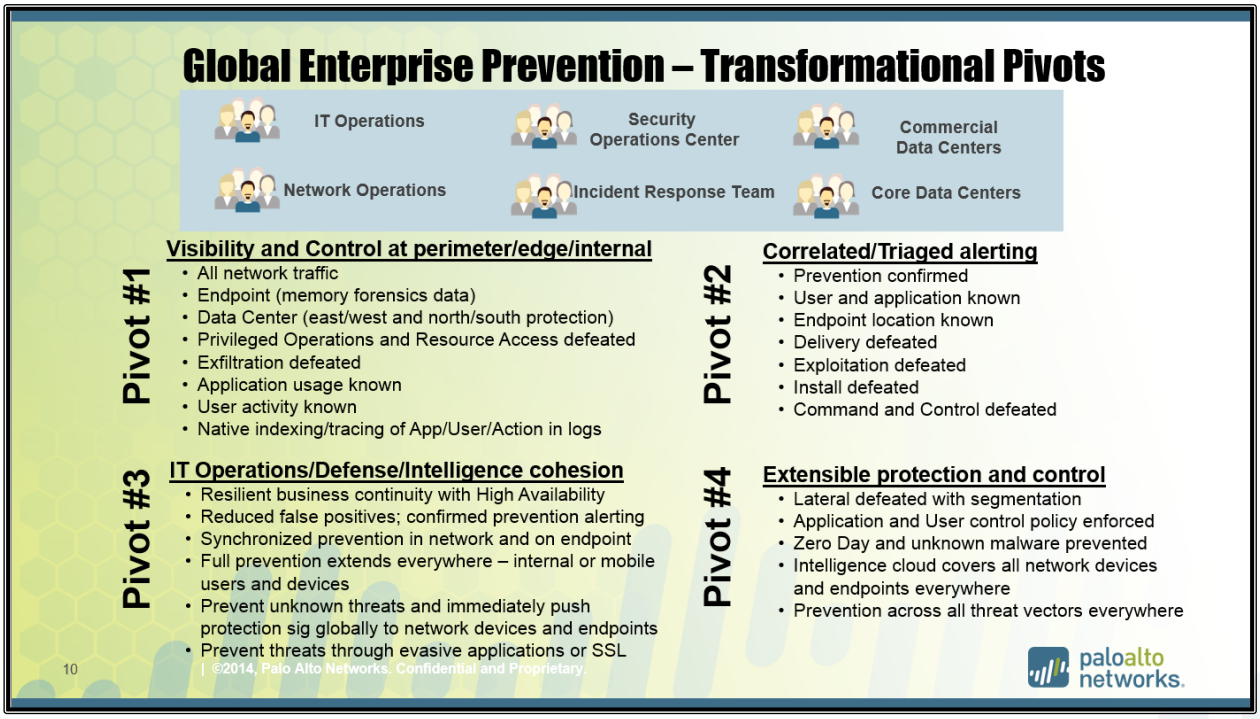



***Figure 6: Global Enterprise Prevention***

The integrated capabilities that protect organization against all threat vectors grow cohesion between global IT, defense and intelligence professionals. It is not enough to detect the adversary at different points in the Attack Chain, you must take action to prevent aggression and disseminate intelligence signatures immediately to protect the entire enterprise.

### Pivot #1: Visibility and Control at the perimeter, subscriber edge and internal enterprises

We mentioned earlier that maintaining visibility across the entire environment is a fundamental aspect of any enterprise security strategy. Limited visibility allows adversaries to take advantage of blind spots. From



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

a prevention perspective, there are no blind spots in enterprise. You control all users, applications and content no matter where they operate on the enterprise. If an action is not desired or authorized based on policy, it does not happen. Instead, the platform immediately isolates the unwanted activity from traversing the network, and sends and alert to the IT and defense team.

Best of breed approaches with limited visibility across the enterprise currently rely on correlation of massive amounts of logs to identify unwanted activity. This a reactive stance that happens after the activity takes place without taking immediate action to isolate the activity. The IT operations and defense professionals lose critical time chasing the activity to determine what they stole from the enterprise. This creates frustration for defenders and leadership since they must wait days to get answers about what is happening on the enterprise. We have a better way.

