Thwarting Attackers: Defending Against Growing Security Sophistication while Managing Complexity

Raj Kumar

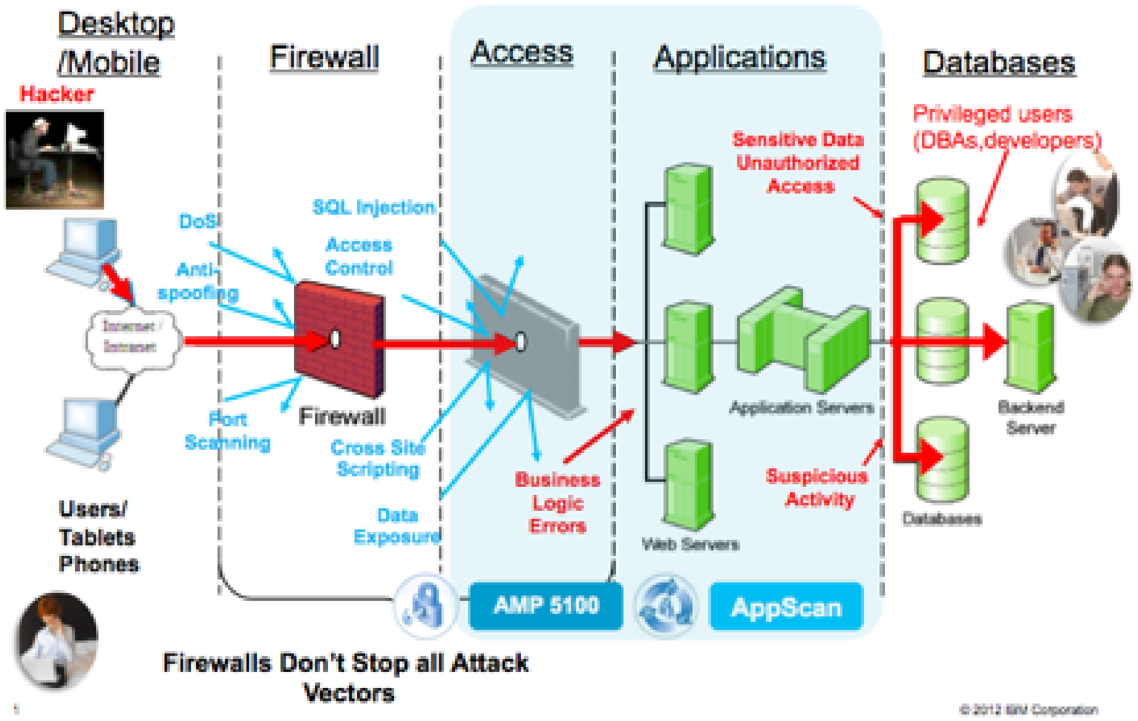
Thwarting Attackers: Defending Against Growing Security Sophistication while Managing Complexity

- Managing evolving threats with a network-based and tiered solutions approach, reducing overall costs and complexity
- Adhering to regulatory and industry compliance standards
- Managing headcount and budgets when evaluating new security and threat intelligence solutions

Managing evolving threats with a network-based and tiered solutions approach, reducing overall costs and complexity

Why network based and tier solutions?

