paloalto® NETWORKS

The Enterprise Buyer's Guide to IoT Security

5 Must-Haves to Look For in a Best-in-Class IoT Security Solution

Table of Contents

IoT Adoption is Growing in the Enterprise

Companies that successfully integrate the Internet of Things (IoT) into their business models stand to reap huge benefits for their own internal processes, employees and customers.

While some of the most striking benefits of IoT revolve around business process efficiency, productivity, and cost reduction, an increasing number of enterprises are also recognizing IoT as an extraordinary source of intelligence into how their products are really changing the lives of their employees and customers.

This is due to the fact that the true value of enterprise IoT comes from data. Insights derived from IoT-generated data are proving to be invaluable to business decision makers.

More than 30% of all network-connected endpoints are IoT devices at the average enterprise today. Needless to say, these numbers are projected to keep growing—and exclude mobile devices. A report by Gartner predicts adoption of IoT endpoints to soar to 5.81 billion this year.

Sources:

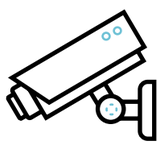
1 - Gartner: Scenarios for the IoT Marketplace, 2019
2, 3, 4 - 451 Research's Voice of the Enterprise: Internet of Things, Budgets and Outlook, 2019

46%
Enterprises already using IoT (including paid pilot projects)[2]

23%
Enterprises in proof of concept with IoT[3]

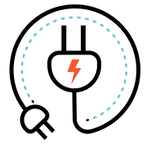
18%
Enterprises planning to deploy IoT in the next two years[4]

ENTERPRISE SEGMENTS WITH HIGHEST USE IN 2020



PHYSICAL SECURITY

1.09B
IoT endpoints in 2020



UTILITIES

1.37B
IoT endpoints in 2020

ENTERPRISE SEGMENTS WITH LARGEST GROWTH IN 2020

42% Building Automation

31% Automotive

29% Healthcare

The transformation opportunity for IoT, IoMT & OT-enabled business models in the enterprise is massive. But to reap the benefits of transformation, enterprises need leading edge security that reliably enables IoT.

But Growth Brings New Security Challenges

The influx of IoT devices in the enterprise poses a new set of challenges, particularly for security teams.

Enterprise security teams are already tasked with protecting IT endpoints connected to the enterprise network. Under the new normal—with the exciting new concept of IoT at the helm—they also have to contend with challenges arising from the increasing prevalence IoT devices connected to an enterprise's central network yet generally unmanaged.

Unique IoT Security Challenges Faced by Enterprise Security Teams

INVENTORY

Not having true understanding of what IoT devices are in the network and how to keep track of new ones

DATA VOLUME

Overseeing vast amounts of data generated from both managed and unmanaged IoT devices

DIVERSITY

The sheer diversity of IoT devices in terms of their limitless forms and functions

THREATS

Lack of well embedded security into IoT device operating systems that are hard or impossible to patch

OWNERSHIP

New risks associated with management of IoT devices by disparate teams within the organization

OPERATIONS

The unification crisis wherein IoT devices are critical to core operations yet difficult for IT to integrate into core security posture

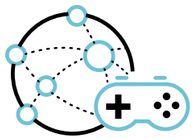
Current Solutions Don't Address These Challenges

Prevailing security mechanisms are not adequate–or effective–when it comes to securing IoT in the enterprise.

A growing number of virtually invisible IoT devices are becoming invariable constituents in enterprise networks. From building and street light sensors, flow monitors, surveillance cameras to IP phones, point-of-sale systems, conference room technology, medical devices, and so much more, IoT, IoMT and OT are on the network and in the organization. These devices significantly expand an organization's attack surface. Prevailing network perimeter defenses are poorly equipped to address the security challenges arising out of this inflow.

Current Solutions That Fall Short

Vulnerability Assessment
for IoT devices are inherently more complicated because of the diversity of hardware, software and communication protocols involved. While helpful to a degree in identifying potential weaknesses, they don't actually solve the problem.



