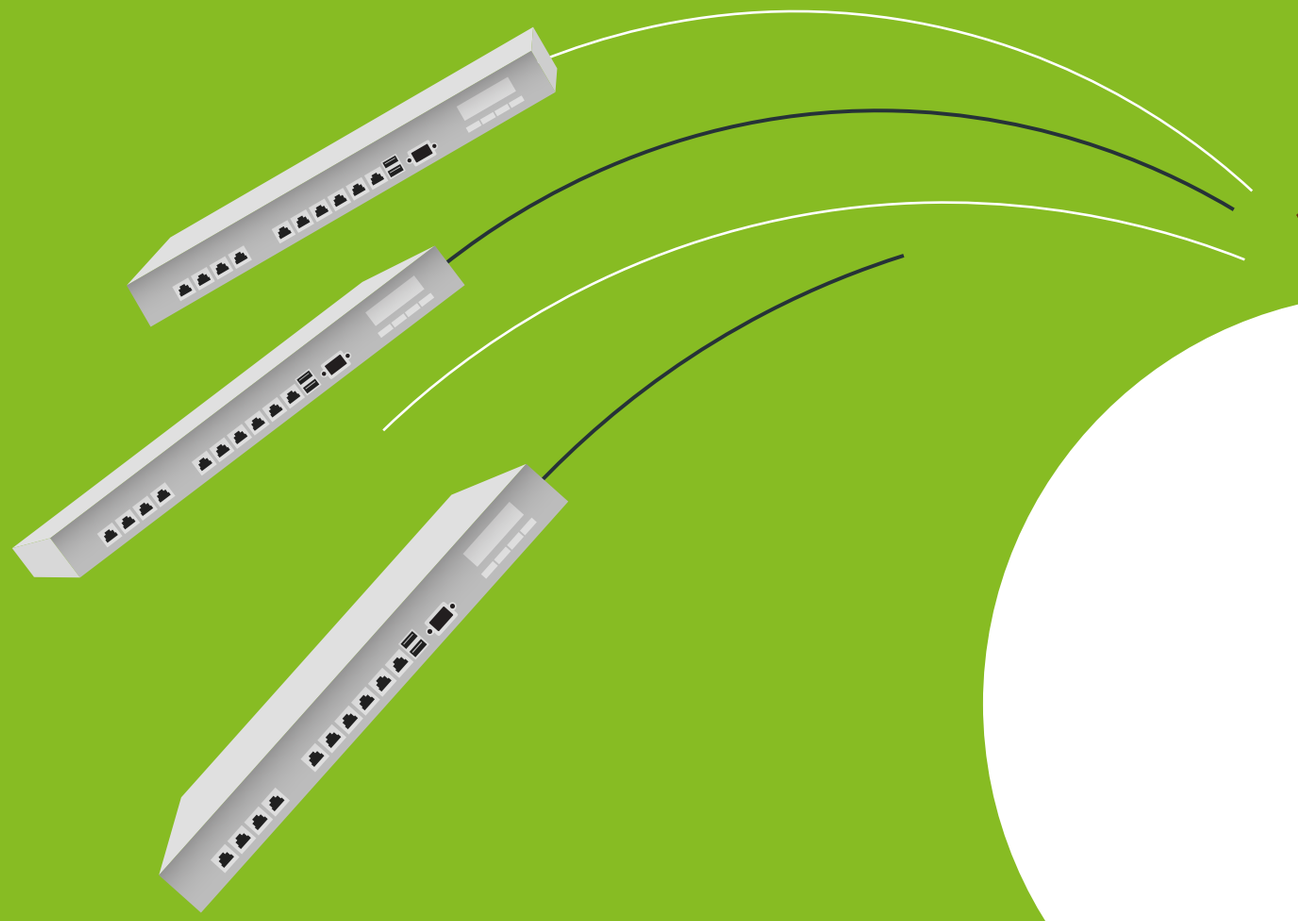
Switching Firewall Vendors?