Our modern approach introduces some create ways to control unwanted activity. The flexibility of virtual and physical platform devices provides a scalable means to control all user, content and application activity continuously. If you see a user behaving badly, simply move the user into a pre-built isolation segment on the enterprise. Automatically block unauthorized applications anywhere on the enterprise. This keeps users from intentional or unintentional harm while you reach out to understand the activity. This active isolation approach for users and applications stems from the platform's granular control and visibility of all activities on the enterprise.

The inclusion of an integrated platform endpoint agent provides you full control and protection all the way to the endpoint. Such control and protection allows operators to drill-down focus on portions of the environment and immediately determine that the platform has prevented an attack. This drastically reduces the manual burden that exists today and improves efficiency of operating and defending the enterprise. It also plays a significant role in defeating unwanted **Privileged Operations and Resource Access** attack stage activities. It also plays a significant role in defeating **Exfiltration** since all devices and agents receive the latest intelligence from the global threat intelligence cloud converting and disseminating the prevention signatures across the globe.

In addition, the native platform plays a critical role in traceability of users, application and content activity with log events. Activity log indexing activity happens organically and reduces the need for the manual integration of overwhelming logs that exists with best of breed appliances. Your professionals get to spend more time defending the organization than forcing integration of disparate systems.

## Pivot #2: Correlated and triaged alerting

The need to spend precious resources sifting through and correlating logs from multiple appliances created a daunting dilemma for network operations and defense professionals. Today, professionals spend more time trying to visualize data in overwhelming logs than performing analysis, intelligence and hunting activities required to defend the network.

Our platform always knows what actions a user is taking and the applications supporting their actions. As such, the platform immediately determines whether the action is within policy at the time of the act. When an action falls outside approved policies, the platform blocks the action immediately and reports on the prevention. For IT operations and defense professionals, this translates to:

- Saving significant time that is essential to support business operations and reduce risk.
- Synchronized prevention in the network and on endpoints.
- Enabling planners to think in terms of architecture, mission continuity, team cohesion, scalability, security and protection.



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

- Modernizing legacy technology silo approaches for network operations and defense.

When time is fleeting during an incident, network operations and defense professionals need to know the user, location, OS, type of device, etc. immediately. Our integrated and purpose-built platform goes beyond this detect and respond framework. The platform provides this critical information to all operators immediately and confirms the prevention. Again, we defeat the attackers before they exploit a vulnerability and provide operators continuous and full control of all users and applications on the enterprise. In this fashion, the IT operations and defense teams gain outstanding control and ability to act. With automated help from the platform, teams actively prevent delivery, exploit, install and C2 to defeat attackers before they gain access and persistence in the environment.

## Pivot #3: IT operations, defense and intelligence cohesion

We continue to learn and understand guiding principles to operate and defend the contested domain of cyber. It is a young domain, and we now realize that IT operations, defense and intelligence cohesion is an essential transformation pivot. As smart devices and evasive applications increase in number, operational cohesion will allow operators to maintain mission assurance and protection.

We can achieve mission assurance and high availability through cohesion – the Enterprise Security Platform from Palo Alto Networks provides a new approach. The integrated architecture provided through the platform ensures cohesion and prevention as the enterprise expands or contracts based on business needs. This is critical when business operations change based on market and industry demands. Ultimately, the platform provides cohesion and prevention as a stable foundation in environments that require constant change.

## Pivot #4: Extensible protection and control

Lateral movement continues to create havoc for network operations and defense professionals. The reactive nature of legacy approaches makes combating lateral movement reactive and ineffective. The dwell time afforded to advanced attackers in enterprises allows them to maintain persistence and effectively cloak their activities. A platform approach changes this dynamic by extending prevention and control to every location on the enterprise.

The prevention scales to every location on an enterprise, and the control enables customers to use any application required to perform business function. As such, the platform reduces the attack surface on an enterprise and enforces governing polices everywhere.

In addition, the native zero-trust includes segmentation that eliminates blind spots where attackers achieve persistence and dwell. Extensible protection ensures the threat prevention, protection and control covers all enterprises, all network traffic, all endpoints, all data centers and all mobility devices.