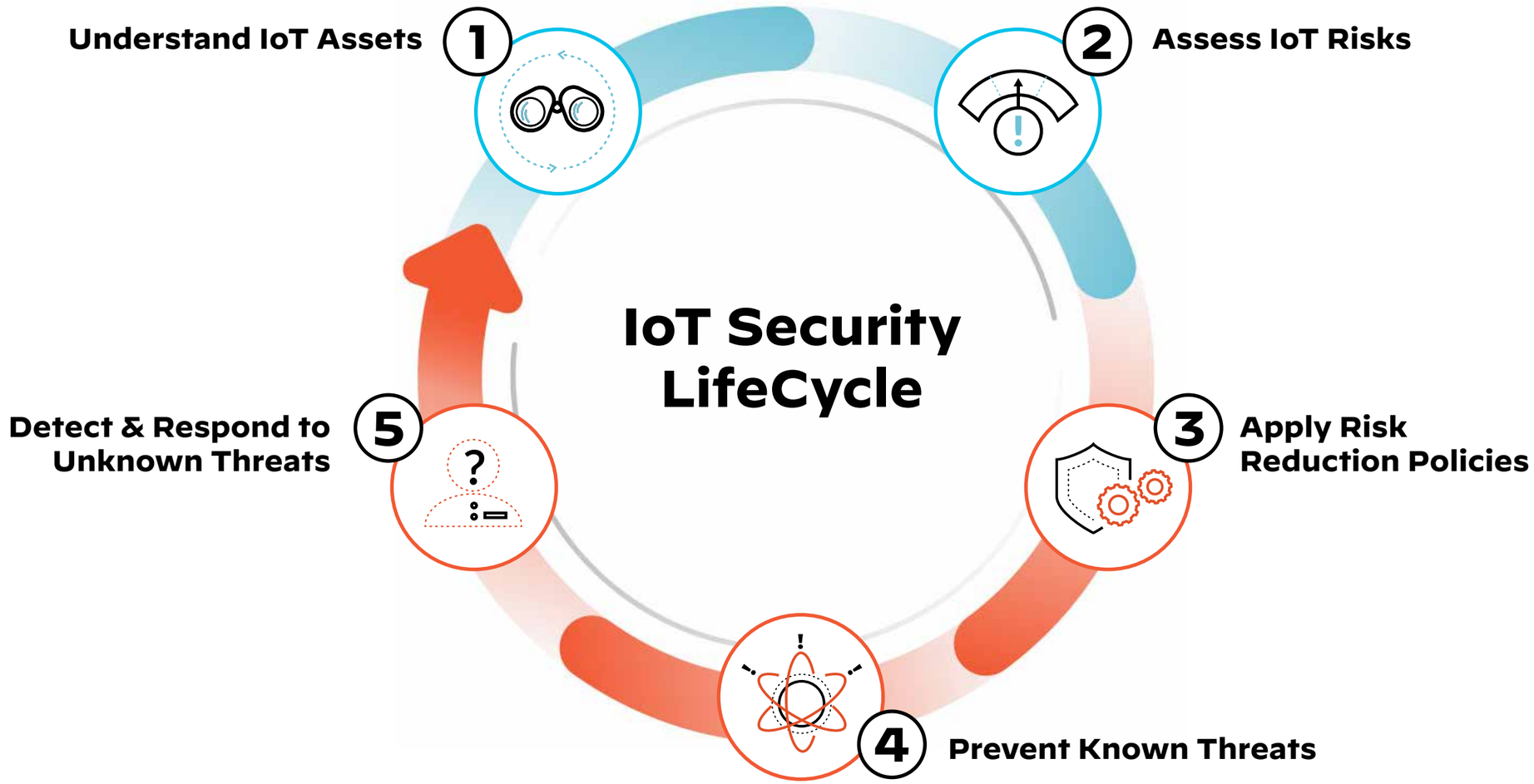
NAC or Network Access Control
solutions and methodologies just don't scale well for the IoT. They lack the sophistication required to identify and provide adequate security to IoT devices in the context of today's threat landscape and can merely be used for enforcement only after an issue is identified.