Drop the Box!

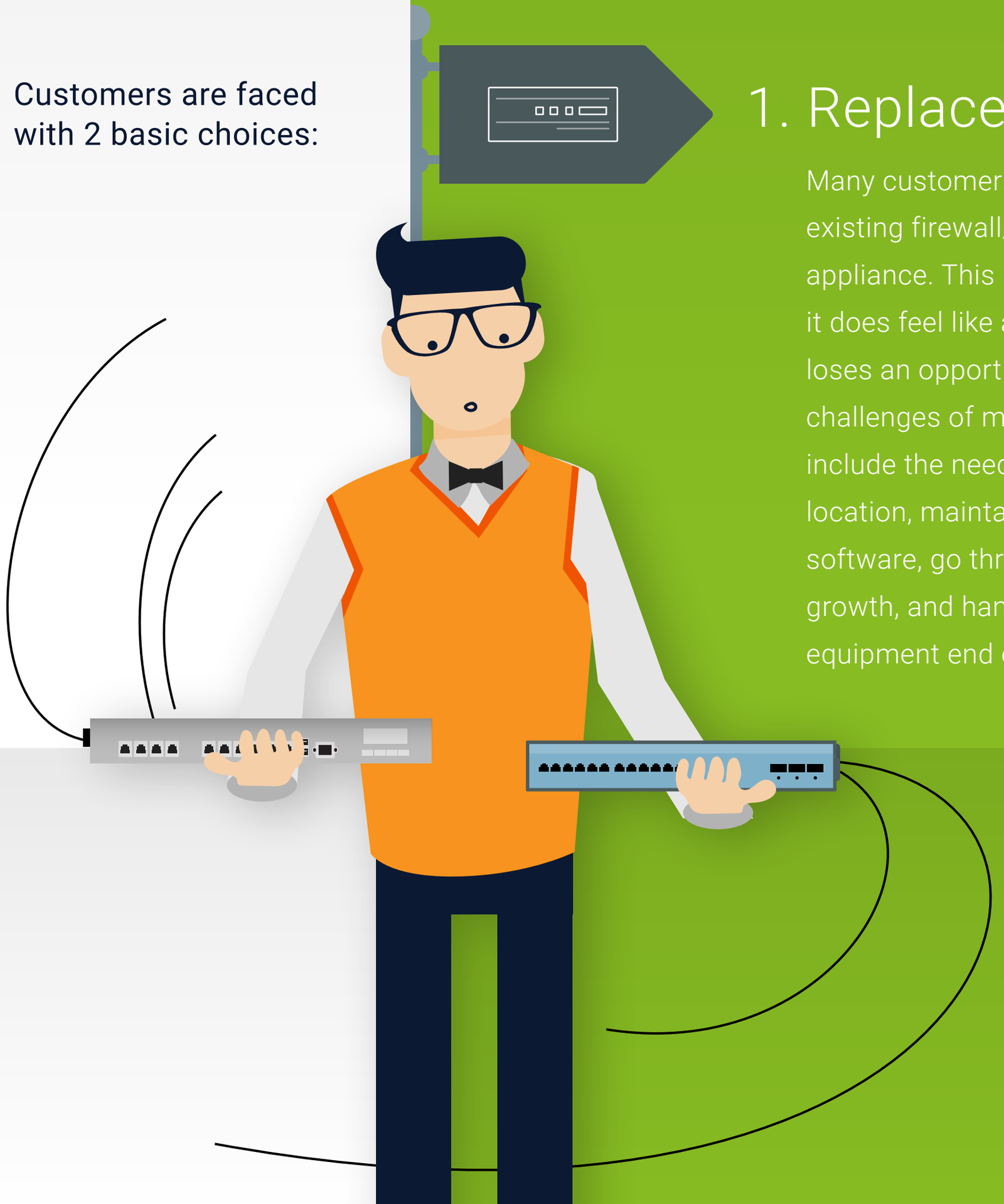


CATO
NETWORKS

Organizations often arrive at a crossroad when they need to re-evaluate their existing firewall vendors. This can be a result of pending hardware refresh, budget constraints, product limitations, etc.

