



INTRODUCING QUANTUM TITAN

PREVENTION | IOT SECURITY | MANAGEMENT | PERFORMANCE

**AI Deep Learning Threat Prevention
against DNS, Phishing, and IoT attacks**

New Quantum Cyber Security Platform, version R81.20



YOU DESERVE THE BEST SECURITY

Network Security Challenges

88% of organizations had **DNS attacks**

90% of data breaches due to **Phishing attacks**

More than **1B IoT attacks**

AI prevention, Automation, and Scale
are required to keep up with a fast-evolving threat landscape



IT'S TIME TO REBOOT NETWORK SECURITY




Check Point Infinity: Best Security, Consolidated Architecture

NEW


QUANTUM
Secure the network



CLOUDGUARD
Secure the cloud



HARMONY
Secure users & access



HORIZON
Unified management & security operations

THREATCLOUD

Quantum Titan - The Network Security You Need

3 New Software Blades – AI & Deep Learning

New advanced DNS Security

New Zero-Day Phishing Prevention

New IoT Autonomous Threat Prevention

3X speed boost for large file transfers

Improvements for Network Operations

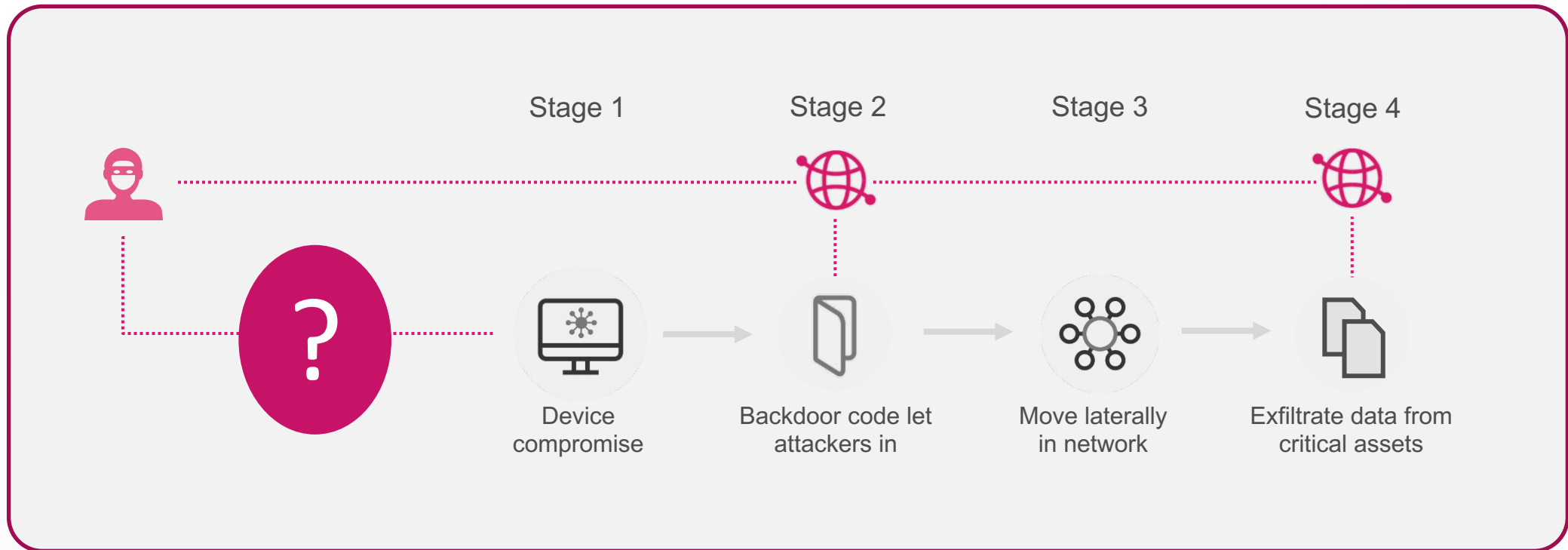
The logo features a stylized atom symbol with three overlapping lobes in shades of purple, pink, and yellow. Below the symbol, the text 'Quantum Cyber Security Platform' is written in a sans-serif font, with 'Quantum' in orange and 'Cyber Security Platform' in dark grey. Underneath that, 'Titan release' is written in orange. The entire logo is centered within a large, white, circular shape that has an orange border and is set against a background of overlapping orange circles.

Quantum
Cyber Security Platform
Titan release

DEEP LEARNING THREAT PREVENTION

```
mirror_mod.use_y = True
mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True
    #selection at the end of MIRROR_Z back the deselection
    mirror_ob.select=1
    modifier_ob.select=1
    bpy.context.scene.objects.active = modifier_ob
    print("Selected object (modifier_ob)")
except:
    #one = 1 / 0
    #copy.data, object
    mirror_mod = modifier_ob.modifiers[0]
    if selected_objec+ +
```

