

ŠTA NAM NOVO DONOSI PALO ALTO NETWORKS?

- **Novosti u PanOS 12.2 (Ceres)**
- **Novi HW**
- **AI Security**
- **Prisma Access Browser**

Novosti u PanOS 12.2 (Ceres)

Advanced IP Defense

Advanced IP Defense: Blocking attacker infrastructure before they can strike

Modern threat actors continuously work to hide their attacks and evade existing controls. Adversaries are increasingly evading traditional perimeter detection of their command-and-control traffic by leveraging direct-to-IP connection techniques that bypass DNS and URL inspection entirely. Attackers are also weaponizing massive proxy networks and hundreds of thousands of residential IP addresses to conduct stealthy, large-scale scanning, brute-force attacks, and exploitation that bypass traditional defenses such as IP reputation and blocklists.

To counter this, Palo Alto Networks is introducing a new preventative solution, **Advanced IP Defense**, with three powerful new capabilities:

- **Real-time IP-layer intelligence.** We leverage global telemetry from over 70,000 customers to track and block attacker infrastructure inline across the entire attack lifecycle. Our researchers track these threats 24/7, so your team doesn't have to.
- **Zero-Trust IP enforcement.** We don't just look at an IP's past reputation. We verify the intent of the connection itself. By validating that every network connection maps to a legitimate DNS resolution, we provide a critical guardrail against attackers attempting to evade detection.
- **Powerful IP-layer context.** We continuously monitor every connection across more than 40 distinct security attributes, letting you proactively shrink your attack surface and block high-risk traffic from the internet's "bad neighborhoods" with confidence.

Advanced URL Filtering = reputation/intelligence about URLs

DNS Security = intelligence about domains/DNS

Advanced IP Defense = intelligence about the IP infrastructure itself

Local Deep-Learning analysis for Command Injection

Advanced Threat Prevention Local Deep Learning Support for Command Injection

Release Date: July 2026 | Last Updated: July 2026

While inline cloud analysis for Advanced Threat Prevention provides robust command injection protection, it can restrict traffic volume and introduce 100–200 milliseconds of latency—challenging for high-throughput environments. Local Deep Learning for command injection resolves this by running the Palo Alto Networks deep learning model directly on supported NGFWs. This allows you to inspect significantly more inbound traffic locally, delivering verdicts up to 100 times faster than cloud-only analysis.

Local Deep Learning for command injection uses the same proven model that runs in the Advanced Threat Prevention cloud, optimized for on-device execution through new CPU instruction sets and memory-efficient model loading. You configure the feature in the **Vulnerability Protection profile** under the Inline Cloud Analysis tab—a new Local Deep Learning column lets you enable or disable the feature for the command injection ML model. Local Deep Learning is enabled by default when you enable Inline Cloud Analysis on a new Vulnerability Protection profile, giving you immediate command injection protection without additional configuration.

During operation, the NGFW evaluates suspicious HTTP traffic against the local model and processes benign verdicts instantaneously. If the model identifies a potential command injection exploit, it forwards the traffic to the cloud for a false-positive check and returns the cloud verdict when available. If the cloud is unreachable or times out, the NGFW uses the local model verdict and takes the action you configured—eliminating the fail-open gap where threats could pass uninspected. A new local packet capture option lets you retain forensic evidence for detections made when the cloud is non-responsive.

Content updates deliver the latest command injection models automatically, keeping your on device detection current without manual intervention.

Local Deep Learning for the Anti-Spyware profile (HTTP and HTTP2 Command and Control detectors) is available on the following platforms:

- PA-5500 Series
- PA-5400 Series, excluding the PA-5450 appliance.
- VM-Series (must allocate at least 16GB of total memory)
- VM-Series Public Cloud
- VM-Series Private Cloud

Starting with PAN-OS 12.2, Local Deep Learning extends to the Vulnerability Protection profile, enabling on-device command injection analysis. This allows you to inspect significantly more inbound traffic and receive verdicts up to 100 times faster than cloud-only analysis. Local Deep Learning for command injection is available on the following platforms:

- PA-3400 Series
- PA-5400 Series (PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445)
- PA-7500
- VM-Series

Advanced Threat Prevention Plus and Frontier Virtual Patching

Proactive Vulnerability Discovery: Instead of the reactive process of waiting for attacks against new CVEs or public disclosure of vulnerability details, our solution proactively hunts for hidden vulnerabilities inside critical software, including both open source and commercial software.