***Our Enterprise Security Platform is modern and delivers the innovative pivots that change the game for protecting an enterprise. The capabilities we include natively on all platform devices provide IT Operations and Defense teams' superior visibility, control and protection. Our platform lives up to the responsibility to provide Confidentiality, Integrity and Availability on global enterprises.***



**Palo Alto Networks** 4401 Great America Parkway Santa Clara, CA 95054 **Main:** 408.753.4000 **Sales:** 866.320.4788 **Fax:** 408.753.4001 **paloaltonetworks.com**

## What Prevention Looks Like – superior protection with global reach

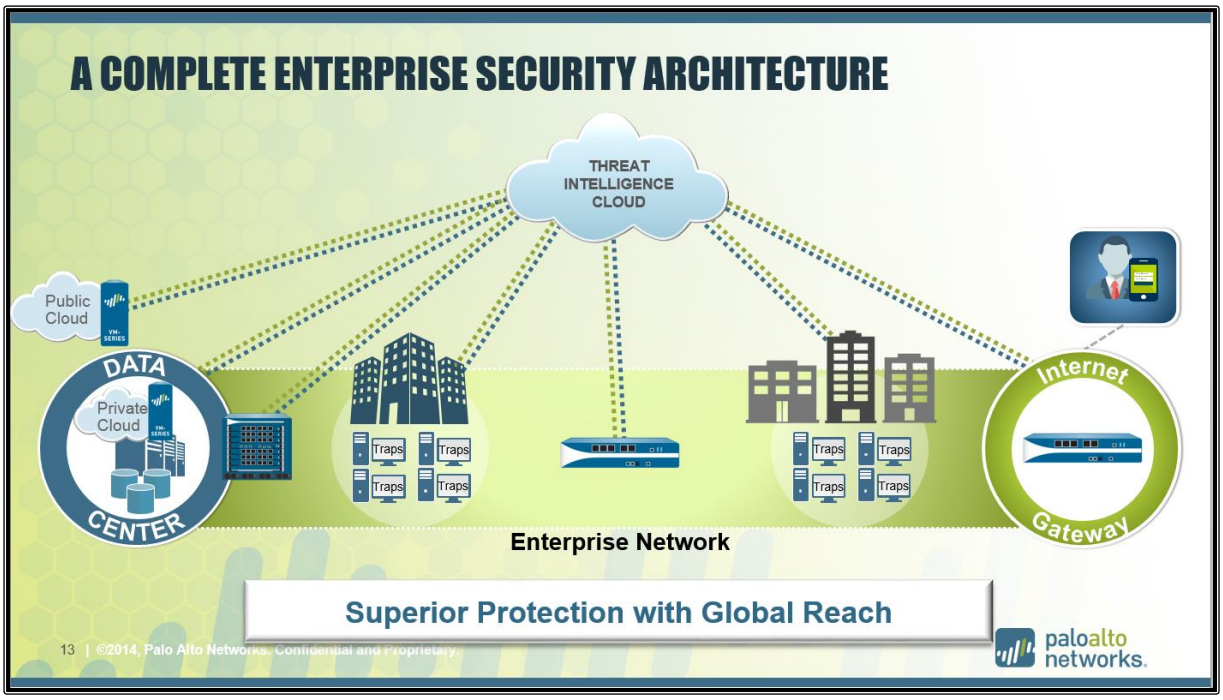



***Figure 7: Modern Prevention Approach***

The visual in **Figure 7** provides an extensible overall view of how the Palo Alto Networks Enterprise Security Platform changes the game for defending enterprises. Undoubtedly, the purpose-built and integrated platform provides novel prevention and a new approach for defense. Inherently, the platform modernizes the layered approach for cyber security and raises the bar for prevention. The visibility and control allows organizations to extend time sensitive intelligence for unknown threats while maintaining rigor and integrity to prevent known threats. As attackers escalate their actions to gain access, synchronized and cohesive operations counter their advance.

In **Figure 7**, all deployed Enterprise Security Platform devices and endpoint agents control applications, users and content to ensure mission continuity. This serves as an enabler for Business, IT and defense operations. At the same time, all devices and agents maintain real-time connections with a **Global Threat Intelligence Cloud** to push and pull the latest intelligence as attackers initiate offensive operations. ***Our initiative to provide platform devices in both physical and virtual options ensures flexibility and scalability needed for global reach.***

The power of our platform continues to disrupt the industry. When we fully integrated our technologies with innovative partners like VMware, Citrix, Aruba, AWS and Splunk, we redefined the cyber security market.

### Enterprise Defense and Resilience – defeating lateral movement

When you turn on Palo Alto Networks advanced protection, it extends prevention and resilience everywhere you have the Palo Alto Networks virtual or physical platform devices and endpoint agents.