SOPHISTICATED ATTACK FLOW IN A NUTSHELL



Average cost and frequency of data breaches by initial attack vector

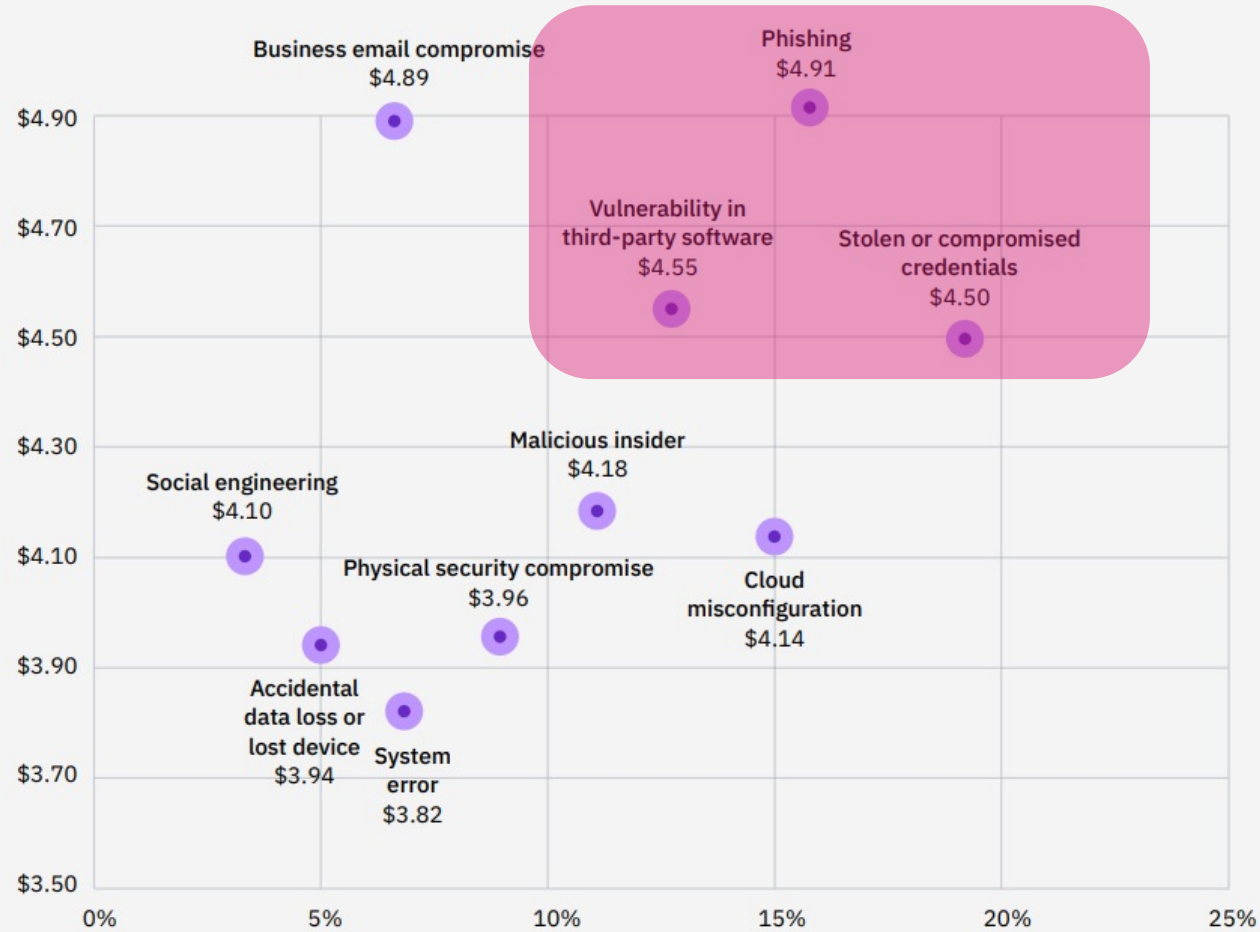
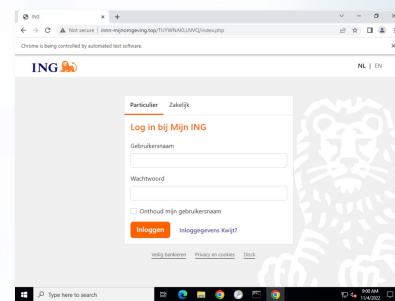
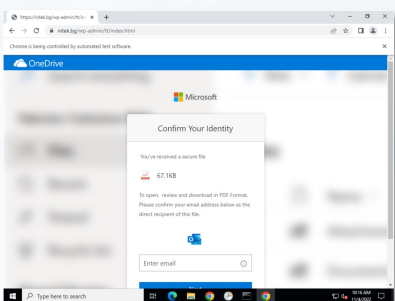
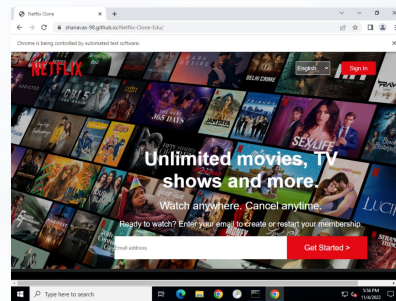
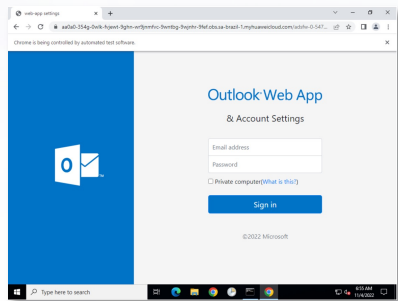
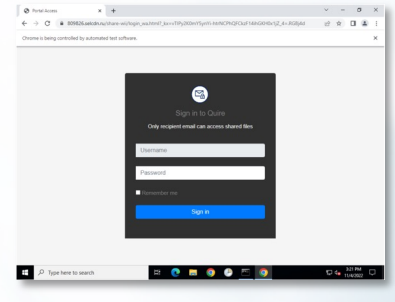