- **Open Source Discovery:** Palo Alto Networks research uses our frontier AI harness (NOVA) to proactively detect and verify new vulnerabilities within thousands of critical open-source repositories.
- **Critical Defense Program:** CDP is the most comprehensive program in the industry to identify vulnerabilities as early as possible. Collaborators share existing CVEs or new, undisclosed vulnerability data with Palo Alto Networks, enabling us to provide rapid and comprehensive network protections (“virtual patches”) within hours of initial discovery to mutual customers. This program builds on our existing collaborations with IBM and Red Hat (as part of Lightwell), Microsoft (as part of MAPP) and OT leaders like Siemens and the Idaho National Laboratory (as part of the OT Threat Research Lab). We recently expanded the collaboration to include Anthropic, OpenAI, OT leaders like Mitsubishi and Axis Communications, industry consortiums for sharing risk information like Analysis and Resilience Center for Systemic Risk and Health-ISAC, OT research organizations like the independent, non-profit Energy R&D Institute (EPRI) and OSS initiatives like Akrites (an initiative from the Linux Foundation).
- **Traditional Sources:** We complement these proactive sources with over 20 traditional, reactive sources like in-the wild exploits, vulnerability feeds, bug bounties and commercial providers for public vulnerabilities.

NOVA AI research	Finds vulnerabilities proactively in open-source software
Critical Defense Program	Vendors/researchers share undisclosed vulnerabilities early
Existing intelligence	CVEs, exploits, feeds, bug bounty programs, observed attacks

PanOS Shield

PAN-OS Shield provides vulnerability protection for firewalls with GlobalProtect gateway or portal. When you enable PAN-OS Shield, the firewall scans inbound control traffic using threat prevention signatures and takes action against detected exploits before they reach the management plane. This protects PAN-OS services from vulnerabilities—including critical exploits such as those targeting privilege escalation after initial compromise—by inspecting traffic at the data plane before it is forwarded to management plane processes.

PAN-OS Shield requires PAN-OS 12.2.2 or a later release. An Advanced Threat Prevention license provides signatures through regular content packages, but the license is not strictly required—signatures are also delivered through application-only content updates.



You can enable PAN-OS Shield without GlobalProtect gateway or portal configured, but the feature doesn't protect anything until GlobalProtect control traffic is present.

PAN-OS Shield operates through a dedicated internal virtual system (panos-shield-vsyt) that the firewall creates automatically when you enable the feature. This internal vsyt hosts a vulnerability protection profile and a security policy that are delivered and updated through content packages. You don't need to configure multi-vsyt mode or allocate additional vsyt licenses—the internal vsyt is created independently of your licensed vsyt capacity.

The vulnerability protection profile and security policy that PAN-OS Shield uses are read-only—they are delivered through content updates and you cannot modify them directly. However, you can add threat exceptions to override the action for specific threat IDs if you encounter false positives that impact your environment. When a signature triggers, the firewall generates a threat log with the matched threat ID, action taken, and relevant session details.

PAN-OS Shield is disabled by default. After you enable or disable the feature, a commit and reboot is required for the change to take effect. If you disable PAN-OS Shield, a confirmation warning explains the security implications of removing the protection.

When PAN-OS Shield is enabled, a read-only vulnerability protection profile appears under **Objects > PAN-OS Shield > Vulnerability Protection**. You can add threat exceptions to this profile to change the action for specific threat IDs.