Point Solutions for IoT Security
equire too much effort for security teams—implementing single purpose sensors, integrating with existing systems and enduring a high learning curve.

CISOs must consider a "lifecycle approach" to level up their IoT security strategy.

Take a Lifecycle Approach to Address Challenges

The concept of a lifecycle approach is critical to securing the IoT, IoMT and OT devices. An ideal IoT security solution seamlessly integrates all stages of the IoT lifecycle—from discovery of IoT devices and their associated risks to security actions that enforce protections and defend these devices from known and unknown threats.



To implement the IoT Security lifecycle, look for *5 must-haves* in your *IoT security solution.*

Your IoT Security Solution Must Provide

1

Complete visibility into all IoT devices connected to the enterprise

Before deciding on a security posture, you must have full visibility into your IoT attack surface. Your IoT security lifecycle begins here. To **understand your IoT assets,** employ device discovery for complete visibility. Your IoT security solution should be able to discover the exact number of devices connected to your network, including the ones you are aware and not aware of—and those forgotten. This discovery helps collect an up-to-date inventory of all IoT assets. Apart from this, the solution should surface essential device attributes to provide full context on each device.

Decide on a solution that:

- ✓ Leverages multipurpose sensors that integrate into existing infrastructure.
- ✓ Delivers essential IoT device attributes such as device make, model, operating system, firmware, ports, applications, VLAN, subnet, presence and status of anti-virus software etc.
- ✓ Detects new, never-seen-before devices without reliance on human support or constant update of signatures.
- ✓ Performs detection of newly plugged-in devices within minutes.
- ✓ Identifies at least 90% of devices in visible segments within 48 hours.
- ✓ Differentiates unmanaged IoT, IoMT and OT devices from managed IT assets.
- ✓ Logs a tally of IT devices allowing desktop security teams to also identify unmanaged IT devices.

Your IoT Security Solution Must Provide

2

Proactive monitoring of IoT devices to continually detect risky behavior

To fulfill the requirements of the **IoT risk assessment** stage in the IoT security lifecycle, your solution must actively monitor IoT devices at all times. Real-time monitoring, reporting, and alerting are crucial for organizations to manage IoT risks. Traditional endpoint solutions cannot protect IoT assets since they require software agents that IoT devices are not designed to take. Assessing risk in your IoT security lifecycle lets you take a better approach. Implement a real-time monitoring solution that continuously analyzes the behavior of all your network-connected IoT devices to contextually segment your network for granular control over lateral movement of traffic between your IT and IoT devices—and their workloads.

Make sure the solution:

- ✓ Integrates with multiple threat feeds to accurately map vulnerabilities with the IoT inventory.
- ✓ Detects and reports anomalies in IoT device behavioral changes that may lead to risk changes.
- ✓ Tracks changes to IoT device risk and keeps complete device risk history for compliance.
- ✓ Calculates risk scores on IoT devices and device categories to report.
- ✓ Integrates with vulnerability management systems for centralized IoT risk management.
- ✓ Integrates with IoT device vendors to deliver information to security teams.
- ✓ Includes Manufacturer Disclosure Statement for Medical Device Security (MDS2) information like antivirus capabilities, ePHI, FDA recalls, and vendor patching information for healthcare delivery organizations.

Your IoT Security Solution Must Provide

3

Automated risk-based security policy recommendations and enforcement

Your IoT security solution must be easy to deploy without the need for any additional infrastructure or investment from your side. Look for a solution that leverages your existing firewall investment for comprehensive and integrated security posturing. Running in conjunction with the capabilities of your firewall, the solution must **automatically recommend and natively enforce security policies** based on the level of risk and the extent of untrusted behavior detected in your IoT devices.