A more strategic driver is the state of the vendor's product roadmap and divestiture decisions that create doubts about the future direction and viability of vendor's software and hardware.

Customers are faced with 2 basic choices:



1. Replace a Box for a Box

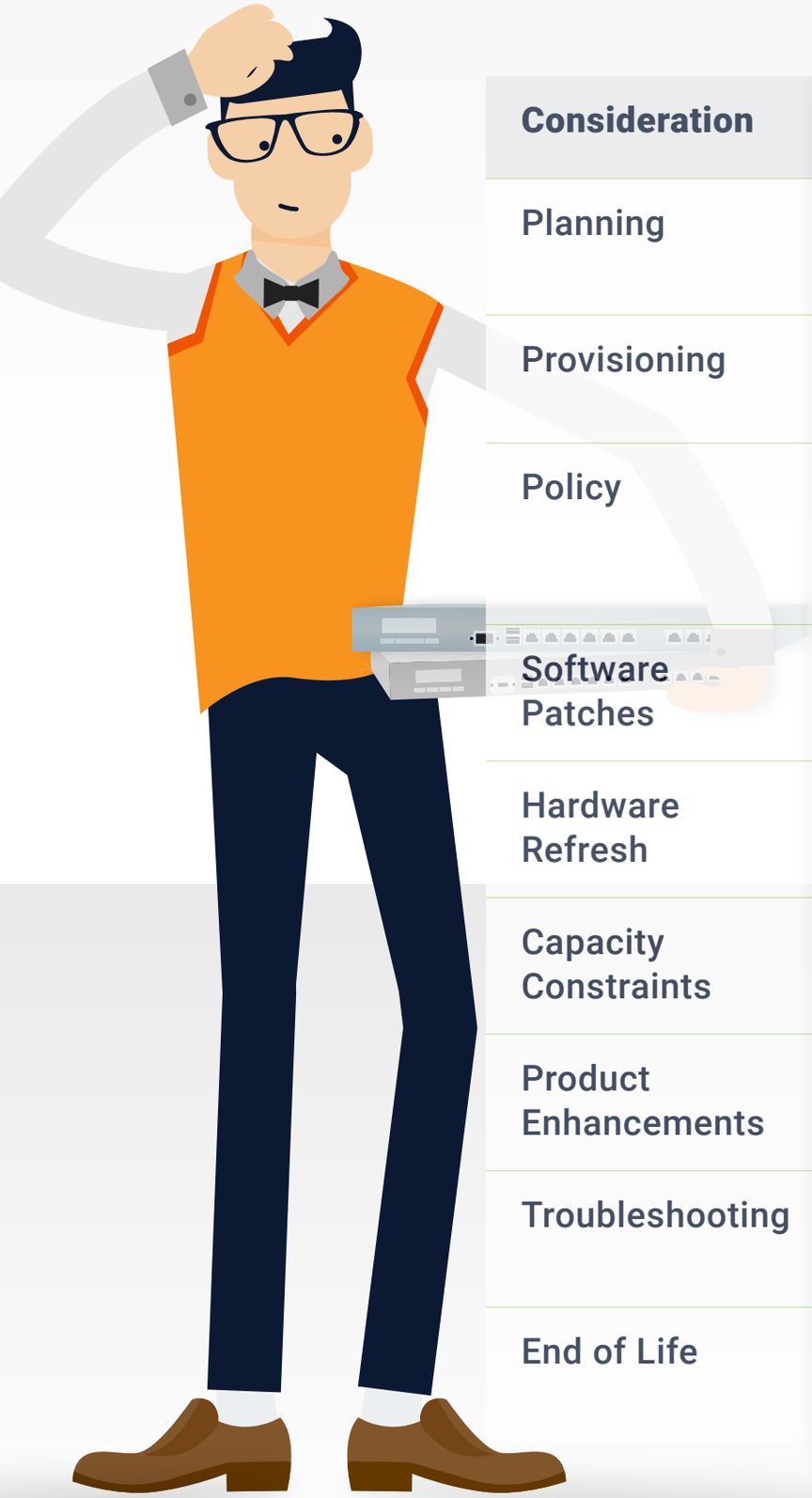
Many customers would consider replacing their existing firewall/UTM appliance with another vendor's appliance. This is a long and complicated process but it does feel like a safe choice. However, the customer loses an opportunity to address the long standing challenges of maintaining firewall appliances. These include the need to do capacity planning for each location, maintaining the hardware and patching the software, go through forced upgrades due to business growth, and handling new security requirements and equipment end of life.