L2 Switching Functionality

Layer 2 Switching on Next-Generation Firewalls

Release Date: July 2026 | Last Updated: July 2026

When you need to consolidate your network infrastructure, the [Layer 2 Switching feature](#) on Next-Generation Firewalls allows you to operate your firewall as a fully functional Layer 2 switch. This feature introduces comprehensive switching capabilities directly on the firewall, enabling you to configure access and trunk VLANs per port, deploy Multiple Spanning Tree Protocol (MSTP) for robust loop avoidance, utilize Link Aggregation (LAG), and apply Storm Control to mitigate excess broadcast, unknown unicast, and multicast traffic.

You can leverage this capability primarily to achieve a *branch in a box* deployment, which is specifically targeted at small to medium-sized network environments such as retail locations, healthcare facilities, and financial branch offices. By merging your traditional standalone switch, router, and firewall into a single appliance, you significantly reduce overall hardware costs and simplify your ongoing network management.

Furthermore, this architecture empowers you to implement micro-segmentation and Zone-Based Forwarding (ZBFW) for lateral traffic, allowing you to secure east-west communication within and across VLAN boundaries.

This capability is rolling out across:

- Select 5th-Generation PA-500 Series Platforms (Supported in the [PAN-OS 12.2.2 release](#))
- All 5th-Generation PA-1500 Series Platforms (Supported in a future release at product launch)

Table 1: PA-Series platforms support for Layer 2 switching

Model	Data Ports
PA-1530-POE*	32 ports (16 PoE) (1Gx8, 5Gx4, 10Gx16, 25Gx4)
PA-1520-POE*	32 ports (16 PoE) (1Gx8, 5Gx8, 10Gx12, 25Gx4)
PA-1510-POE*	32 ports (16 PoE) (1Gx16, 5Gx8, 10Gx8)
PA-560	24 ports (1Gbps x 20, 10Gbps x 4)
PA-555-POE	16 ports (8 PoE) (1Gbps x 10, 2.5Gbps x 4, 10Gbps x 2)
PA-550	16 ports (1Gbps x 14, 10Gbps x 2)
PA-545-POE	16 ports (4 PoE) (1Gbps x 12, 2.5Gbps x 4)

Browser Identification & Enforcement in the NGFW

Prisma Browser is the only browser that can be cryptographically identified by NGFW, allowing its traffic to be distinguished from other browsers.

Organizations can apply policies specifically to Prisma Browser traffic, preventing access to corporate resources from unapproved or unsecured browsers. This allows organizations to reduce resource consumption in the NGFW by enforcing all security policies within Prisma Browser instead of during inline inspection through NGFW. This reduces the need to decrypt browser traffic.

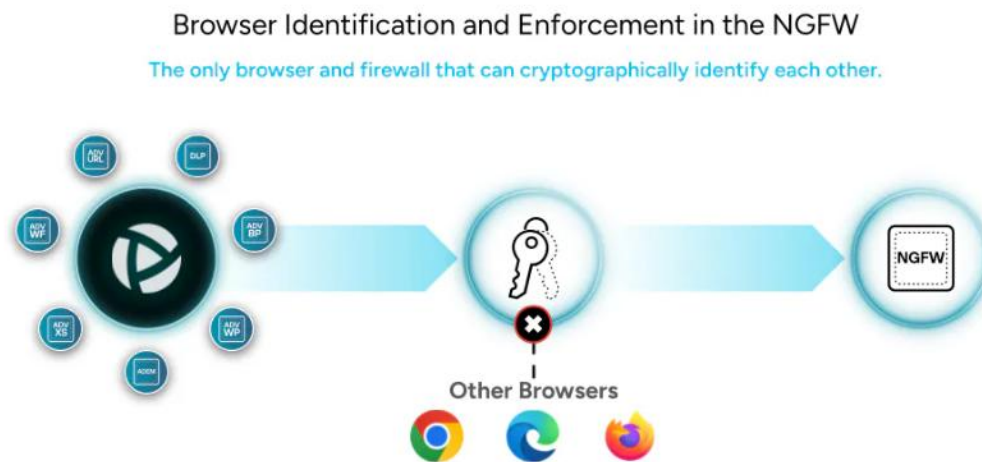


Figure 4. Ensure corporate resources can only be accessed through Prisma Browser.