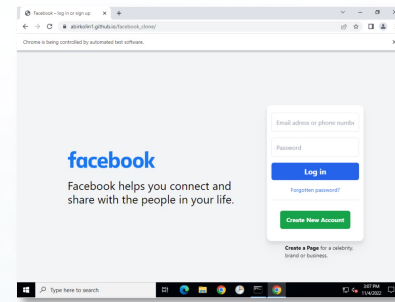
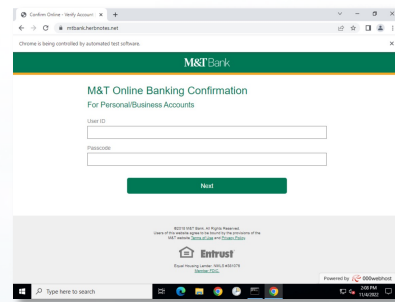
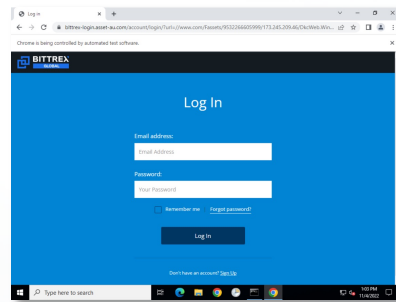
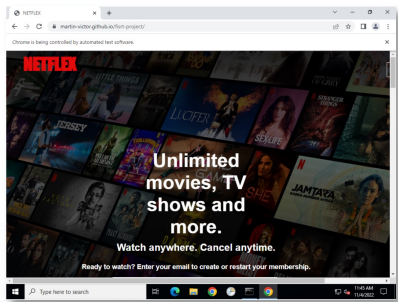
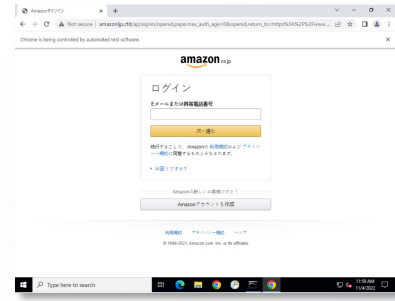
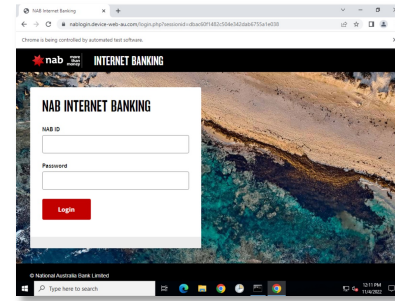
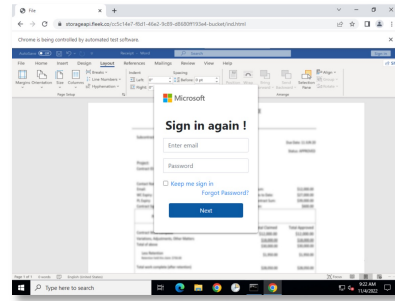
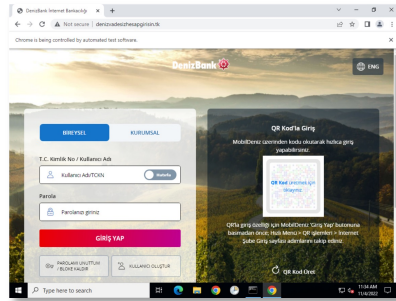
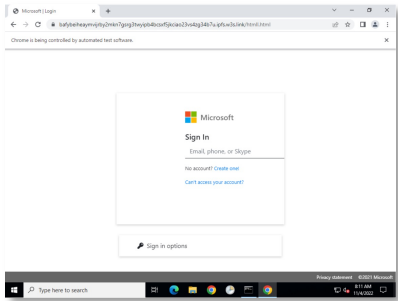


