Yesterday's mobile security was designed for a different purpose

Security technologies used in the past are incapable of securing the 5G opportunity of the future.

For 5G to live up to its promise of transforming industries, enterprises need the confidence that 5G provides enterprise -grade security

A strange thing happened on the way to digital transformation. By moving our work, our lives and our photos of Aunt Jenny to the cloud, we found that the rules we thought we understood and lived by in order to secure our digital assets weren't a protection at all. It turns out that the bad guys and gals are really good at looking like you.

Now that pandemic and economic disruption and techno-social change have picked the locks and busted down the gates of our walled gardens, we are free to move about, living and working where we like. Unfortunately, so are the criminals: making lateral moves, dropping in man-in-the-middle attacks, gumming up gNBs, swarming cloud-based platforms, or creating more havoc with rogue base stations.

"Know the rules well, so you can break them effectively."

– Author unknown

In the midst of this upheaval, technology promises more opportunity and disruption. Enterprises see the next generation of mobile technology, 5G, as an opportunity for digital transformation. It is perceived as a key enabler for data-driven, opex optimized, constantly adapting, mass customization with instant time-to-market. For 5G, the stakes are higher because of the critical applications it carries. At the same time, yesterday's mobile security is not up to the task to provide the needed level of security. The legacy solutions for mobile security have many problems, but in a nutshell, they still rely on security derived through implicit trust of validated users, devices, applications and infrastructure.

We need a new way of securing mobile users, mobile applications, and mobile infrastructure - one that is adaptable and sustainable.

Breaking Trust: Building Sustainable Security for 5G

The concept of Zero Trust has been around for a few years now. However, with the advent of 5G, replete with thousands, or even millions of devices communicating across IP-based networks, comes the expansion of an attack surface that challenges network security professionals to gain granular visibility and control while managing and responding to threats with automation and AI.

Zero Trust for 5G is an opportunity to modernize and rebuild our technology platform and the ways in which we use it. This new method of defense does more than simply protect assets sustainably. It offers an opportunity to transform what we do and how we do it.

Whether a mobile network operator (MNO), an enterprise, or an end user, it's important to understand that Zero Trust is a strategic approach to cybersecurity that uses the principle of least privilege and then continuously validates every stage of a digital interaction. Zero Trust for 5G removes implicit trust all along the mobile landscape, regardless of what the situation is, who the user is, where the user is or what application they are trying to access.

MNOs must consider the impact of Zero Trust on network security, specifically how it protects the security of sensitive data and critical applications by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention and simplifying granular user-access controls. Where traditional security models operate under the assumption that everything inside an organization's perimeter can be trusted, the Zero Trust model recognizes that trust is a vulnerability.

In cybersecurity, for example, you'll often see mentions of trusted networks, channels, interfaces, devices, certificates, credentials and many other elements of the IT infrastructure that have been personified, in order to achieve simplification. This perception of trust comes from the implicit belief that these components have somehow earned the right to be used without restriction, most likely because of their present location or the fact they have proven their identity at least once, successfully.

This is what we call "Implicit Trust."

Attackers do indeed gain an advantage when they are able to take control of a machine that is implicitly trusted and therefore access other systems without any further security checks.

The migration to software-defined architecture, as evidenced by the quick adoption of cloud platforms, the proliferation of 5G vendors, and other COTS or open source software in 5G, presents something of an open door for hackers. Implicit trust has led to "walled gardens" or "castles" in which traffic is trusted. This frame of reference must be abandoned completely, moving toward a new, consistently applied approach to Zero Trust for 5G for all authentication and access requests,

whether by human or machine users. The ecosystem needs assistance to protect the 5G infrastructure and the business-critical traffic it carries with modern cybersecurity technologies.

This really means that specific capabilities are required to be successful in deploying Zero Trust strategically, but while adopting them, we need to carefully consider how we are going to deal with the myriad of individual products and vendors that claim to solve an individual problem related to implicit trust.