This unique integration between Prisma Browser and NGFW is a key advantage of the Palo Alto Networks platform, allowing you to better protect on-premises environments, reduce NGFW resource consumption, support new business continuity scenarios, and extend advanced security across all on-campus network access.

Novi Hardware

PA-1500 POE NGFW



PA-1510-POE



PA-1520-POE



PA-1530-POE

PA-1500 POE NGFW

Table 1. Performance and Capacities of PA-1500 Series Quantum-Optimized NGFWs

	PA-1510-POE	PA-1520-POE	PA-1530-POE
Firewall throughput (appmix)*	15 Gbps	25 Gbps	35 Gbps
Threat Prevention throughput (appmix)†	9 Gbps	18 Gbps	27 Gbps
IPsec VPN throughput‡	7 Gbps	14 Gbps	18 Gbps
Max. concurrent sessions§	1,095,000	1,495,000	1,750,000
New sessions per second	140,000	180,000	220,000
Virtual systems (base/max)#	1/6	1/11	1/11

Table 1. PA-3400 Series Performance and Capacities

	PA-3410	PA-3420	PA-3430	PA-3440
Firewall throughput (appmix)*	14 Gbps	19 Gbps	29 Gbps	35 Gbps
Threat Prevention throughput (appmix)†	7.5 Gbps	10 Gbps	15 Gbps	20 Gbps
IPsec VPN throughput‡	6.6 Gbps	9.9 Gbps	12 Gbps	14.5 Gbps
Max concurrent sessions§	1.4M	2.2M	2.5M	3M
New sessions per second	145,000	220,000	240,000	268,000
Virtual systems (base/max)#	1/11	1/11	1/11	1/11

PA-1500 POE NGFW

Table 3. PA-1500 Series Hardware Specifications

I/O
PA-1510-POE: 10/100/1000 Cu (12), 1G/2.5G/5G Cu (8), 1G SFP (4), 1G/10G SFP+ (8)
PA-1520-POE: 10/100/1000 Cu (8), 1G/2.5G/5G Cu (8), 1G/2.5G/5/10G Cu (4), 1/10G SFP+ (8), 10G/25G SFP28 (4)
PA-1530-POE: 10/100/1000 Cu (8), 1G/2.5G/5G Cu (4), 1G/2.5G/5/10G Cu (8), 1/10G SFP+ (8), 10G/25G SFP28 (4)
Storage Capacity
PA-1510-POE, PA-1520-POE: 480 GB
PA-1530-POE: 960 GB

Table 3. PA-3400 Series Hardware Specifications

I/O
PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3420: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3430: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
PA-3440: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
Storage Capacity
480 GB SSD