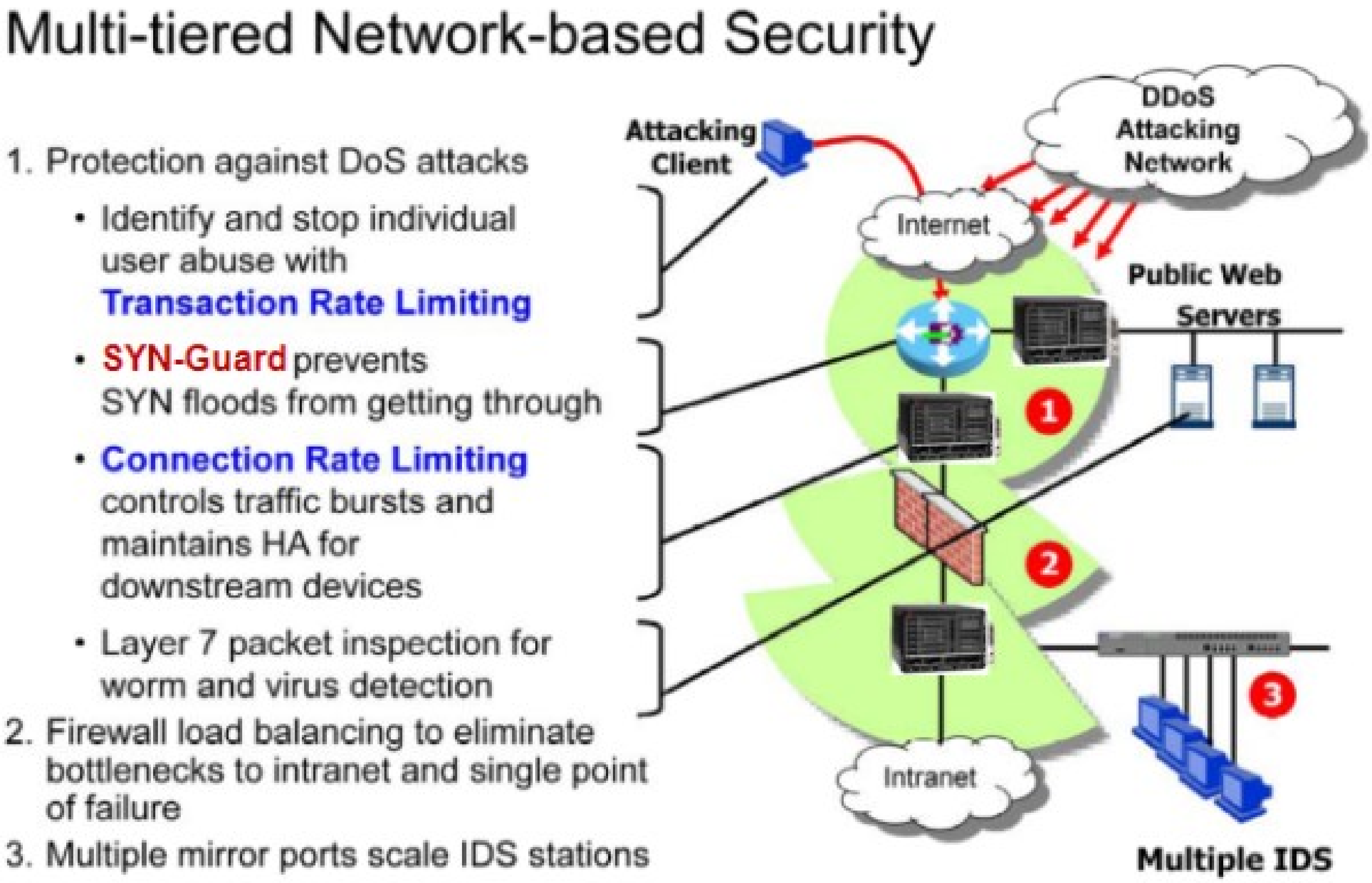
- Cyber threats keep evolving
- Need for enhanced layered network security approach
- There is a need for monitoring:
  - Command and control servers
  - Suspect sites and IP addresses
  - Netflow sessions
  - Unusual activities
  - Growing number of unknown threats



