

# IBM Services

Cybersecurity solutions from  
IBM and Palo Alto Networks

Protect your critical  
data assets with  
industry-leading technology



## Summary

3 IBM® Technology Support Services and Palo Alto Networks

4 Why IBM and Palo Alto Networks?

For more information

References

- *Helps organizations stay on the cutting edge with continuous integrated security innovations that instantly find and stop attacks*
- *Provides cloud security services that effectively predict, prevent, detect and respond to security and compliance risks*
- *Utilizes an open and integrated AI-based security platform*
- *Delivers a collaborative support model that includes remote and onsite support, cost savings and downtime reduction*



### Industry recognition

IBM was named a Leader in the Gartner 2018 Magic Quadrant for Managed Security Services Worldwide.<sup>1</sup>

Palo Alto Networks was named as an enterprise network firewall market Leader by Gartner seven times in a row.<sup>2</sup>



### Experienced support specialists

IBM support specialists have an average of 14 years of experience, specifically in network, storage, server and cybersecurity technology and Palo Alto has an experienced team of more than 5,000 employees.



### Multivendor support

IBM offers proactive and reactive onsite and remote IT support for over 30,000 IBM and third-party devices, including Palo Alto products.



### Global partnership

Integrated framework of offerings designed to help ensure consistent security across cloud, network endpoints and mobile devices.

## **IBM Technology Support Services and Palo Alto Networks**

In a digital enterprise, outpacing the competition requires quick thinking, as well as agile business and security practices. IT teams are undergoing tremendous change to stay ahead, embracing innovations in the cloud, automation and big data analytics to speed application delivery and enable digital transformation. Meanwhile, the perimeter has expanded—data is becoming increasingly distributed, and users, devices and applications are everywhere. As a result, IT leaders are consistently challenged to minimize risk while keeping pace with evolving business demands.

According to a 2018 study by the Ponemon Institute, 65 percent of organizations said the severity of cyberattacks has increased compared with previous years while 57 percent said the time taken to resolve an incident has increased.<sup>3</sup> In addition, the cost of data breaches is also increasing year on year—the average total cost of a breach in 2018 was USD 3.86 million, 6.4 percent higher than it was in 2017.<sup>4</sup>

If you want to protect your organization from today's advanced cybersecurity attacks, you need to move away from traditional point-product approaches to security. You need a new approach that will help you consolidate your security infrastructure, improve your security posture and reduce your total cost of ownership (TCO), while ensuring your critical assets remain protected at all times.

### **Helps protect data and networks with a robust security platform**

Palo Alto Networks is a full next-generation security operating platform. Unlike traditional disparate stand-alone systems that offer limited control and that are more prone to cyber threats, Palo Alto's platform consists of a tightly integrated system of components and services that delivers consistent security across the network, endpoints and cloud. By working as an integrated system, the Palo Alto Networks Security Platform simplifies security by leveraging consolidated threat intelligence information, automation, machine learning (ML), and data analytics. Additionally, IBM leading security systems, processes, big data resources and support specialists help maintain and expand your security posture around Palo Alto Networks technologies.

### **Embrace the future of cybersecurity**

The Palo Alto Networks® Security Operating Platform prevents successful cyberattacks through data-driven automation and takes advantage of precise analytics to streamline routine tasks, letting security teams move out of firefighting mode and prioritize the threats that really matter to the business. Moreover, the platform lets your organization easily adopt best practices, such as Zero Trust, to reduce opportunities for attack and transform your security to a prevention-based architecture.

Through cloud-delivered services, tight integration and an ecosystem of partners, the Security Operating Platform provides consistent security across clouds, networks and endpoints, including servers and mobile devices.



## Why IBM and Palo Alto Networks?

Palo Alto Networks is a leading provider of cybersecurity solutions, recognized by industry analysts as a leader in the enterprise firewall market. IBM Technology Support Services for Palo Alto Networks products acts as a one-stop shop to help ensure your enterprise continually has the network security, visibility and granular control of all network activity.

## For more information

To learn more about cybersecurity solutions from IBM and Palo Alto Networks, contact your IBM representative or IBM Business Partner, or visit [ibm.com/us-en/marketplace/support-for-palo-alto-products](http://ibm.com/us-en/marketplace/support-for-palo-alto-products)

## References

- 1 “Gartner Magic Quadrant for Managed Security Services, Worldwide.” Gartner. Toby Bussa et al. Published 27 February 2018. ID G00325535
- 2 “Magic Quadrant for Enterprise Network Firewalls.” Gartner. Adams Hils et al. Published 4 October 2018. ID G003379688  

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
- 3 “The Third Annual Study on the Cyber Resilient Organization.” Ponemon Institute, March 2018. [ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=65013965USEN&](http://ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=65013965USEN&)
- 4 “The 2018 Cost of a Data Breach Study.” Ponemon Institute, July 2018. [ibm.com/account/reg/us-en/signup?formid=urx-33316](http://ibm.com/account/reg/us-en/signup?formid=urx-33316)

© Copyright IBM Corporation 2019

IBM Corporation  
New Orchard Road  
Armonk, NY 10504

Produced in the United States of America  
June 2019

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Palo Alto Networks Next-Generation Security Platform is not an IBM product or offering. Palo Alto Networks Next-Generation Security Platform is sold or licensed, as the case may be, to users under Palo Alto Networks terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for Palo Alto Networks Next-Generation Security Platform is the direct responsibility of, and is provided directly to users by, Palo Alto Networks.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



Please Recycle