PA-3500 Series NGFW



PA-3510



PA-3520



PA-3530



PA-3540

PA-5500 Series NGFW



PA-5510



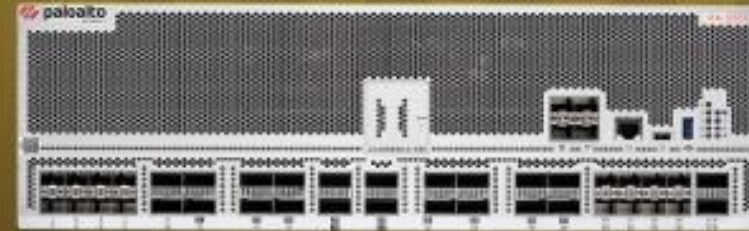
PA-5520



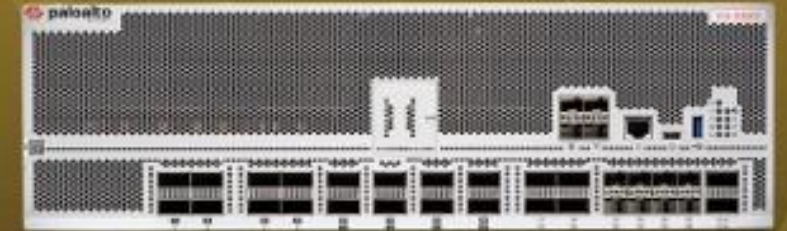
PA-5530



PA-5540



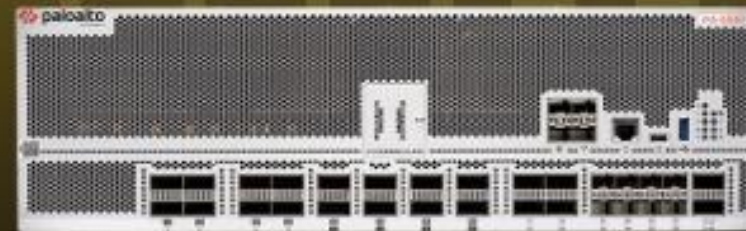
PA-5550



PA-5560



PA-5570



PA-5580

AI Security

- AI Access Security
- AIRS

Prisma Access Browser

The Browser is **the Modern Workspace**

The browser is where

85-100%

of a workers day is spent.¹

And it's the new OS

Cookies
MFA Identity context App-level access
JavaScript
Cache and local storage PWAs
Tokens
WASM
3rd-party scripts Access controls
Extensions
OSS

But, Browsers are Vulnerable

491

vulnerabilities were found in
browsers in 2025.²

280M

malicious extensions downloaded
unknowingly in one study.³

~95%

of organizations experienced a
security incident originating in
the browser in 2024.⁴