Firewalls Don't Stop all Attack Vectors

© 2012 IBM Corporation

Network-based and tiered solutions approach

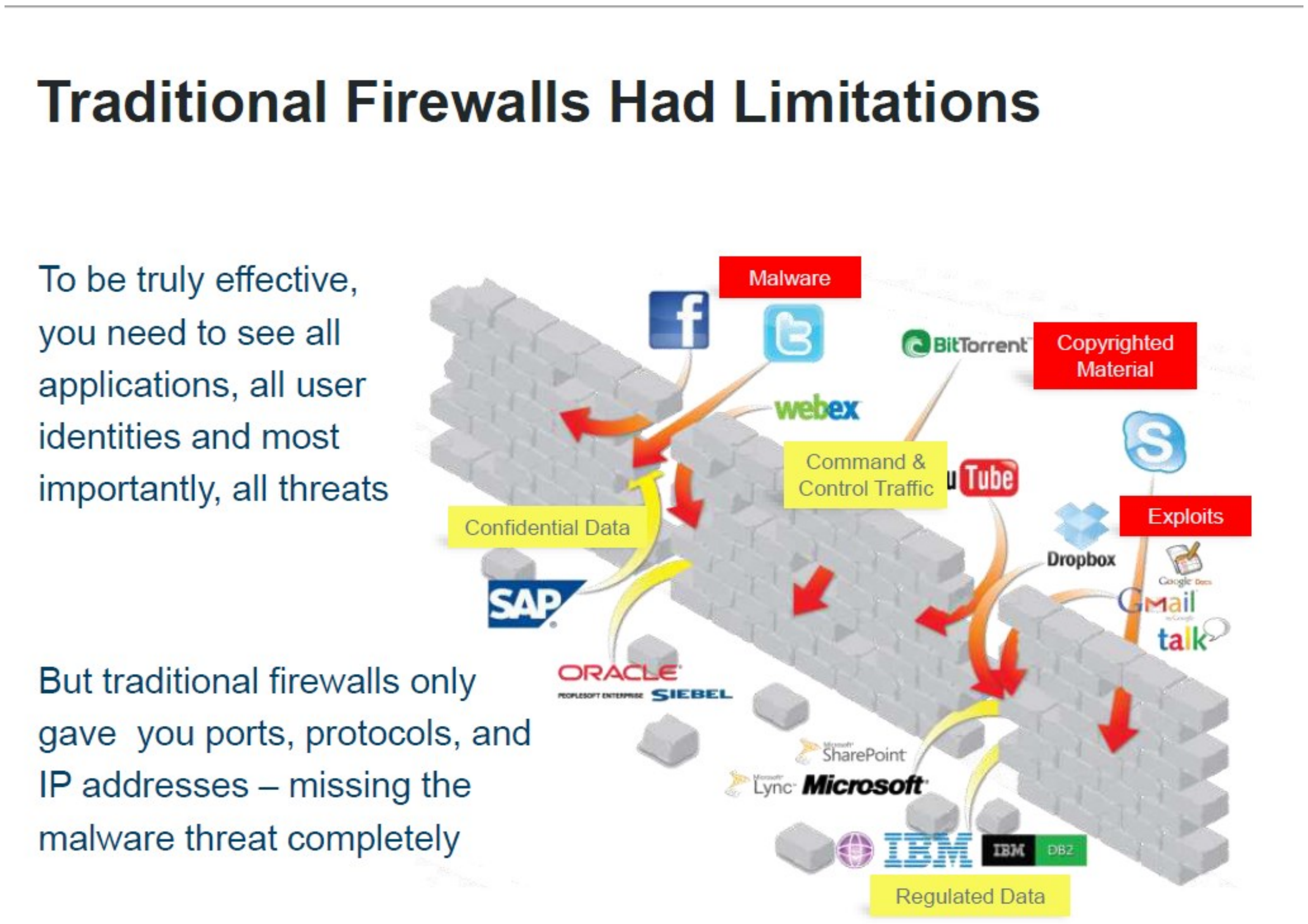


Multi-tiered Network-based Security

1. Protection against DoS attacks
   - Identify and stop individual user abuse with **Transaction Rate Limiting**
   - **SYN-Guard** prevents SYN floods from getting through
   - **Connection Rate Limiting** controls traffic bursts and maintains HA for downstream devices
   - Layer 7 packet inspection for worm and virus detection
2. Firewall load balancing to eliminate bottlenecks to intranet and single point of failure
3. Multiple mirror ports scale IDS stations

https://community.brocade.com/t5/Application-Delivery-ADX/Multi-tiered-Network-based-Application-Service-Security/ta-p/3999