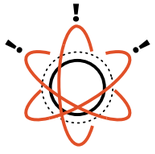
Taking into account that trust is nothing but a vulnerability, your IoT solution must directly align with the principle of zero-trust to enforce policies for least-privileged access control. This significantly reduces the pathways for adversaries, whether they are inside or outside your organization, to access your critical IoT assets.

Verify whether the solution:

- ✓ Automatically converts IoT device behaviors into policies to only allow trusted behaviors.
- ✓ Allows multi-tier policy enforcement for a group of devices.
- ✓ Supports both allow lists and block lists.
- ✓ Track devices and applications to enforce policies regardless of where they reside within the network.
- ✓ Update policies automatically once set to limit manual updates every time a change occurs.

Your IoT Security Solution Must Provide

4



Swift action on preventing known threats

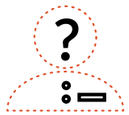
The diverse nature of IoT devices creates a highly distributed environment in your network with numerous points of compromise. Successful outcomes of your security posturing in stage four of the IoT security lifecycle will require actionable insights into **detection and prevention of known threats** to your IoT devices for a swift response to threat mitigation. Look for a threat prevention mechanism that uses payload-based signatures to block advanced threats on your IoT devices. This will ensure the most up-to-date security posture and defense against known threats for rapid, real-time responsiveness to anomalous IoT device vulnerabilities, weaknesses across your network and importantly doesn't overburden security teams with detection alerts that could be stopped—saving time and heartache.

Check to see if the solution:

- ✓ Selectively enables security threat protections based on the IoT device group's risk posture.
- ✓ Detects and prevents known threats from IoT malware, spyware, exploits.
- ✓ Blocks IoT attacks stemming from bad URLs and malicious websites.
- ✓ Prevents IoT attacks that use DNS for command and control and data theft.
- ✓ Prohibits unknown IoT threats delivered via payloads.

Your IoT Security Solution Must Provide

5



Fast detection and rapid response to unknown threats

When it comes to **detecting and preventing truly unknown threats,** legacy approaches isolate threat data each organization receives and generates, creating silos and reducing the possibility of prevention. To meet the requirements of the last step in the IoT security lifecycle, your IoT security solution should be capable of leveraging a new approach, drawing from a collective threat intelligence engine that delivers real-time malware analysis and protections from zero-day attacks to your IoT devices. Tapping into crowdsourced data from a global community of subscribers not only provides collective immunity but also saves your IT security team valuable time by leveraging IoT identity information, risk scores, vulnerability data, and behavioral analytics to investigate never-heard-before threats unique to your IoT environment right from the outset. This last step will also uncover potential threats missed in earlier stages and leads you into a cyclical process for continual improvement.

Also make sure the solution:

- ✓ Detects abnormal behaviors at different tiers—first at the device category level, then at the device vendor/model level, and last at the device instance level.
- ✓ Leverages crowdsourcing intelligence using machine learning enhanced with threat modeling to detect unknown threats or attacks and provide proactive notifications or actions.
- ✓ Integrates into ITSM, SIEM, NAC and SOAR using a playbook-based approach to orchestrate actions.
- ✓ Streamlines with active IoT security researchers to discover any new IoT threats.

IoT Security by Palo Alto Networks

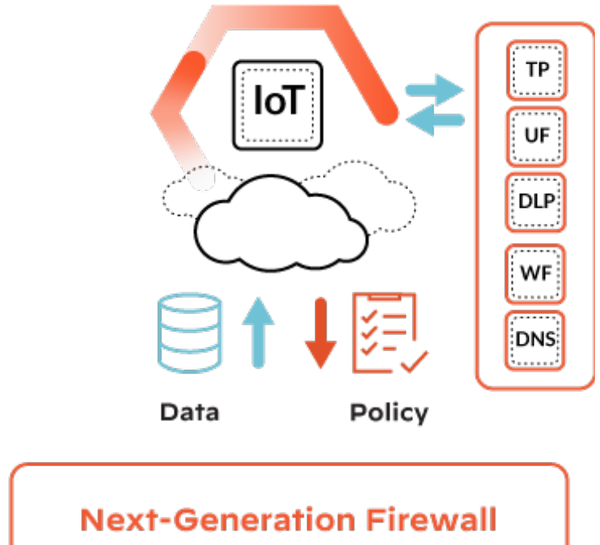
Offers all five must haves

IoT security is the only solution to use machine learning with our leading App-ID technology and crowdsourcing telemetry to quickly and accurately discover all seen and never seen before devices, assess risk, detect anomalies, and provide automatic policy recommendations.