Figure 11: Measured in USD millions

Source: [Ponemon](#), Aug'22

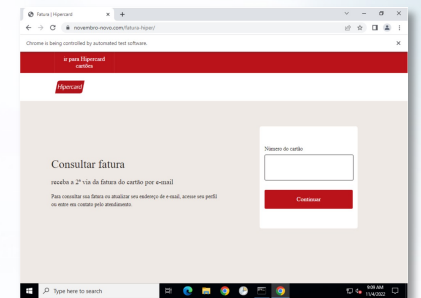
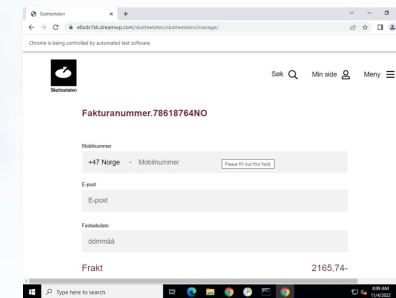
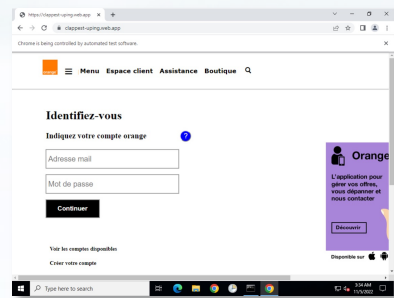
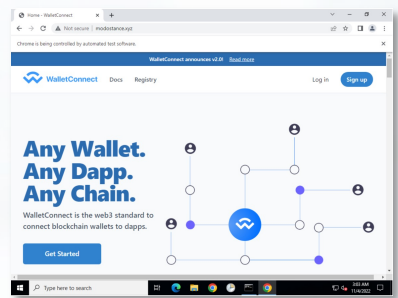
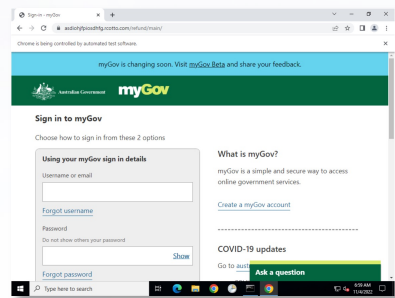
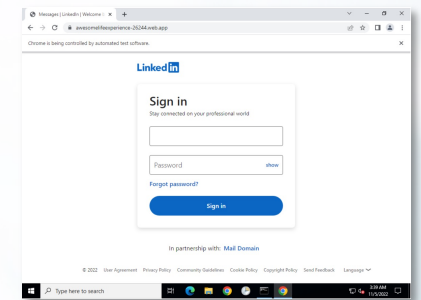
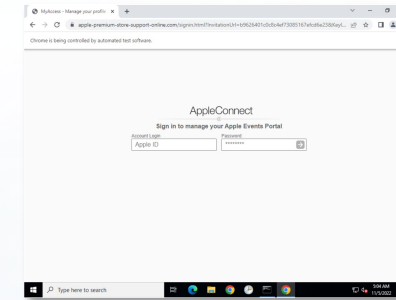
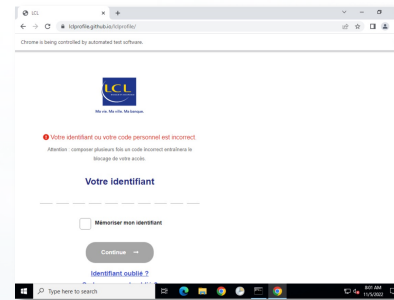
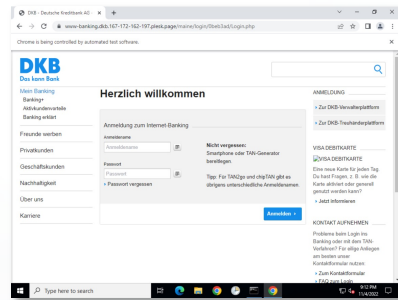
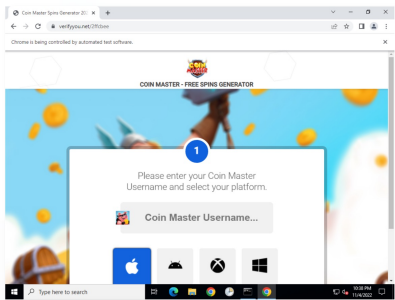
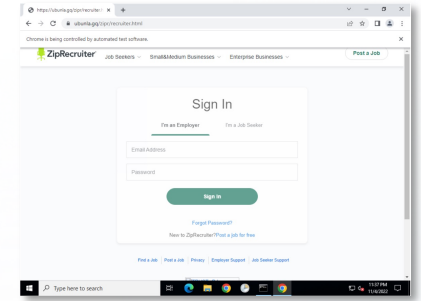
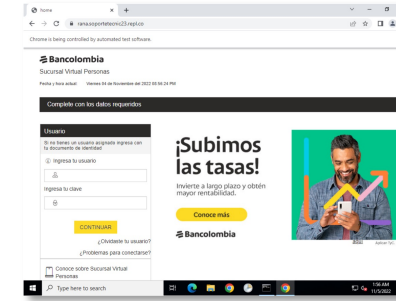
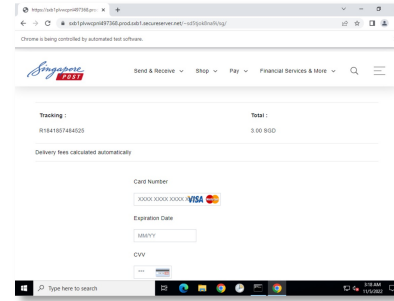
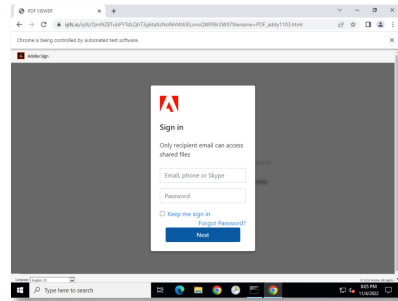
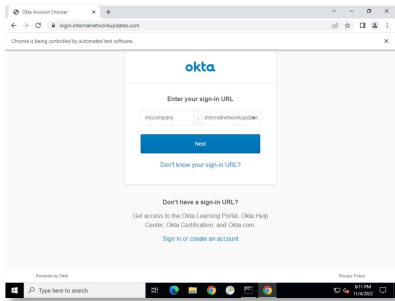
PHISHING, PHISHING, AND SOME MORE PHISHING...

Samples from a period of 72 hours



PHISHING, PHISHING, AND SOME MORE PHISHING...

Samples from a period of 72 hours



The Danger of **Zero-Day** Phishing Websites

Phishing attacks become more sophisticated

- Targeted and customized
- Time triggered
- Enormous scale

Traditional Solutions are not enough

- Classic reputation services are static and can be easily bypassed to launch attacks

62%

Open **custom**
phishing messages

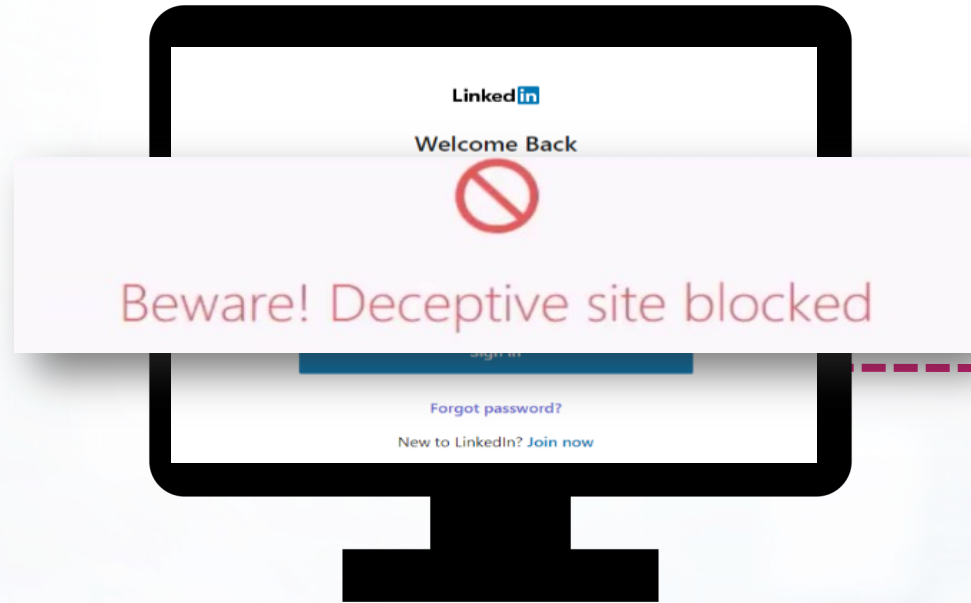
Introducing: Zero-Day Phishing Software Blade