Network-based and tiered solutions approach

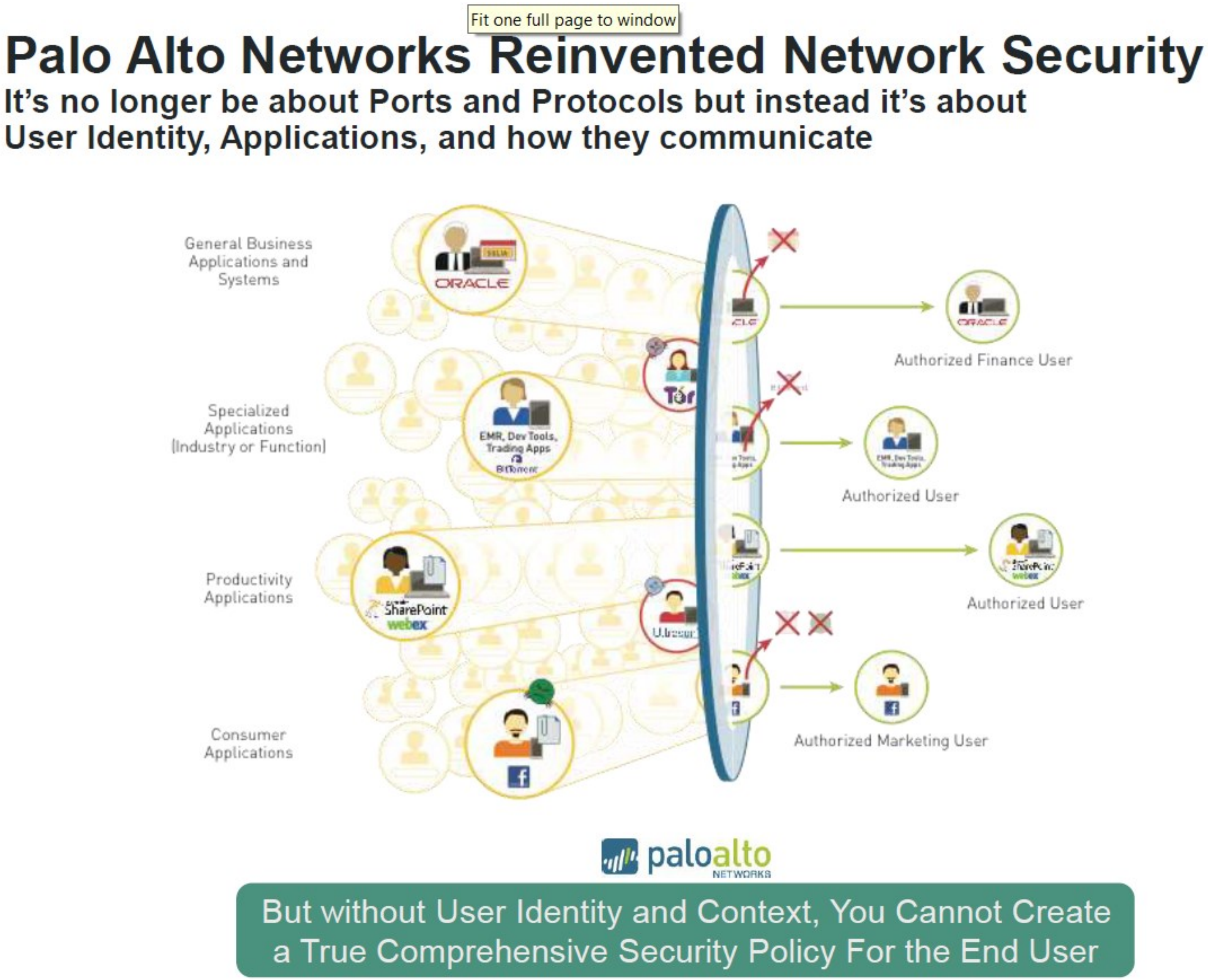


Traditional Firewalls Had Limitations

To be truly effective, you need to see all applications, all user identities and most importantly, all threats

But traditional firewalls only gave you ports, protocols, and IP addresses – missing the malware threat completely

Network-based and tiered solutions approach



Fit one full page to window

Palo Alto Networks Reinvented Network Security

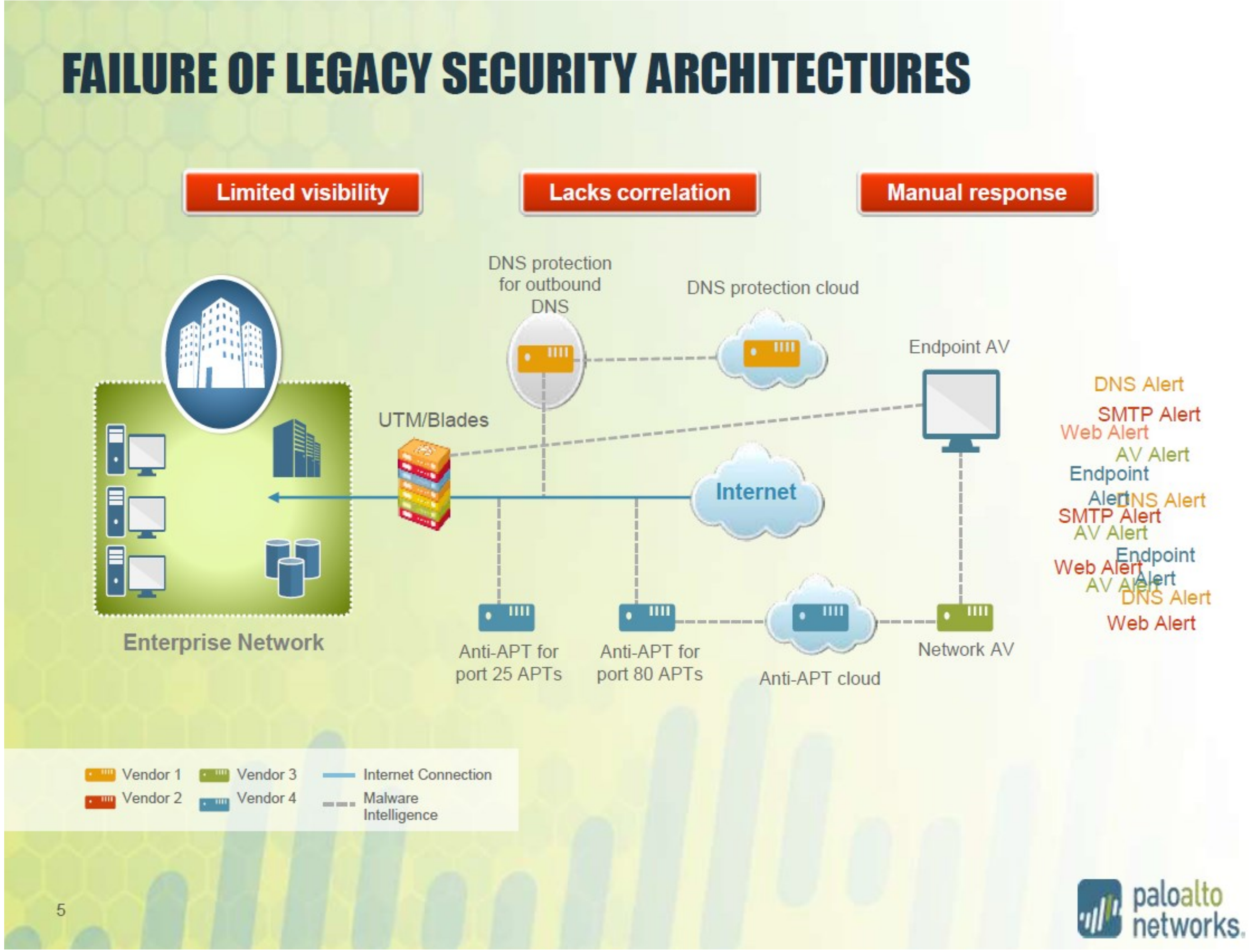
It's no longer be about Ports and Protocols but instead it's about User Identity, Applications, and how they communicate