> **Resilience:** Palo Alto Networks stops zero-days prior to exploitation, and automatically sends endpoint process memory to analysts to confirm the prevention. At the same time, the platform knows more about your traffic because of the application and user control, quality of service, and



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

segmentation. The platform provides unmatched control over authorized traffic *and* unauthorized traffic so IT operations and defense teams know and control everything that happening at all times.

**Data center:** Palo Alto Networks has integrated directly with VMWare, AWS and Citrix to scale prevention into the data center – on both physical and virtual platforms. The same visibility, advanced threat prevention, control and resilience extends, natively, within the data center for inter-VM (east-west) traffic to commercial and organic data centers. No more manual engineering required. Palo Alto Networks already works with commercial data centers today to provide visibility, control and protection for internal Data Center traffic.

**Future-proof:** The platform's extensibility and architecture provides the ability to turn on new functionality without the need for new hardware. The Palo Alto Networks' platform approach helps ensure freedom to change without increasing risk. We provide businesses the flexibility means to expand networks, contract networks or isolate applications, users and activity in creative ways without disrupting business continuity.

# Appendix: The Enterprise Security Platform

## Core Value Proposition

When we started Palo Alto Networks, we realized a fundamental key for protecting networks was getting control of the massive number of evasive applications hitting the market. We simply believed that port based security approaches were legacy and did little more than help companies maintain compliance with mandated bureaucratic guidelines. Our passion and diligence paid off and transformed the firewall industry forever with our **Next-Generation Firewall**. We now provide better native visibility, control and protection of all network traffic than any other vendor – this includes native ability to inspect all network traffic – no matter the port an application uses application uses, including SSL encrypted traffic.

We never intended to stop at the firewall. We wanted to control applications everywhere in a way that enables organizations to embrace new technology without increased risk. This desire led to the creation of a **Global Threat Intelligence Cloud** that allowed us to take our research intelligence and convert it into signatures quickly so our entire install base maintains full visibility, control and protection for their organizations at all times.

As we honed our ability to visualize, control and protect organizations with our **Next-Generation Firewall** and **Global Threat Intelligence Cloud**, we wanted to go even further – all the way to the endpoint. In 2014, we added our **Advance Endpoint Protection** that is integrated with our **Global Threat Intelligence Cloud**. It provides the ability to prevent exploitation of vulnerabilities by known, unknown or zero-day malware – this combined to create a novel forward advancement in prevention and disrupting the Cyber Attack Chain.