As the only single-platform solution available in the market today, IoT Security delivers native enforcement while seamlessly integrating into your workflows, reducing cost and complexity. With built-in prevention, instead of an alert-only approach, our cloud-delivered security services are seamlessly integrated with IoT Security to keep IoT devices safe with inline protection. Stopping known and unknown file-based threats **(WildFire)**, vulnerabilities **(Threat Prevention)**, and malicious web activity **(URL Filtering** and **DNS Security)**, saves network and security teams countless hours in alert triage and manual response.

Deploying IoT Security is easy—and does not require any single purpose sensors as a cloud-delivered service natively integrated with our ML-Powered Next-Generation Firewall. As an existing customer, simply enable the service on your Palo Alto Networks ML-Powered Next-Generation Firewall to extend leading-edge protections to your previously unmanaged IoT, IoMT and OT assets. For potential customers, we eliminate the need to purchase, integrate, and maintain multiple point products or change your operational processes to get IoT security.

Our ML-powered Next-Generation Firewall can simply be used as a sensor for the IoT Security service, providing you the flexibility to implement best-in-class prevention and enforcement within a single platform, or integrating into existing processes and technologies.



Supports 3rd-Party Integrations

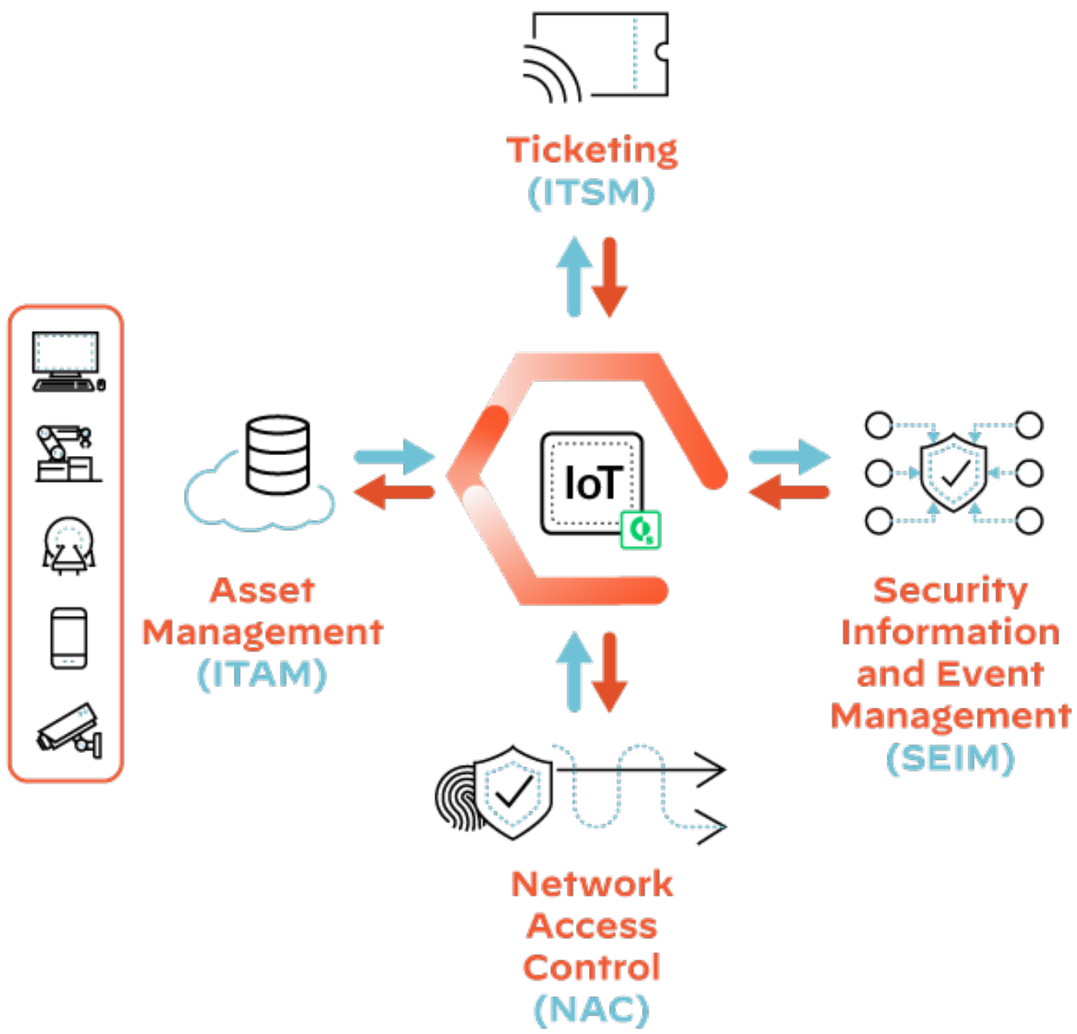
Powered by Built-in XSOAR Technology

Seamlessly integrate into your existing workflows and avoid resource intensive API led integrations, reducing the burden on infrastructure and security teams.

Leverage native integrations into your existing IT and security workflows to strengthen your current

- IT Asset Management (ITAM)
- IT Service Management (ITSM)
- Network Access Control (NAC)
- Security Information and Event Management (SIEM)
- and other use cases.