1. Palo Alto Networks/Omdia Forrester, 2.CVE Details,
3. Stanford University 4. Palo Alto Networks/Omdia Forrester

M E E T

PRISMA[®] BROWSER

BY PALO ALTO NETWORKS



Any user



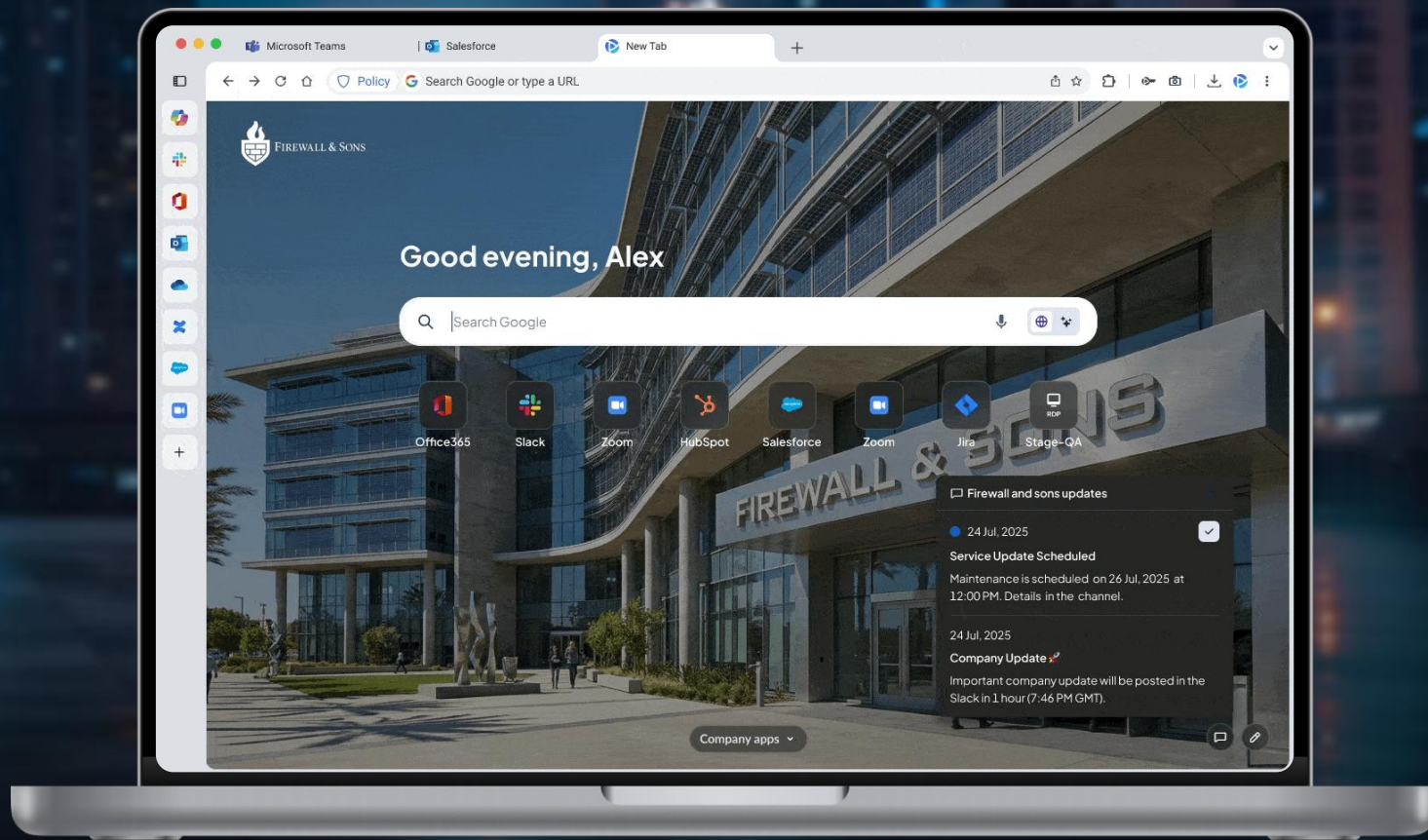
Any device



Any location



Any application



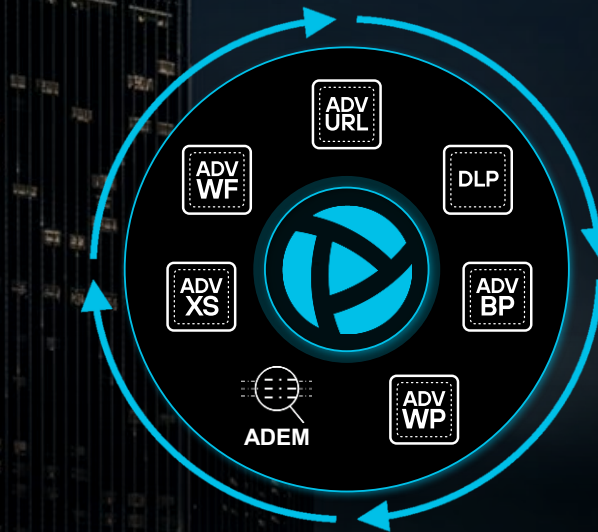
The Most Secure Browser for the Modern Workspace

PRISMA BROWSER PLATFORM

✓ Chromium-based, native UX

✓ Zero infrastructure changes

✓ No admin privileges required



Leveraging Palo Alto Networks **AI-Powered Security**

Fight AI with AI



Advanced WildFire®

Industry's largest cloud-based malware prevention engine



Advanced URL Filtering

Industry's biggest AI-powered threat intel database



Advanced Threat Protection

Real-time defense against known and unknown network-based exploits

Identify Attacks Legacy Tools Miss

NEW

Advanced Web Protection

Real-time AI-powered scanning of all web pages before the page loads, and continually after

NEW

Advanced Browser Protection

Detects and blocks 0-days with patented exploit mitigation technology in the browser

NEW

Advanced eXtension Security

Detect and continually monitor extensions for suspicious browser behavior and compromise