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

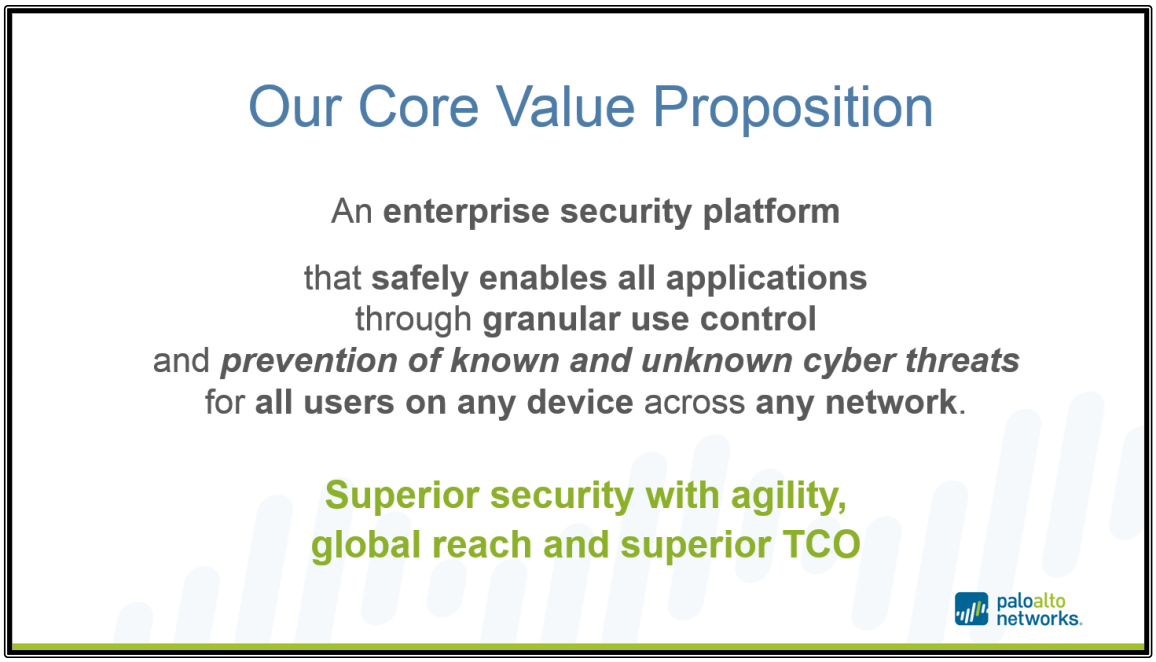



***Figure 8: Palo Alto Networks Core Value Proposition***

**Figure 8** provides an overview of our core value proposition. We created a purpose-built fully integrated **Enterprise Security Platform** to provide organizations a modern means to protect enterprises and prevent attacks across the Cyber Attack Chain. The intent is to enable organizations to embrace evolving technology without compromising security or increasing risk. As the figure shows, we safely enable the use of applications through granular control while preventing known and unknown cyber threats. Our modern approach to prevention provides relevant, scalable and extensible protection to all users on any device across any network. The modern prevention provides superior security with agility and global reach at a superior total cost of ownership.

## Palo Alto Networks Enterprise Security Platform

Continued interest and investment in technology from Palo Alto Networks is due in large part to our Enterprise Security Platform approach to cyber security. Our platform is a purpose-built product. The platform exists in all network traffic and endpoint memory in a way that allows a native ability to prevent zero-day and known malware delivery and execution.

To defend against advanced cyber adversaries, we designed and created a disruptive modern approach from the ground-up. **Figure 9** provides a visual of our fully integrated Enterprise Security Platform approach. The platform approach yields numerous cyber security benefits starting with the ability to see *all* network traffic everywhere on the enterprise, not just at the perimeter or on a handful of specified ports. Any solution that focuses on a limited set of ports leaves you vulnerable. In today's environment, evasive applications use multiple ports making port based security a losing proposition against attackers. You must be able to address *every* stage of the Cyber Attack Chain. The Palo Alto Networks platform is a zero trust enabling system with visibility and control across *all* network traffic and ports, regardless of where an attacker uses them – at the network edge, in the data center or at the endpoint. No other vendor has this extensibility.



**Palo Alto Networks** 4401 Great America Parkway Santa Clara, CA 95054 **Main:** 408.753.4000 **Sales:** 866.320.4788 **Fax:** 408.753.4001 **paloaltonetworks.com**