General Business Applications and Systems
ORACLE
Specialized Applications (Industry or Function)
EMR, Dev Tools, Trading Apps
BitTorrent
Tor
Productivity Applications
SharePoint
webex
Uloader
Consumer Applications
f
Authorized Finance User
Authorized User
Authorized User
Authorized Marketing User
paloalto NETWORKS

But without User Identity and Context, You Cannot Create a True Comprehensive Security Policy For the End User

ITU-D 1992 2017 CELEBRATING 25 YEARS OF ACHIEVEMENTS

Network-based and tiered solutions approach



FAILURE OF LEGACY SECURITY ARCHITECTURES

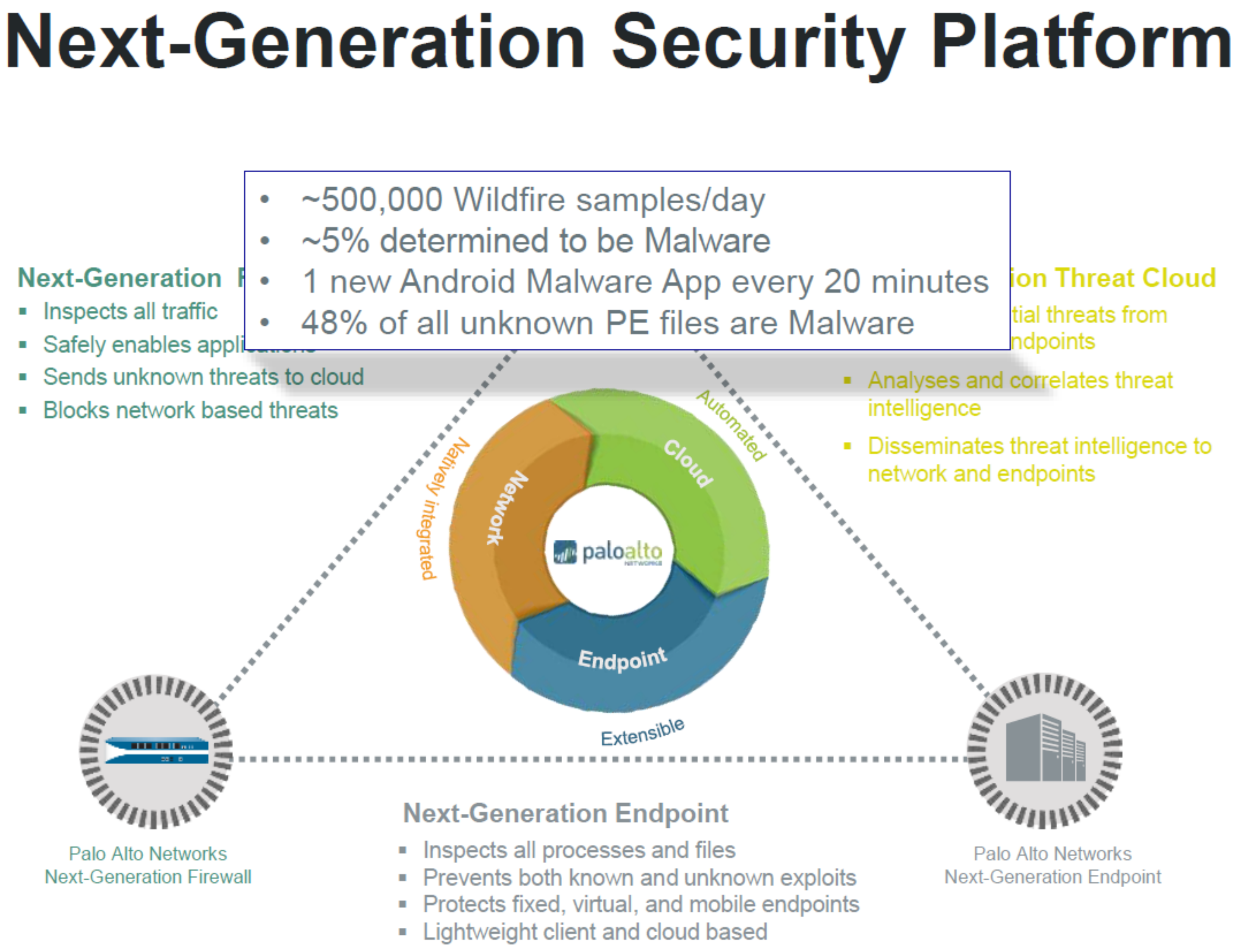
Limited visibility

Lacks correlation

Manual response