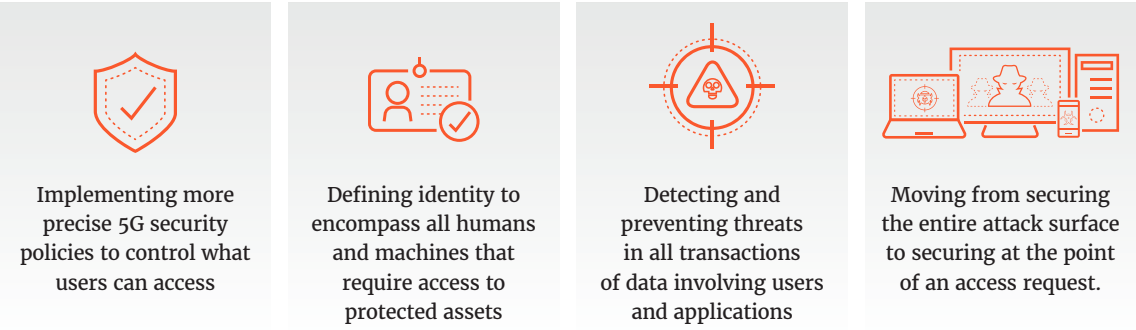
The problem with this approach is that it never ends and every implicit trust problem generates the need for an additional product or solution that will try to mitigate it.

It is not a mystery that businesses adopting cyber-security solutions are forced to do so in a very piecemeal approach and proceeding in a tactical, disjointed fashion.

In order to solve the issues with Zero Trust that have been pervading cybersecurity for over a decade, we need to focus on the strategy first, and sort out the technology second.

Implementing a Zero Trust Architecture for 5G

Deploying a Zero Trust architecture (ZTA) supports a smoother, more efficient path to digital transformation. Implementing Zero Trust architecture has some differences between the service providers, who primarily provide 5G infrastructure and services, and the enterprises, who use 5G as the connectivity fabric for their critical applications and operations. The common elements that span both players will protect assets more confidently by:



Common elements of a Zero Trust Architecture for 5G

As with traditional network access controls, 5G users should only have access to what is needed to perform their day-to-day functions. Because newly connected devices will rely on analytics from the applications they work with, all network traffic will need to be segmented and prioritized to make sure the highest-performing traffic has the necessary quality of service, latency and network performance.

For 5G to live up to its promise of transforming industries, enterprises need the confidence that 5G provides enterprise-grade security. We need a Zero Trust approach where we consistently protect all facets of the 5G infrastructure:

1. **All layers** - Apps, signaling, data, etc. You can't secure what you don't see.
2. **All locations** - This might seem obvious, but it's important to secure the entire lifecycle of an attack. This means being in all of the places where an attack may occur.
3. **Advanced threats** - The level of sophistication in the attacker landscape, including nation states and nation state level attacks, is very apparent. If Colonial Pipeline was running over 5G, would they be secure? The answer needs to be yes.
4. **DevOps, CI/CD** - Security teams must engage developers and DevOps teams to integrate security and compliance checks into development and DevOps workflows, providing actionable feedback and guardrails to prevent misconfigurations.

Fortunately, building a Zero Trust architecture is simpler than it appears. Because Zero Trust is an augmentation of your existing architecture, it does not require a complete technology overhaul. Rather, it can be deployed iteratively while allowing you to take advantage of the tools and technologies you already have.

Using a five-step model for implementing and maintaining Zero Trust, you can understand where you are in your implementation process and where to go next. These steps are:

1. **Define the protect surface.** Working tirelessly to reduce the attack surface is not viable in today's evolving threat landscape. The attack surface is always expanding, making it difficult to define, shrink or defend against. However, with Zero Trust, rather than focusing on the macro level of the attack surface, you determine your protect surface. The protect surface encompasses the critical data, application, assets and services—DAAS—most valuable for your company to protect.

   Here are some examples of DAAS you might include in your protect surface:

Data

Credit card information (PCI), protected health information (PHI), personally identifiable information (PII) and intellectual property (IP)

Applications

Critical business applications across edge clouds and data centers

Mobile assets

SCADA controls, point-of-sale terminals, medical equipment, manufacturing assets and IoT devices

Mobile infrastructure

5G network functions and telco cloud assets

Once defined, you can move your controls as close as possible to that protect surface to create a microperimeter with policy statements that are limited, precise and understandable.

2. **Map the transaction flows.** The way traffic moves across a network determines how it should be protected. Thus, it's imperative to gain contextual insight around the interdependencies of your DAAS. Documenting how specific resources interact allows you to properly enforce controls and provides valuable context to ensure the controls help protect your data, rather than hindering your business.