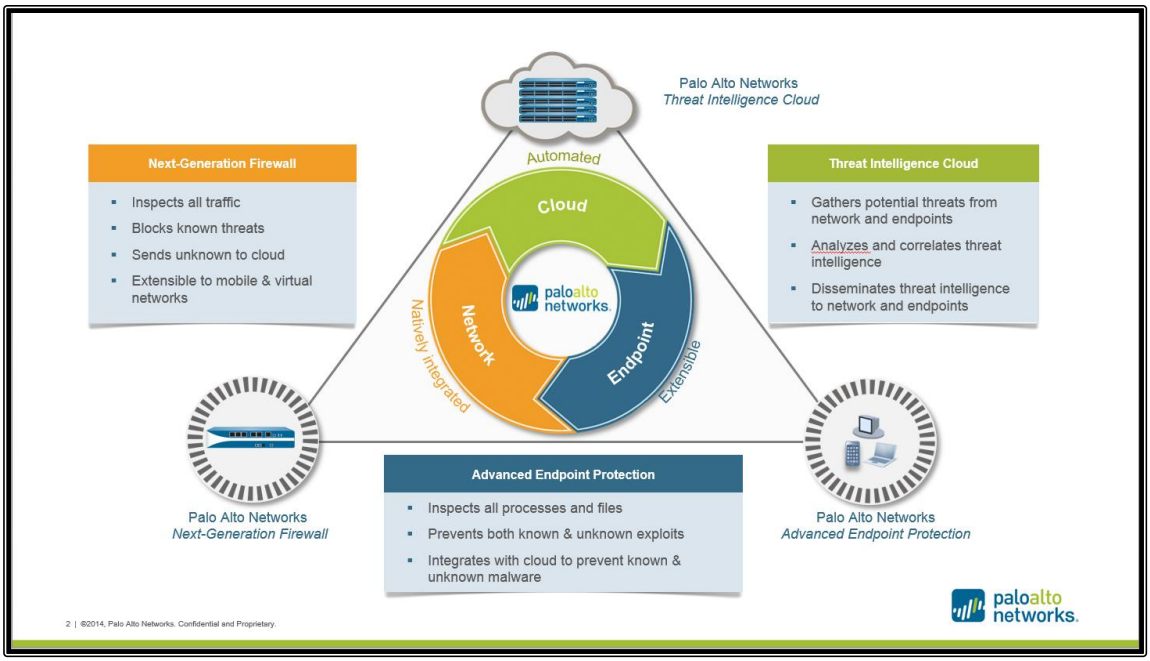



***Figure 9: The Enterprise Security Platform***

Our Enterprise Security Platform fully integrates **Next-Generation Firewall**, **Global Threat Intelligence Cloud** and **Advanced endpoint protection** components to raise the bar for prevention. Together, with strategic partners like VMware, Citrix, Splunk, AWS and Aruba, the Palo Alto Networks platform ensures quality of service and protects *every* part of a global enterprise network.

In addition, our platform approach not only addresses all threat variants, it addresses them across *all* threat vectors - not just a finite set of applications. Finally, it enables a cost effective, less complex, scalable deployment to address cyber threats with a centralized management capability. Less reliance on manual operations and the consolidation of functions otherwise provided by point tools translates into saved OpEx and CapEx with better efficiency in equipment and personnel.

## Endpoint + Network Visibility + Intel Conversion – key to advanced attack prevention

The days of chasing malware have proven inefficient and ineffective. The Palo Alto Networks *Enterprise Security Platform* is comprised of three elements best poised to prevent advanced attacks: **next-generation firewall**, **threat intelligence cloud**, and **advanced endpoint protection**. As **Figure 9** shows, the platform's **advanced endpoint prevention** adds endpoint threat protection to prevent active exploits of software vulnerabilities by mitigating the finite number of exploitation techniques an attacker must use to deliver their exploit. This approach, rather than analyzing and reacting to every exploited vulnerability, thus prevents delivery entirely. With this important triumvirate, the platform approach is the *key* to preventing advanced attacks and zero-days. The platform has added advantage of fast intelligence conversion that allows organizations to quickly turn intelligence around and deploy protection signatures across all network traffic, data centers, endpoints and mobility devices.

## Application Identification Intelligence – fast conversion to control evasive apps

In addition, Palo Alto Networks' intelligence and research team constantly gathers intelligence on evasive applications and converts the intelligence back into all platform devices. This ensures that organizations maintain control of evasive applications to ensure authorized activity traverses the networks while unauthorized activity fails to route. Our application research and intelligence team is available to perform custom intelligence analysis on any application a customer deems necessary to ensure quality of service and control at every location on the enterprise. This is an example of how the platform goes beyond



**Palo Alto Networks** 4401 Great America Parkway Santa Clara, CA 95054 **Main:** 408.753.4000 **Sales:** 866.320.4788 **Fax:** 408.753.4001 **paloaltonetworks.com**

eliminating the effectiveness of zero-days. The platform ensures high-quality service, control and protection.

### User Identification

The platform Operating System provides a straightforward and scalable approach for integration with user authentication. Nicely enough, this provides defenders the exact user targeted when an alert happens. It also informs the defenders about the applications used by users. From a scalability and architecture perspective, operators end up gaining efficiency without compromising on security. For instance, the embedded User-ID technology ensures that operations and defense teams knows the status of a user and the location of the device they are using at all times.

Analysts know the user and location because the platform includes pre-engineered server profiles that allow the platform Operating System to connect directly with all devices that authenticate users. This makes a big difference during investigations, not to mention the fact that organizations reduce the engineering time for integrating with multiple types of authentication. When you talk about architecture and scalability, this is a perfect example of many that allow the environment architecture to expand while automatically ensuring network operations and defense teams retain visibility.