Network-based and tiered solutions approach

- ~500,000 Wildfire samples/day
- ~5% determined to be Malware
- 1 new Android Malware App every 20 minutes
- 48% of all unknown PE files are Malware



Next-Generation Security Platform

Next-Generation F

- Inspects all traffic
- Safely enables appl
- Sends unknown threats to cloud
- Blocks network based threats

ion Threat Cloud

- tial threats from ndpoints
- Analyses and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints

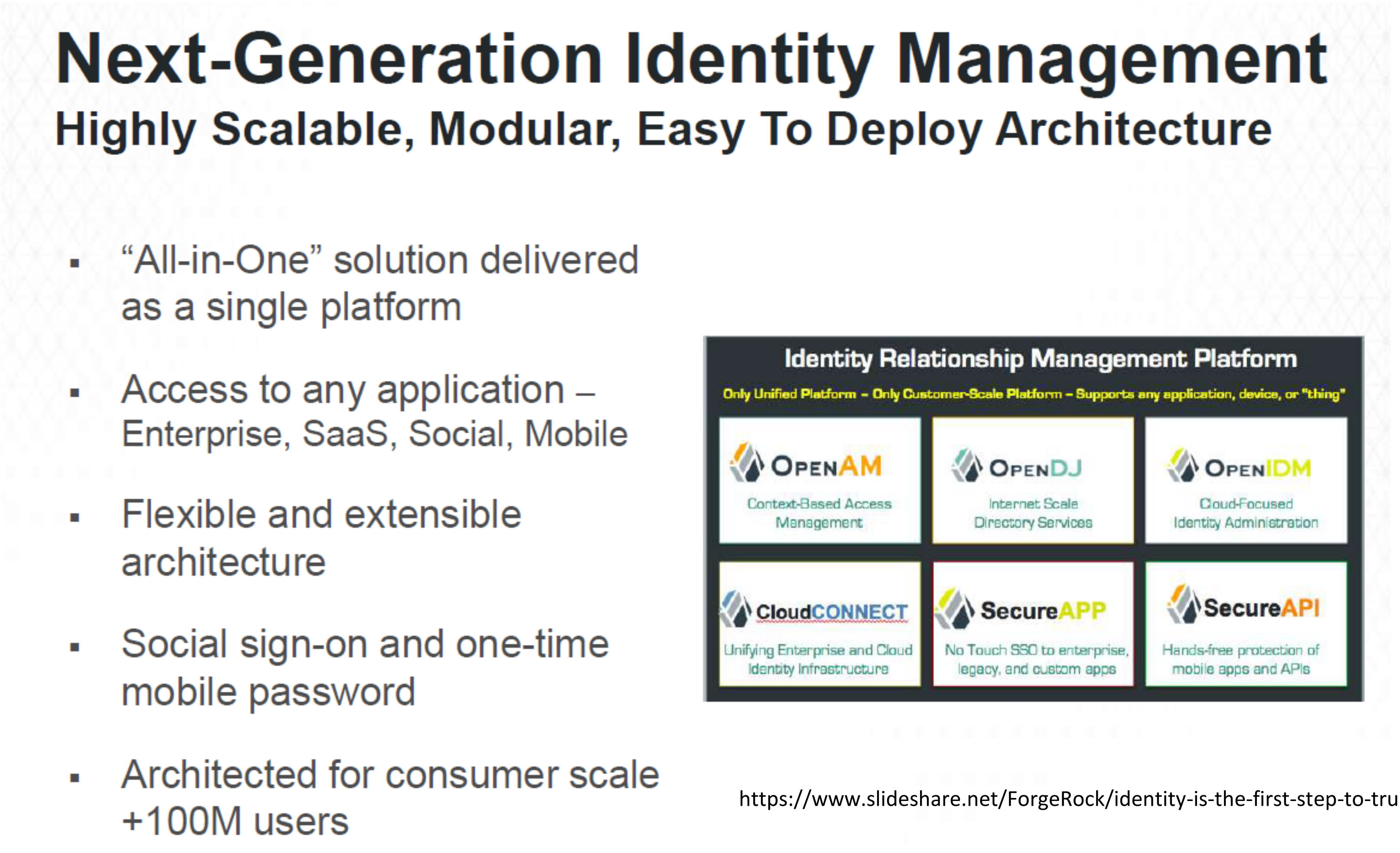
Next-Generation Endpoint

- Inspects all processes and files
- Prevents both known and unknown exploits
- Protects fixed, virtual, and mobile endpoints
- Lightweight client and cloud based