Blocks 4X more Zero-Day Phishing than Signature based solutions

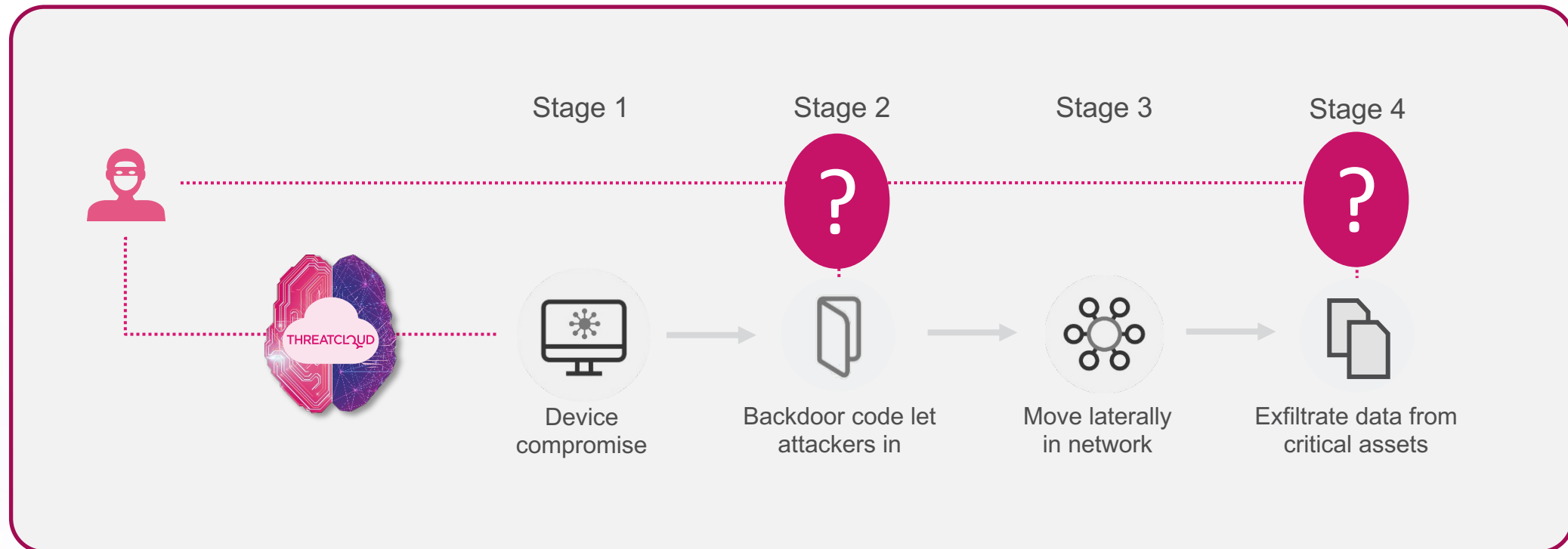
Real time scanning and AI engines prevent zero-phishing threats



Quantum Security Gateway



SOPHISTICATED ATTACK FLOW IN A NUTSHELL



DNS is not secure!

Attackers abuse **DNS** protocol to:

- Communicate with Command & Control new domains
- Exfiltrate data over DNS (tunneling)

Traditional Solutions are **not** enough

- Classic reputation services can't catch up with millions of new generated domains every second



DNS

Introducing: advanced DNS Security Software Blade

Blocks 5X more Zero-DNS attacks than signature based technologies



Best Security with most innovative AI and Deep Learning Technologies

Zero-Day Phishing New Software Blade

4X

More attacks blocked compared
to **Signature** based technologies

40%

Zero-phishing attacks **MISSED** by
other **AI** based technologies

advanced DNS Security New Software Blade

5X

More attacks blocked compared
to **Signature** based technologies

47%

Zero-DNS attacks **MISSED** by
other **AI** based technologies

Two new software blades

Next Generation Firewall (NGFW)

Firewall
VPN
Application-Control

3 Blades

Next Generation Threat Prevention (NGTP)

Next Generation Firewall +
IPS
Anti Virus
Anti Bot
URL Filtering
Anti Spam
Advanced DNS Security ★