3. **Architect a Zero Trust network.** Zero Trust networks are completely customized, not derived from a single, universal design. Instead, the architecture is constructed around the protect surface. Once you've defined the protect surface and mapped flows relative to the needs of your business, you can map out the Zero Trust architecture, starting with a next-generation firewall. The next-generation firewall acts as a segmentation gateway, creating a microperimeter around the protect surface. With a segmentation gateway, you can enforce additional layers of inspection and access control, all the way to Layer 7, for anything trying to access resources within the protect surface.

4. **Create the Zero Trust policy.** Once the network is architected, you will need to create Zero Trust policies using the "Kipling Method" to whitelist which resources should have access to others. Kipling, well known to novelists, put forth the concept of "who, what, when, where, why and how" in his poem "Six Serving Men." Using this method, we are able to define the following:

   - ☐ Who should be accessing a resource?
   - ☐ What application is being used to access a resource inside the protect surface?
   - ☐ When is the resource being accessed?
   - ☐ Where is the packet destination?
   - ☐ Why is this packet trying to access this resource within the protect surface?
   - ☐ How is the packet accessing the protect surface via a specific application?

   With this level of granular policy enforcement, you can be sure that only known allowed traffic or legitimate application communication is permitted.

5. **Monitor and maintain the network.** This final step includes reviewing all logs, internal and external, all the way through Layer 7, focusing on the operational aspects of Zero Trust. Since Zero Trust is an iterative process, inspecting and logging all traffic will provide valuable insights into how to improve the network overtime.

Once you have completed the five-step methodology for implementing a Zero Trust network for your first protect surface, you can expand to iteratively move other data, applications, assets or services from your legacy network to a Zero Trust network in a way that is cost-effective and non-disruptive.

5G-Native Security offers a comprehensive approach to protect all facets of the 5G networks. Service providers can deploy a Zero Trust architecture for their 5G network infrastructure and the business-critical enterprise, government and consumer traffic it carries. Enterprises and organizations can protect their 5G users, applications and infrastructure with the same Zero Trust approach they use in their other network segments.

Palo Alto Networks for the Zero Trust Enterprise

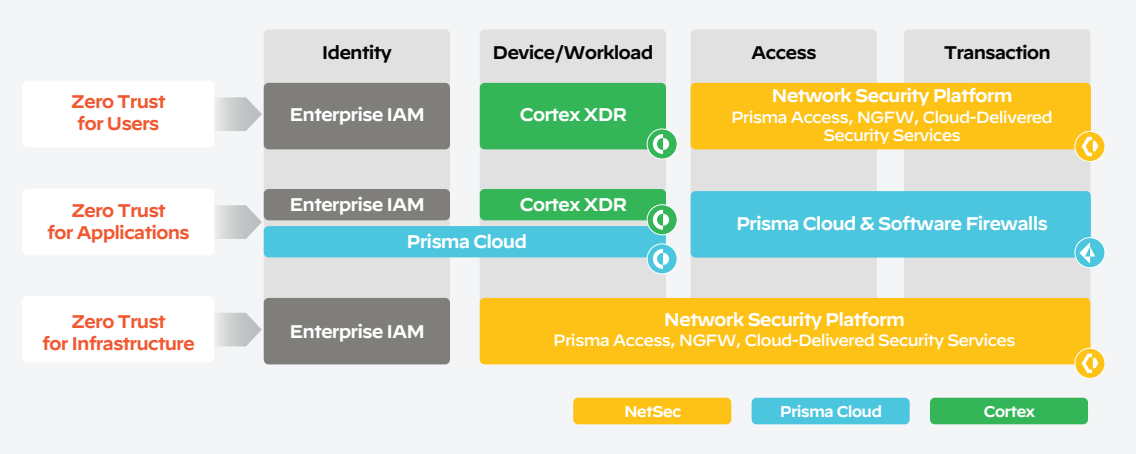


Figure 1: Above presents key Zero Trust capabilities required to secure 5G across users, applications, and infrastructure.