Natively integrated
Automated
Extensible
Network
Cloud
Endpoint
paloalto NETWORKS
Palo Alto Networks Next-Generation Firewall
Palo Alto Networks Next-Generation Endpoint

CELEBRATING 25YEARS OF ACHIEVEMENTS ITU-D 1992 2017

Network-based and tiered solutions approach



Next-Generation Identity Management

Highly Scalable, Modular, Easy To Deploy Architecture

- "All-in-One" solution delivered as a single platform
- Access to any application – Enterprise, SaaS, Social, Mobile
- Flexible and extensible architecture
- Social sign-on and one-time mobile password
- Architected for consumer scale +100M users

Identity Relationship Management Platform

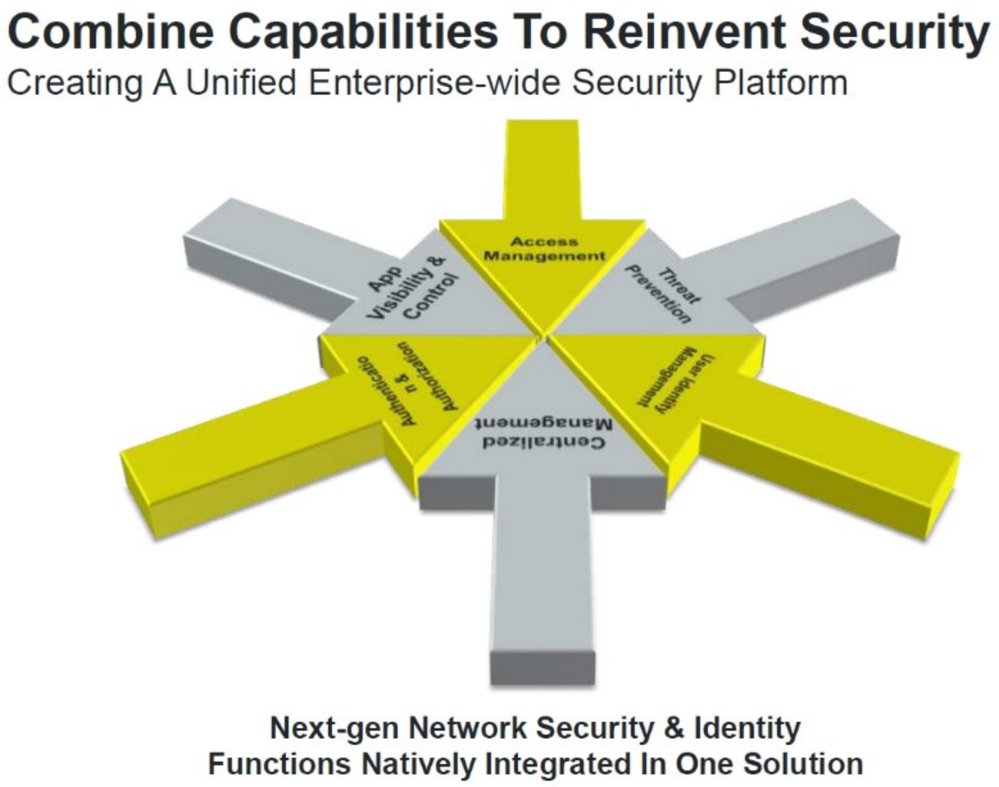
Only Unified Platform – Only Customer-Scale Platform – Supports any application, device, or "thing"

OpenAM Context-Based Access Management	OpenDJ Internet Scale Directory Services	OpenIDM Cloud-Focused Identity Administration
CloudCONNECT Unifying Enterprise and Cloud Identity Infrastructure	SecureAPP No Touch SSO to enterprise, legacy, and custom apps	SecureAPI Hands-free protection of mobile apps and APIs

https://www.slideshare.net/ForgeRock/identity-is-the-first-step-to-true-network-security

Network-based and tiered solutions approach

- Understand more about the user before granting them access to corporate resources
- Create a feedback loop to take appropriate action on both ends:
  - The network blocks traffic when suspicious identity activity occurs
  - The identity platform blocks access when suspicious network activity occurs
  - Real-time, automated remediation of malicious activity
  - Organizations are much, much safer!!!!