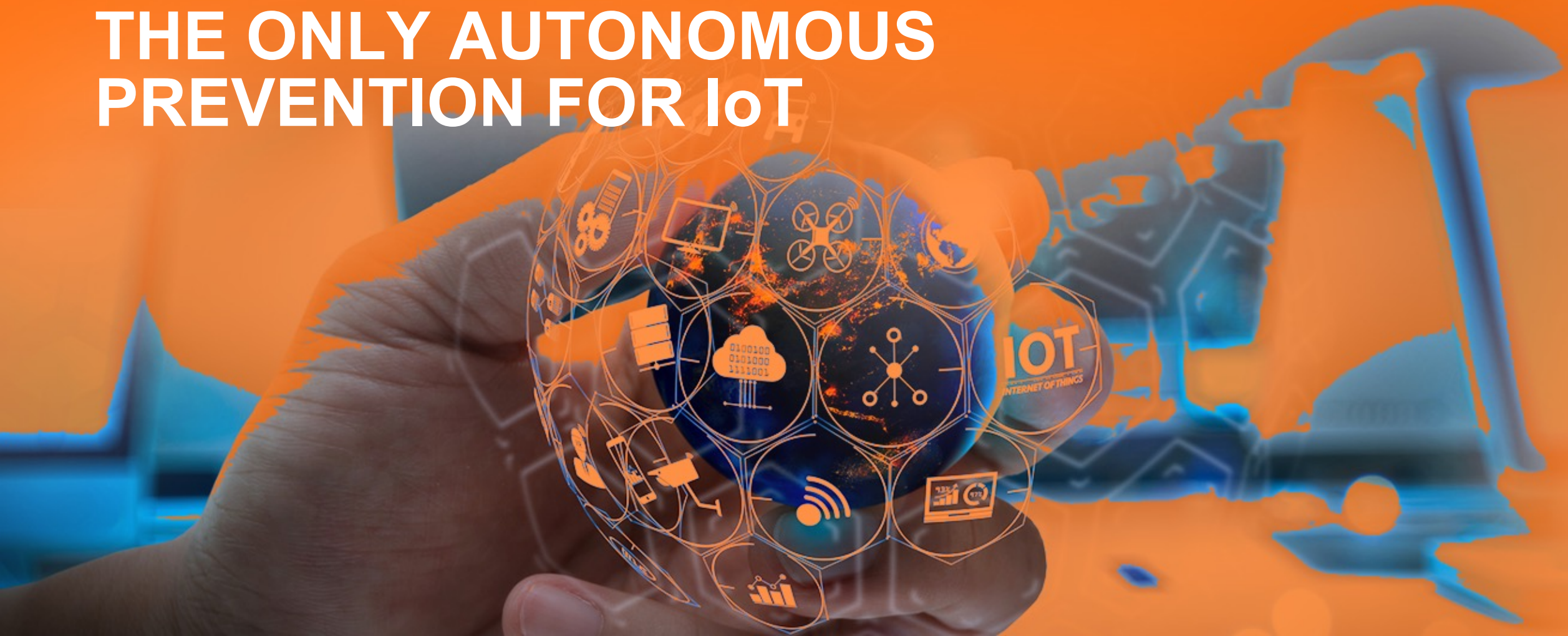
9 Blades

Sandblast - Gen V Threat Prevention (Sandblast / NGTX)

Next Generation Threat Prevention +
Threat Emulation
Threat Extraction
Zero Phishing ★

12 Blades - Best Security

THE ONLY AUTONOMOUS PREVENTION FOR IoT



Attacks Continue to Expand Across Industries

Bloomberg

Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals



The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town



Introducing: Quantum IoT Protect Software Blade

The Only Autonomous Threat Prevention for IoT Devices

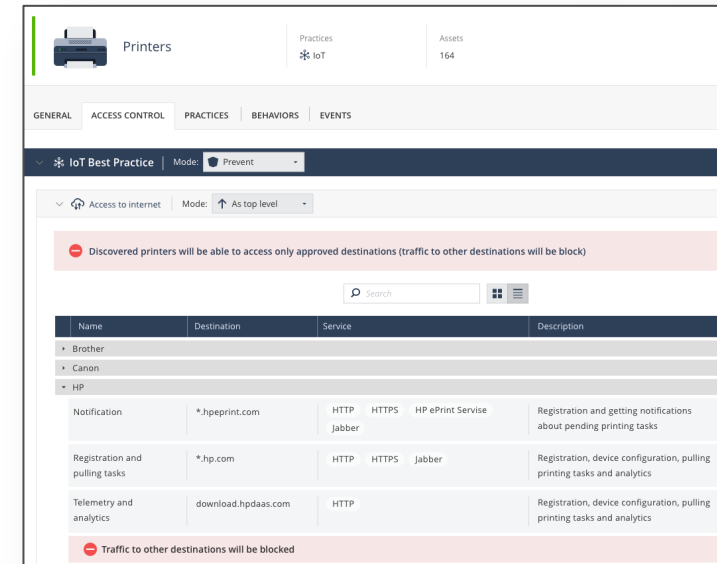
1 DISCOVER & PROFILE IoT ASSETS VIA QUANTUM GATEWAY

2 AUTONOMOUS ZERO-TRUST THREAT PREVENTION PROFILES



ASSETS BY TYPE

	1,024	Smart Locks	24 Recently discovered
	282	Printers	8 Recently discovered
	176	IP Cameras	8 Recently discovered
	24	Smart TVs	...
	18	Projectors	18 Recently discovered
	16	Coffee Machines	...
	10	Smoke Alarm Detector	10 Recently discovered



Printers

Practices IoT Assets 164

GENERAL ACCESS CONTROL PRACTICES BEHAVIORS EVENTS

IoT Best Practice Mode: Prevent

Access to Internet Mode: As top level

Discovered printers will be able to access only approved destinations (traffic to other destinations will be block)

Name	Destination	Service	Description
Brother			
Canon			
HP			
Notification	*.hpeprint.com	HTTP HTTPS Jabber HP ePrint Service	Registration and getting notifications about pending printing tasks
Registration and pulling tasks	*.hp.com	HTTP HTTPS Jabber	Registration, device configuration, pulling printing tasks and analytics
Telemetry and analytics	download.hpdaas.com	HTTP	Registration, device configuration, pulling printing tasks and analytics

Traffic to other destinations will be blocked

IoT Threat Prevention in Minutes!