Palo Alto Networks for the Zero Trust Enterprise

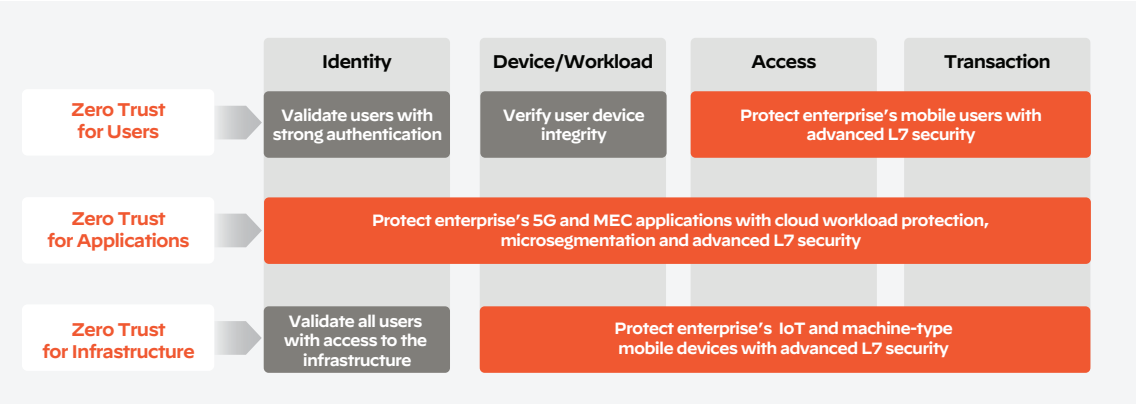


Figure 2: describes the specific actions taken to secure 5G for enterprises within that framework to address vulnerabilities and threats across all network elements.

Palo Alto Networks takes a comprehensive approach to Zero Trust for enterprises. This approach is about eliminating implicit trust across the 5G network. This means eliminating implicit trust related to users, applications, and infrastructure.

Zero Trust for Users

Step one of any Zero Trust effort requires strong authentication of user identity, application of "least access" policies as defined by the enterprise, and verification of user device integrity at every point of access request. One of the most important means of protecting user integrity is through stateful protection with the aid of NGFWs in order to secure L7 transactions and prevent loss of service due to compromised user equipment.

Zero Trust for Applications

Applying Zero Trust to applications removes implicit trust with various components of applications when they talk to each other. This is accomplished with cloud workload protection, microsegmentation, and advanced L7 security. 5G enables a closer integration of the applications and the network, allowing applications to take advantage of low latency and better transport economics. But, the new architectures, including MEC, blur the lines between enterprise and service provider infrastructure. Zero Trust is a fundamental tool to protect the applications deployed in distant edge locations with stateful traffic inspection, microsegmentation and continuous monitoring at runtime is necessary to validate their behavior.

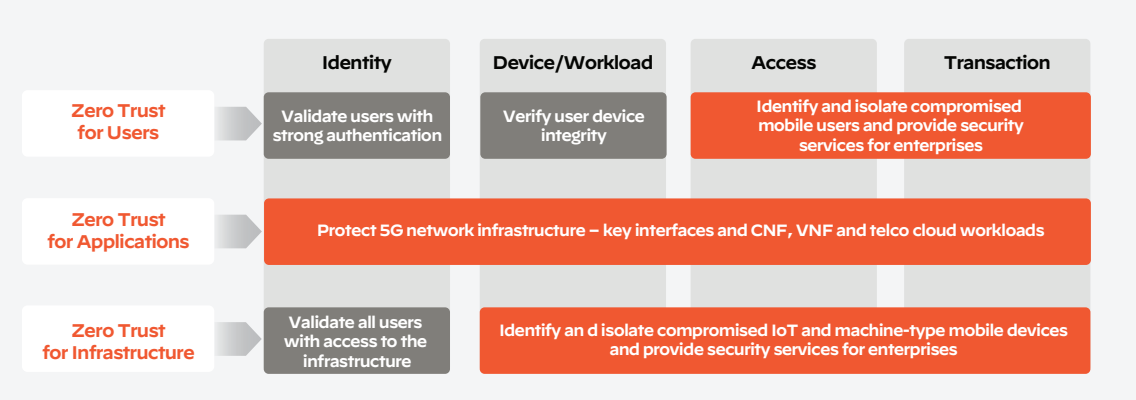
Zero Trust for Infrastructure

As enterprises make use of LTE and 5G mobile infrastructure, IoT and machine-type mobile devices that access this infrastructure are proliferating on a scale never seen before. Limitations of these devices often result in compromises in security capabilities, making mobile devices a soft target. This expanding attack surface, at times with inadequate physical security and gaps in the management and monitoring, poses serious risks of cyberattacks. A Zero Trust approach helps to take control of the vulnerable machine-type assets.