### DNS-Based Intelligence

DNS traffic exists in nearly every organization, creating an overwhelming ocean of data security teams often ignore, or do not have the tools to analyze. Knowing this, cyber attackers are increasingly abusing DNS to mask their command-and-control (C2) activity in order to deliver additional malware or steal valuable data. Malicious domain names controlled by attackers enable the rapid movement of command-and-control centers from point to point, bypassing traditional security controls such as blacklists or web reputation. Palo Alto Networks addresses this by:

- Allowing opt-in passive DNS monitoring, creating a database of malicious domains and infrastructure across our global customer base. This intelligence is used by PAN-DB URL filtering, DNS-based command-and-control signatures, and WildFire to prevent future attacks.
- Enabling customers to create local a DNS sinkhole, re-directing malicious queries to an address of your choosing to quickly identify and block compromised hosts on the local network.

### Threat Prevention

This is the traditional IPS technologies rolled up. All the standard content signatures, Spyware, Anti-Virus, etc. combined into a continuously updated service or customizable environment for signature development. In a matter of mouse clicks, analysts create a policy to enforce traditional threat prevention approaches and apply the policy to all network traffic with deployed platform devices. When you need to modify the policy, you go in and make the change one time then apply it to all your traffic. The team creates custom signatures and filters through the same steps. Scalability without compromising security is the name of the game – network operations and defense professionals use an integrated operating system environment.

### WildFire

This makes up the advanced threat prevention cloud with a purpose of preventing unknown malware used in targeted attacks. We automated the process to provide shared intelligence and prevention signatures to over 4,000 and growing with an install base of over 19,000 enterprises. Wildfire covers numerous file types, performs automated sandboxed payload analysis and deploys signatures to all customers within 15 minutes. Any file sent up to WildFire automatically returns an analysis report with Indicators of Compromise (IOCs). A security operations and incident response analyst can manually submit malware for



Palo Alto Networks 4401 Great America Parkway Santa Clara, CA 95054 Main: 408.753.4000 Sales: 866.320.4788 Fax: 408.753.4001 paloaltonetworks.com

automated analysis that returns a report with IOCs. We are serious about shared intelligence to the point that we started an international consortium with customers and other cyber security companies. The goal is to share actionable intelligence and deploy indicators as fast as possible. WildFire is a feature of our platform that is, again, part of an integrated operating system and integrated with all our technology. That means, we provide coverage across more than just e-mail or browsing ports, the service extends across all ports and all traffic. The analysis extends to SSL encryption as well. The architecture and scalability keeps the Palo Alto Networks platform approach relevant to adapt detection and prevention as advanced attackers escalate methods.

### GlobalProtect

A discussion on scalability and architecture must include the platform's GlobalProtect VPN. Again, this technology comes pre-engineered in the platform as a feature. The platform utilizes GlobalProtect to extend all security, user and content policies to mobile devices. In fact, it extends all our technologies throughout the global environment including mobile devices. We have a platform device called the Mobile Security Manager that eliminates the need for a device manager while extending all the control, visibility and security to protect mobile devices. The GlobalProtect technology ends up being of significant importance to a scalable architecture while giving your operators the same look and feel for traditional premise networks and mobility devices. If an alert comes in, you know the user associated with the device and gain much improved visibility while using one platform for analysis.

### Panorama

This technology is pre-engineered to control all Palo Alto Networks devices. It provides your team a single interface into all the devices. You create policies one time and push them across the entire enterprise. You can access all alerts, events, pcaps, logs and devices from one console. This will save time for investigations and provides the team some interesting ways to command the enterprise. From a scalability and architecture perspective, operators gain great efficiency without compromising security.

## Summary

The Enterprise Security Platform from Palo Alto Networks provides the ability to evolve and remain agile as advanced adversaries initiate attacks on organizations. The platform protects ***every*** part of the global enterprise network, addressing vulnerabilities and malware arriving at the endpoint, mobile device, network perimeter and within the data center. This provides new defense and resilience to prevent attackers at every point of the Cyber Attack Chain. In addition to the resilience and prevention against today's most sophisticated attacks, Palo Alto Networks provides:

- Less reliance on manual operations.
- Easy transition from legacy point-appliances and tools.
- Extensibility – the platform extends prevention and resilience to every location a Palo Alto Networks' device and agent exists within the enterprise: across zero trust segments, into data centers, to defense mobility.

In all, the Enterprise Security Platform reduces costs and risk while introducing an entirely new approach for operating and defending your enterprise everywhere it exists.



**Palo Alto Networks** 4401 Great America Parkway Santa Clara, CA 95054 **Main:** 408.753.4000 **Sales:** 866.320.4788 **Fax:** 408.753.4001 **paloaltonetworks.com**