ADVANCED SECURITY AND OPERATIONAL EFFICIENCY

Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

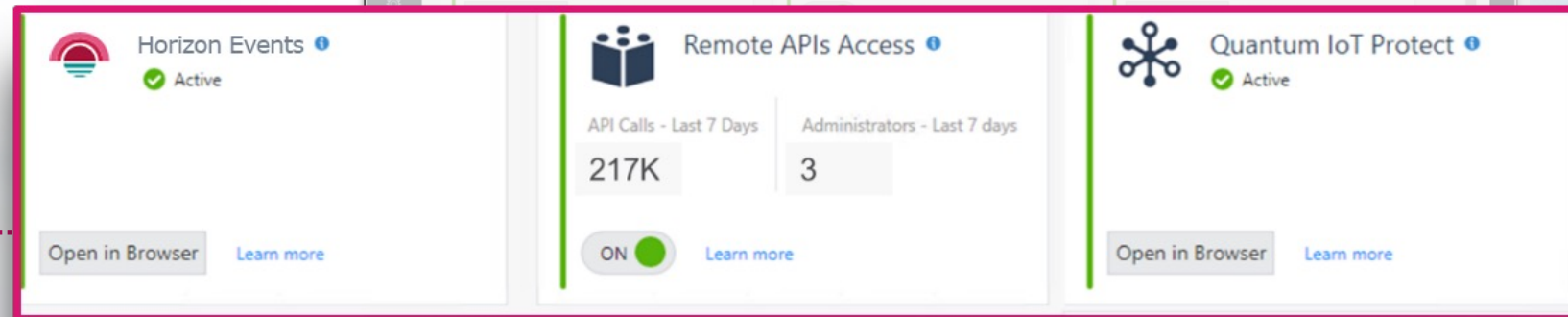
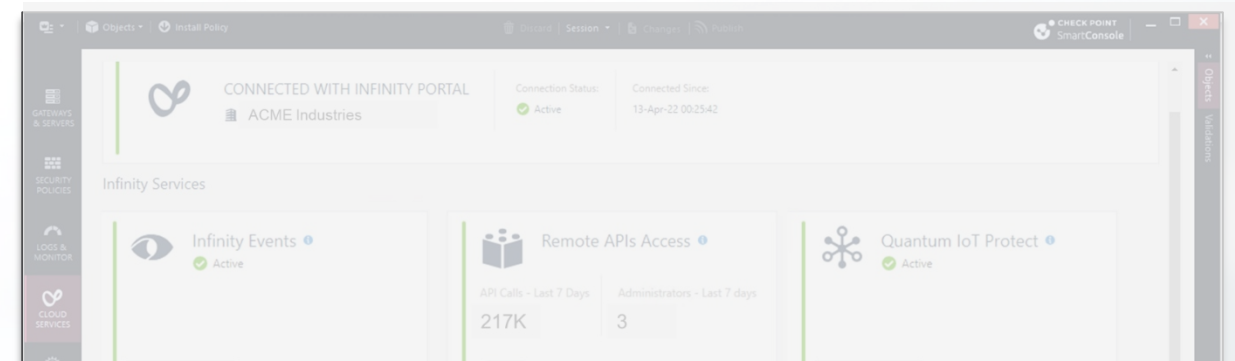
Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management



Fast adoption of New Security Services

Integrate cloud-delivered services into network security policies

- IoT Security
- Unified events platform
- Management APIs for 3rd parties
- *And more to come...*



Complete Event Visibility Across All Domains

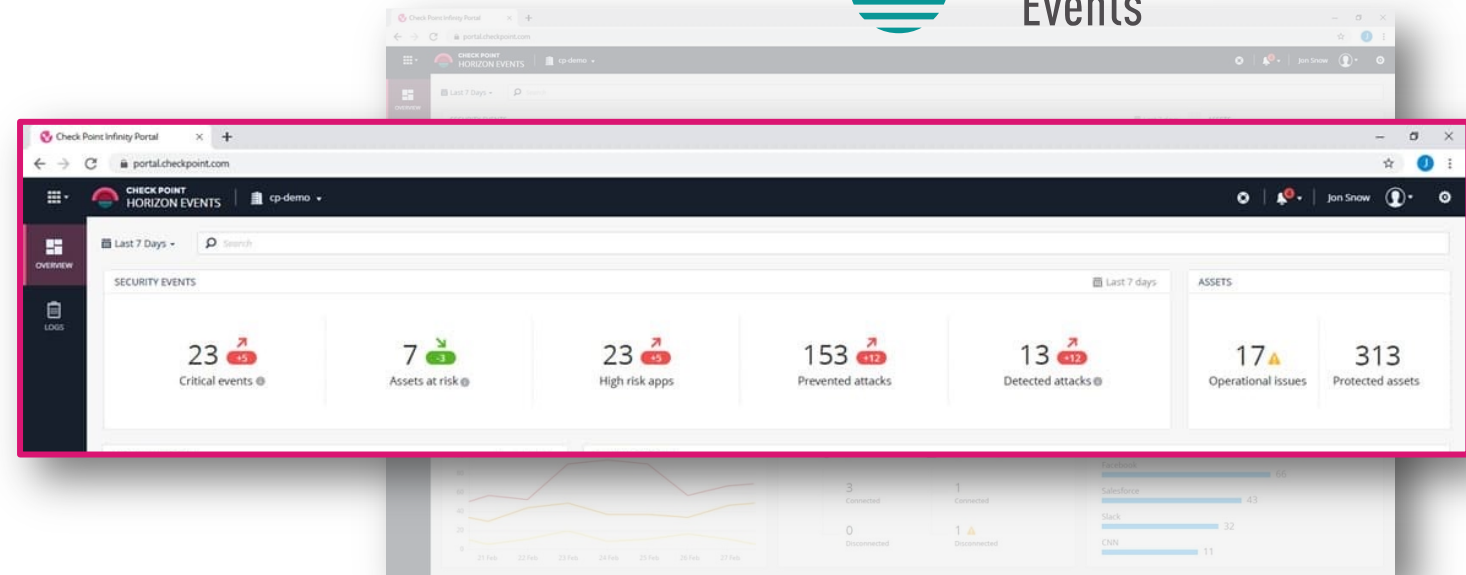
Search and view logs across all Check Point products