Our modular and customized playbook-driven orchestration lets your security team improve operational inefficiencies, enrich asset inventories, accurately onboard IoMT devices, enforce network controls and automate incident responses without having to build integrations from scratch.



Extend Benefits to Your Existing Security Team

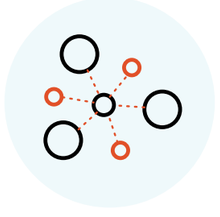
Without the need to form a new team, deploy new infrastructure or change existing operational processes

Unprecedented Visibility and Protection

- ML-Based IoT Device Discovery
- Automated Risk Assessment
- Native Security Policy Enforcement
- Context-Aware Network Segmentation

Easy Deployment with Flexible Form Factor Options

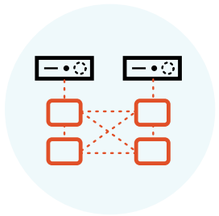
- Hardware PA-Series Firewall Appliances
- Virtualized VM-Series Firewalls
- Cloud-delivered Prisma Access SASE



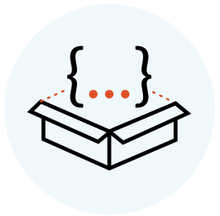
Full Range of IoT, IoMT & OT Device Coverage

- Enterprise and Consumer IoT Devices
- IoMT Devices
- Mission Critical OT Devices
- Legacy Unmanaged Systems

Get enhanced security with advanced threat prevention security subscriptions



Scale linearly as your business grows with elastic cloud infrastructure



Leverage a rich set of 3rd-Party integrations for use cases such as ITAM, ITSM, NAC and SIEM

Think IoT Security.
Think Palo Alto Networks.

At Palo Alto Networks our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We are at the forefront of protecting tens of thousands of organizations across clouds, networks, and devices and help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

Founded in 2005, Palo Alto Networks is based in Santa Clara, California, and serves customers globally with offices worldwide.

For more information, visit: www.paloaltonetworks.com

See what our customer had to say

> *"Within hours of deployment, we discovered and identified thousands of devices, including a few, that gave us critical insight allowing us to take action and implement preventive measures."*

BayCare Medical Group

Curious to learn more? **Watch the Product Demo**

www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

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