Zero Trust is for any enterprise that requires a secure network. So if an enterprise is going through a network transformation, if the data center is moving to the cloud, or if the organization is going through a SecOps transformation, Zero Trust is the right choice.

Zero Trust for 5G Drives New Service Provider Offerings

Palo Alto Networks for the Zero Trust Enterprise



For the *user plane*, the GSM association (GSMA) has published its FS.37 GTP-U Security guideline, which addresses the attack vectors in the user plane and the corresponding features a service provider would need to mitigate those threats. FS.37 provides recommendations for mobile network operators (MNOs) to detect and prevent attacks using General Packet Radio Service (GPRS) Tunneling Protocol for User (GTP-U) plane data on the network, services, and applications. FS.37 recommendations also recommend how to remediate the threat posed by malware or other suspect user traffic. GTP-U is the protocol that carries user data tunnels within the GPRS core network, and between the radio access network and core network.

Palo Alto Networks' ML-Powered NGFW uses GTP-U plane data to statefully detect and remediate in real-time malicious traffic that is attempting lateral movements across the network.

Equally, whether for users, applications, or infrastructure, effective Zero Trust execution by MNOs requires granular visibility and policy control of the user plane. Palo Alto Networks ML-Powered NGFW for 5G can be deployed at the N3 interface where it has full visibility of the user plane traffic. The firewall correlates user plane traffic in N3 with subscriber specific identifiers (user ID, device ID, slice ID) from the N4 interface (PFCP). The resulting granular visibility and control of the user plane traffic enables the mobile service provider to offer vertical or even customer-specific security policies.

Now each enterprise is, according to its security requirements and regulations, uniquely protecting its mobile-based infrastructure from UE-based threats through L7-based security intelligence. All Palo Alto Networks enterprise-grade security capabilities across App-ID and Cloud-Delivered Security Services (CDSS) – including DNS Security, Wildfire, Threat Prevention, URL Filtering, IoT Security, DLP – are available in any combination and configuration.

At the *application layer*, the core 5G network is fully containerized and built for Kubernetes environments, so security should be applied across cloud security posture management, cloud workload protection, cloud network security and cloud infrastructure entitlement management.

- **Cloud security posture management:** monitoring posture, detecting and responding to threats, and maintaining compliance with standards and regulations, such as CIS, PCI-DSS, HIPAA, GDPR, NIST SP 800-190 and FISMA.
- **Cloud workload protection:** securing hosts, containers, and serverless across the application cycle (host security, container security, serverless security, API security).
- **Cloud network security:** monitoring and securing cloud networks and enforcing identity-based microsegmentation.
- **Cloud infrastructure entitlement management:** enforcing permissions and securing identities across workloads and clouds (Identity and Access Management (IAM) security).

Finally, at the *infrastructure level*, accelerated by rapidly increasing IoT devices, the challenge is massive. The devices are heterogeneous across a multitude of software and hardware platforms. The limited computing and battery capacity of these devices often forces the device vendors to make compromises in security capabilities, making mobile devices and the infrastructure they access into soft targets. Infected devices can compromise organizations' business critical data and disturb mission-critical operations. They also pose a risk to the mobile network itself, especially in case of botnet-originated massive coordinated DDoS attacks.

The combination of limited device resources, heterogeneous device types and device vendors' tight control of the platforms makes it difficult to to implement device-based security solutions in scale. Palo Alto Networks' Zero Trust Framework applies network-based security design, which is a highly effective method to protect mobile devices at scale. When supported with granular visibility to user (SUPI) and device (PEI) level traffic flows, network-based security can see and stop advanced threats in real time. Organizations are able to protect their mobile devices across attack vectors including vulnerability exploits, ransomware, malware, phishing and data theft.

Conclusion

Moving to the cloud and digitally transforming operations in a secure manner certainly brings up an old feeling that "you can't get there from here."