Limitless log storage

Single pane of glass for Ops

Cross-accounts view for MSPs



Align Network Security Policy to Dynamic Business Changes

Manage policies without network admin, or opening tickets

Policy changes effective immediately. No need for “policy install.”

		Source	Destination	VPN	Services & Applications	Action
▼ DevOps team access (11-13)						
11	Automation & pipeline tools	Automation_team	Automation_network	* Any	Jenkins CircleCI	Accept
12	Handling real time data	Application_team	Applications_network	* Any	Apache Kafka	Accept
13	Cleanup rules	* Any	* Any	* Any	* Any	Drop

Network Feed Objects

Streamline Policy Change-Review

Superior management with built-in “two sets of eyes”

Intuitive policy change review
and approval cycle

Audit trail for policy compliance

SUMMARY OF REVISION CHANGES | Generated by admin on Tue Jul 12 2022 13:33:26 GMT-0700 (Pacific Daylight Time)

Sessions (1)

Name	Description	Administrator	Time
		admin	Pending

OVERVIEW

ACCESS CONTROL RULES (7)

* 4 New | ✎ 1 Edit | 🗑️ 2 Delete

THREAT PREVENTION RULES (3)

* 0 New | ✎ 1 Edit | 🗑️ 2 Delete

OBJECTS (46)

* 41 New | ✎ 1 Edit | 🗑️ 4 Delete

BUSINESS DRIVEN SECURITY PERFORMANCE

Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

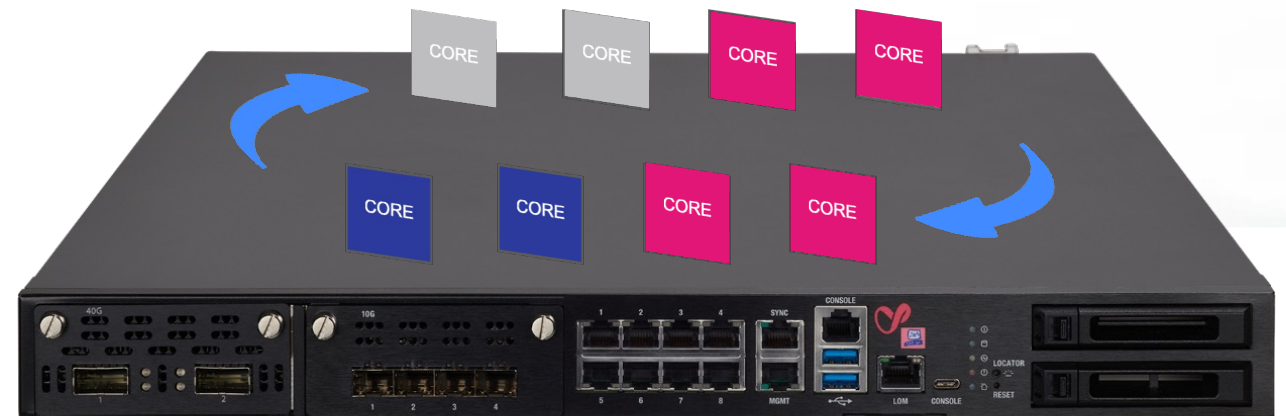


3x Throughput for Large File Transfers

Distribute elephant flows across multiple cores

Dynamic workload distribution

No Configuration needed



HyperFlow with R81.20

Business Oriented Network Security with Maestro

Performance elasticity to your most critical applications

Dynamically shift resources to high priority and peak workloads

Optimize gateway capacity and investment with auto-scaling



Ultra Low Latency for Trusted Business Applications

Fast forward: 100Gbps for trusted connections

800 Nano Seconds latency for large file transfers

Accelerated trusted, secure connections

ZERO performance impact on firewalls



And Even More Capabilities with Quantum Titan including...

Over 20 New Features

- **Strong MFA with SAML:**
Authenticate to SmartConsole & VPN via 3rd party Identity Providers (Okta, +)
- **Seamless Cloud VPN Setup:**
Reduces on-prem to public cloud VPN configuration steps from 25 to 5
- **New Security Management APIs:**
Automate HTTPSi certs, Identity Awareness, and LSM policy
- **CloudGuard Updates:**
Cloud controller now supports Nutanix, Oracle, and more
- **Manage Quantum Clusters Upgrade Directly from SmartConsole:**
Now supports Spark, Edge, and gradual cluster updates



SUMMARY



Quantum Titan - The Network Security You Need

Three New software blades

Prevent advanced DNS attacks

Best Security for Zero-Day Phishing

The Only Autonomous IOT Threat Prevention

More Effective Security Management

3X Performance boost for large file transfers



New Release Terminology

Every major release or Jumbo, will have two stages – starting with **“Latest”**, and once the release gets good feedback - **“Recommended”**

[Sk95746 – Check Point Default Version and Release Terminology](#)



THANK YOU

YOU DESERVE THE BEST SECURITY