Granular Last Mile Data Controls: Context Aware



ALL Actions & Last-Mile
Agnostically on **ANY** App

Files



File upload / download

Last-mile



Copy / paste



Print



Screenshot / screenshare

Web-specific



Web login



Masking



AI Prompts



Camera /
Microphone



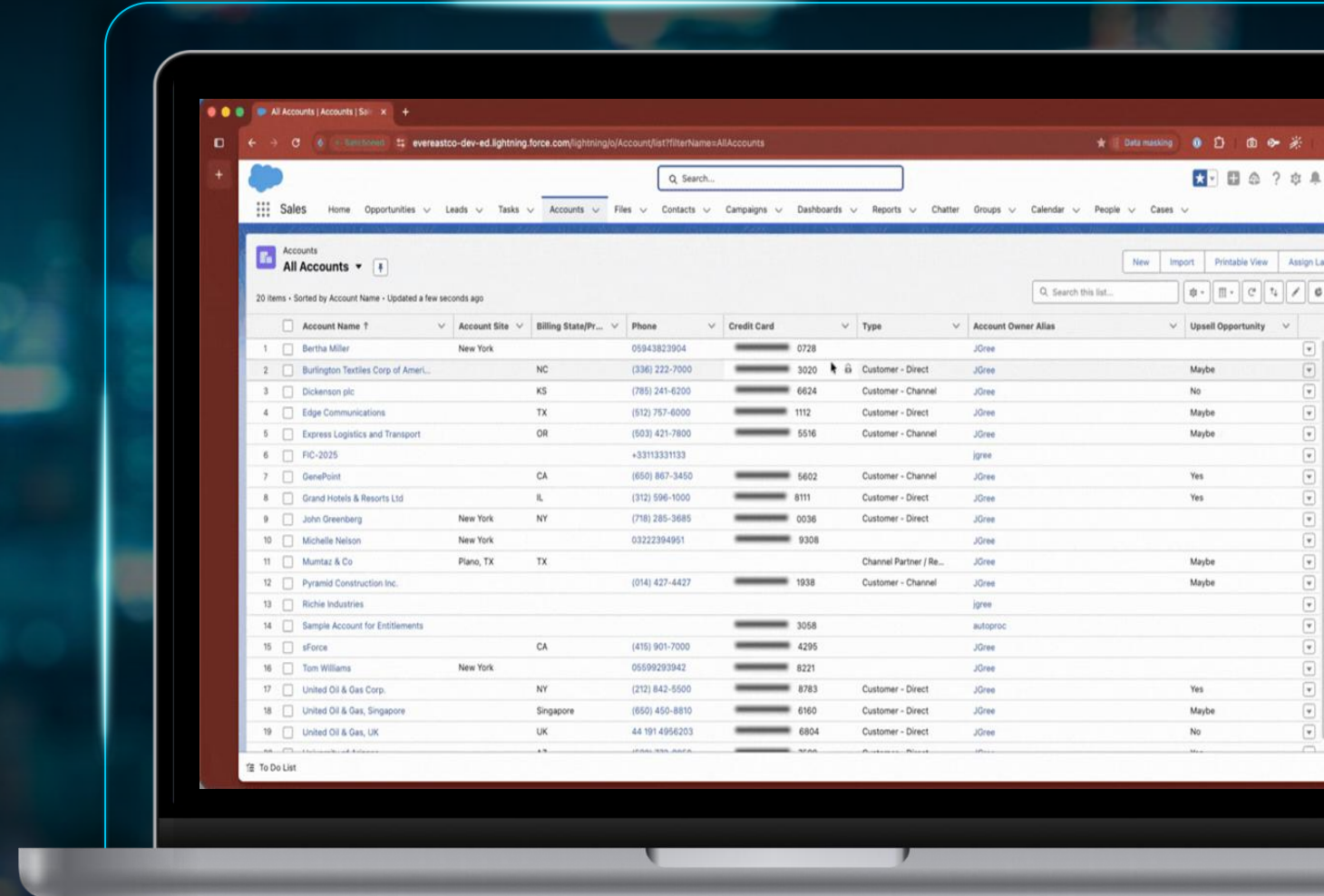
Typing / read-
only



Watermarks



Web elements



Seamless Connectivity to **Private Applications**



Direct access to **SaaS / internet**



Direct access to **private app** via **PB Connector**

True ZTNA with no additional deployments

NGFW, Service Connection, ZTNA Connector, or Colo Connect



DEMO

HVALA!

PITANJA

POWERED BY **NET++** TECHNOLOGY

Net++
TECHNOLOGY