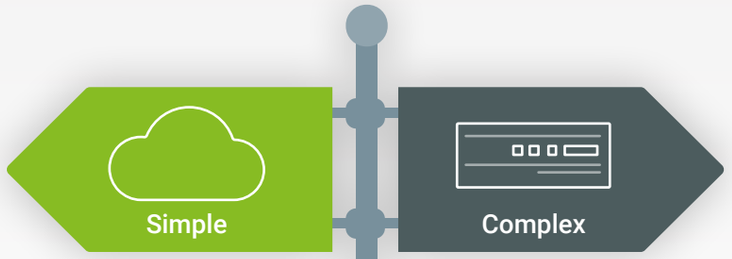
SOPHOS JUNIPER FORTINET Barracuda SonicWALL WatchGuard

2. Drop the box, and replace it with a Firewall as a Service solution (FWaaS)

FWaaS was recently recognized by Gartner as a high impact emerging technology in infrastructure protection. It presents a new opportunity to reduce cost and complexity, and deliver a better overall security for the business. The essence of FWaaS solution is to provide a full network security stack in the cloud by eliminating the care and feeding associated with distributed network security appliances. FWaaS can scale to handle any business traffic, and seamlessly upgrade with new capabilities and countermeasures to take complexity off IT's plate. FWaaS simplifies the way organizations connect and protect their data centers, remote branches, cloud infrastructure and mobile users.

Is FWaaS right for you?





Consideration	Firewall-as-a-Service (FWaaS)	Firewall/UTM Appliance
Planning	Cloud service secures all the traffic that comes through with all licensed services	Complex Requires understanding of traffic shape and service impact on performance
Provisioning	Plug & play, sites provision automatically	Requires skilled staff to support each site
Policy	Single policy centrally managed for all sites and mobile users	Requires understanding of your network topology to make sure traffic is not blocked at source or destination
Software Patches	None, seamlessly done by the cloud service	Periodic maintenance windows are required with downtime risk
Hardware Refresh	Never, hardware included with the service	End of life, capacity or functional constraints
Capacity Constraints	No constraints, cloud service seamlessly scales to support any capacity	Limited by the appliance physical capacity and active services
Product Enhancements	New features are immediately accessible upon release	Limited by the appliance capacity and version, long time to apply
Troubleshooting	Single pane of glass	Both hardware and software can cause issues
End of Life	Never	3-5 years

About Cato Networks

Cato Networks provides organizations with a cloud-based and secure global SD-WAN. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people, and data. Cato Cloud cuts MPLS costs, improves performance between global locations and to cloud applications, eliminates branch appliances, provides secure Internet access everywhere, and seamlessly integrates mobile users and cloud datacenters into the WAN.

Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, co-founder of Check Point Software Technologies and Imperva, and Gur Shatz, co-founder of Incapsula.

Global Backbone. Cloud-Based SD-WAN. Firewall as a Service. All in One

For more information:

www.CatoNetworks.com

@CatoNetworks