Combine Capabilities To Reinvent Security

Creating A Unified Enterprise-wide Security Platform

Next-gen Network Security & Identity Functions Natively Integrated In One Solution

https://www.slideshare.net/ForgeRock/identity-is-the-first-step-to-true-network-security

Adhering to regulatory and industry compliance standards

Some examples of law and regulations on data processing and information security:

- UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.
- The European Union Data Protection Directive (EUDPD) requires that all EU member must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.
- The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland have drawn inspiration when subsequently drafting their own information security laws.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.
- Gramm–Leach–Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.

Adhering to regulatory and industry compliance standards

- **Sarbanes–Oxley Act of 2002 (SOX).** Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.
- **Payment Card Industry Data Security Standard (PCI DSS)** establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- **Personal Information Protection and Electronics Document Act (PIPEDA)** – An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

Adhering to regulatory and industry compliance standards

Information Security Standards

- Cybersecurity standards (also styled cyber security standards)are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization.
- This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.
- The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks. These published materials consist of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies.

Adhering to regulatory and industry compliance standards

- ISO/IEC 27001:2013, part of the growing ISO/IEC 27000 family of standards, is an information security management system (ISMS) standard published in October 2013
- ISO/IEC 27001:2013 formally specifies a management system that is intended to bring information security under explicit management control.
- ISO/IEC 27002 incorporates mainly part 1 of the BS 7799 good security management practice standard.
- ISO 27001 are normative and therefore provide a framework for certification.
- ISO/IEC 27002 is a high level guide to cybersecurity. It is most beneficial as explanatory guidance for the management of an organisation to obtain certification to the ISO 27001 standard. The certification once obtained lasts three years. Depending on the auditing organisation, no or some intermediate audits may be carried out during the three years.
- ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).
- It states the information security systems required to implement ISO 27002 control objectives. Without ISO 27001, ISO 27002 control objectives are ineffective. ISO 27002 controls objectives are incorporated into ISO 27001 in Annex A.

Adhering to regulatory and industry compliance standards

- In the 1990s, the Information Security Forum (ISF) published a comprehensive list of best practices for information security, published as the Standard of Good Practice (SoGP).
- The ISF continues to update the SoGP every two years (with the exception of 2013-2014); the latest version was published in 2016.
- Originally the Standard of Good Practice was a private document available only to ISF members, but the ISF has since made the full document available for sale to the general public.
- Among other programs, the ISF offers its member organizations a comprehensive benchmarking program based on the SoGP. Furthermore, it is important for those in charge of security management to understand and adhere to NERC CIP compliance requirements.

Adhering to regulatory and industry compliance standards

The NIST Cybersecurity Framework (NIST CSF) "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." It is intended to help private sector organizations that provide critical infrastructure with guidance on how to protect it, along with relevant protections for privacy and civil liberties.

- **Special publication 800-12** provides a broad overview of computer security and control areas. It also emphasizes the importance of the security controls and ways to implement them. Initially this document was aimed at the federal government although most practices in this document can be applied to the private sector as well. Specifically it was written for those people in the federal government responsible for handling sensitive systems.
- **Special publication 800-14** describes common security principles that are used. It provides a high level description of what should be incorporated within a computer security policy. It describes what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document. [3]
- **Special publication 800-26** provides advice on how to manage IT security. Superseded by NIST SP 800-53 rev3. This document emphasizes the importance of self assessments as well as risk assessments.
- **Special publication 800-37**, updated in 2010 provides a new risk approach: "Guide for Applying the Risk Management Framework to Federal Information Systems"
- **Special publication 800-53 rev4**, "Security and Privacy Controls for Federal Information Systems and Organizations", Published April 2013 updated to include updates as of January 15, 2014, specifically addresses the 194 security controls that are applied to a system to make it "more secure".
- Special Publication 800-82, Revision 2, "Guide to Industrial Control System (ICS) Security", revised May 2015, describes how to secure multiple types of Industrial Control Systems against cyber attacks while considering the performance, reliability and safety requirements specific to ICS.

Evaluating New Security and Threat Intelligence solutions:

1. **Understand your business mission, requirements and intelligence requirements**
2. **Data Feeds**
   - How many data feeds are available, what platform and file format?
   - How many data source and what are the sources?
3. **Threat Intelligence Report**
   - Does the company provide real time alerts and analyst report?
   - How frequent are the reports generated or summaries issued?
   - Are they industry relevant?
   - Are organisation-specific reports available?
   - Tiered pricing model with number of users?
   - Volume discount offered as numbers increase?
   - Do you have to buy any security devices along with subscription?
5. **Service Provider Support**
   - Do they provide 24/7 support?
   - How fast will they respond to a call?
   - How much is the escalated support call cost?
   - What are the cost and terms of service for incident response?
   - Is training provided as part of the subscription fee?

CELEBRATING 25YEARS OF ACHIEVEMENTS

ITU : I Thank U