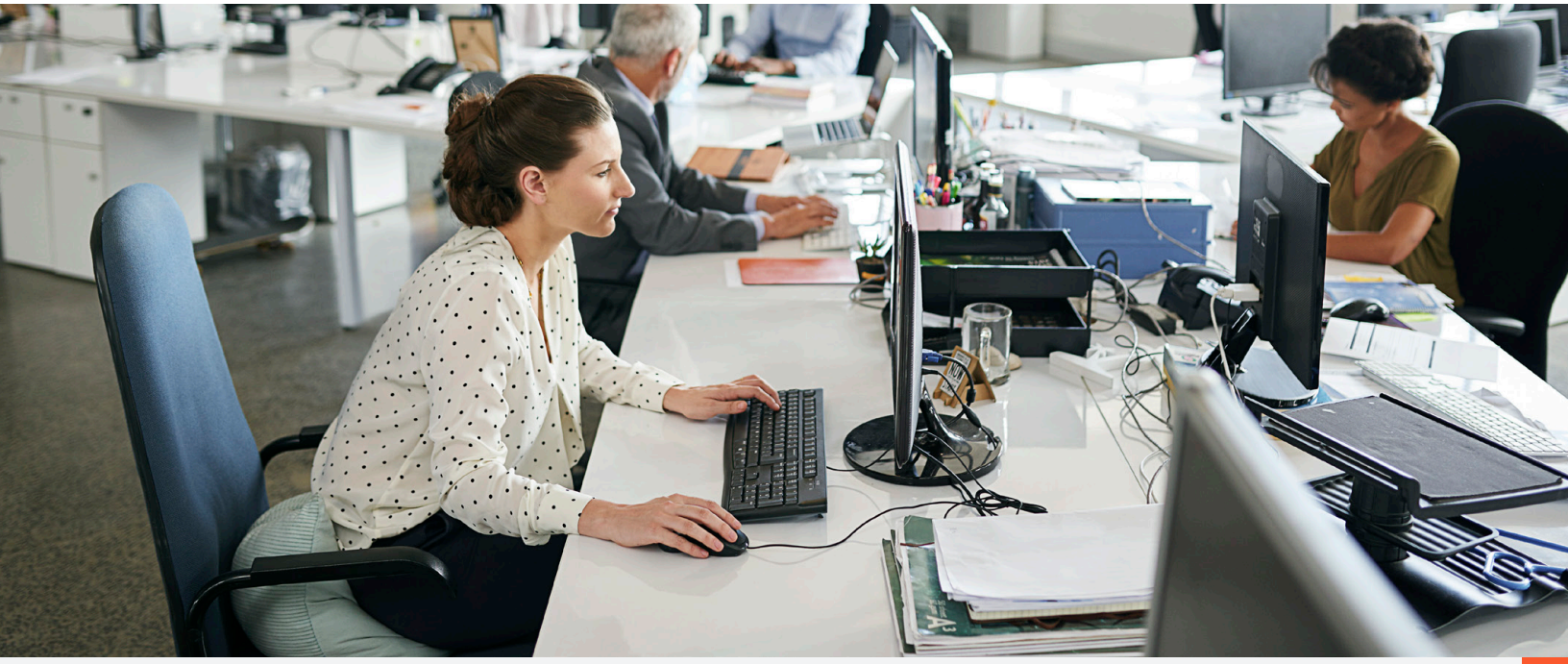
But there are unexpected rewards along the way to that new cloud-based transformation. By embracing a more sustainable Zero Trust approach to 5G security, both service providers and the enterprises they serve can find that they can turn something that they have to do (security as cost center) into something that they want to do (security as a profit center). Excellence in any capability always presents new business opportunities.

Service providers can find that they will:

1. Accelerate enterprise adoption of 5G services by backing them with the level of security and reliability that enterprises need for their business-critical applications
2. Differentiate from the competition - especially important in this era where no one wants to be profiled as "the dumb pipe"
3. Build new ways to serve enterprise customers with value add security services

Enterprises, as well as service providers, will find that building cybersecurity into the fabric of operations and network ecosystems becomes fundamental to how business is done in the 21st century. Securing core business processes will be the way that organizations of all sizes distinguish themselves, setting their operations apart from merely surviving and placing them squarely in the field of thriving.

The fact is that you do have to unlearn the old ways of protecting users, applications, and infrastructure. You have to be willing to bend your mind in new ways. In short, you have to break a few old rules about trust to get to your destination.



paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com