

Check Point Software

Brand & Design Management

Check Point Software is a global leader in enterprise cybersecurity solutions for corporations and governments. The company required consistent, scalable design across its brand, web presence, and marketing initiatives to support global growth and communication.

Role

- Served as a Design Manager, overseeing a diverse portfolio of UX, brand, web, print and digital design projects
- Collaborated with Sales, Product, Marketing, and Executive Leadership to align design with business goals
- Managed the full creative process from scoping and research through strategy, art direction, and reviews
- Mentored and supported a small team of designers and freelancers

Impact

- Delivered a cohesive and modernized brand identity across global channels
- Improved creative workflows by implementing clear design systems and processes
- Strengthened collaboration between design and cross-functional teams
- Enhanced design team performance through mentorship and structured guidance

Projects

2

Brand Refresh & Guidelines

6

Brand Application

9

Annual Reports

11

Social Media Campaigns

12

Marketing Campaigns

13

UX, Web and Digital Design

19

Design Systems, Ops and Strategy

Check Point Software

Brand Refresh + Guidelines

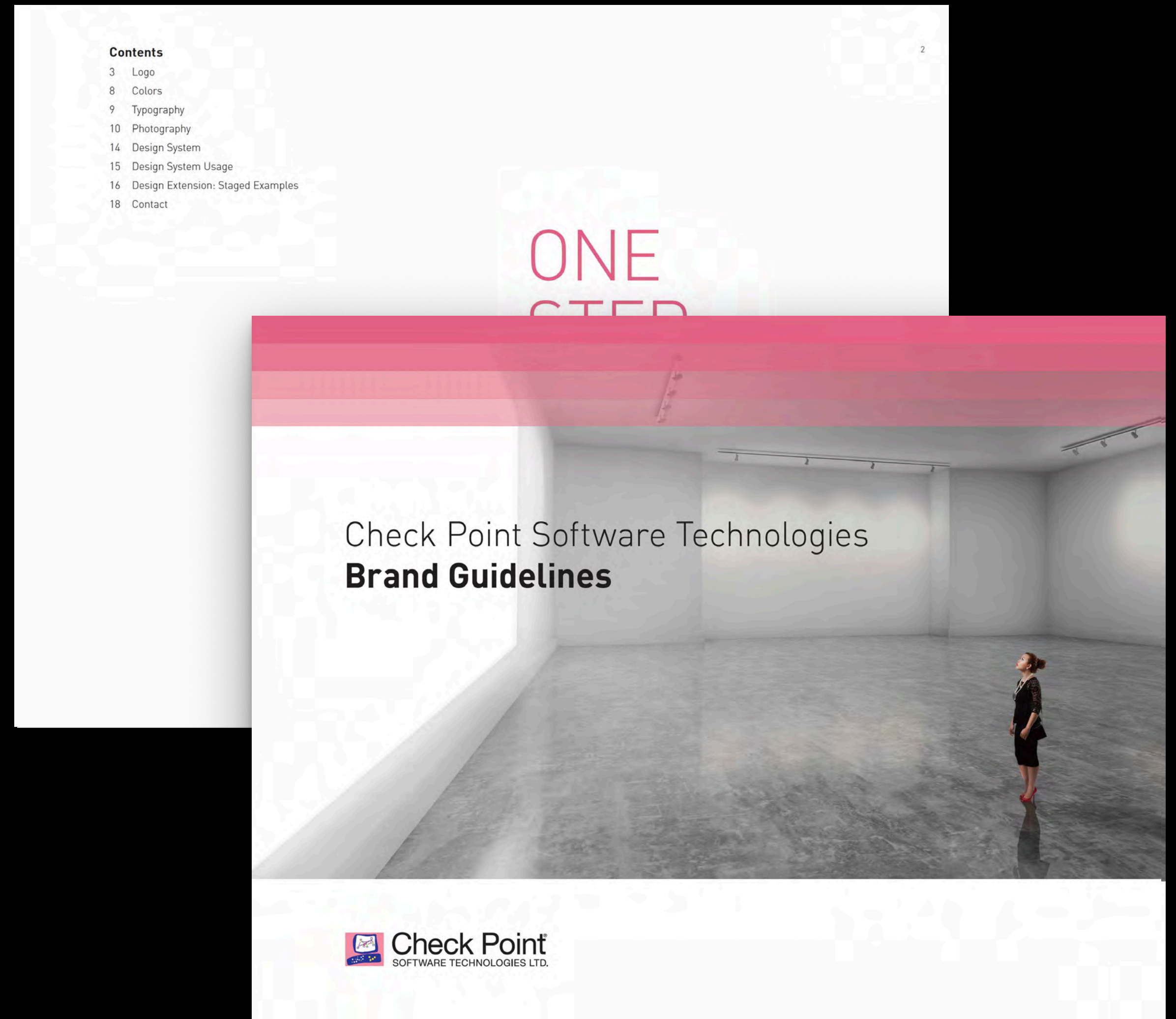
Check Point was undergoing a major brand shift and needed a refreshed identity that felt modern, forward-looking, and scalable. The project focused on evolving the brand through a soft rebrand and updated guidelines that could be applied consistently across all channels.

Role

- Served as Art Director, shaping the creative vision and guiding two supporting designers
- Partnered with the Creative Director and Head of Marketing to ensure alignment with brand strategy and business goals
- Managed the rollout of the refreshed identity across collateral, digital platforms, and campaigns

Impact

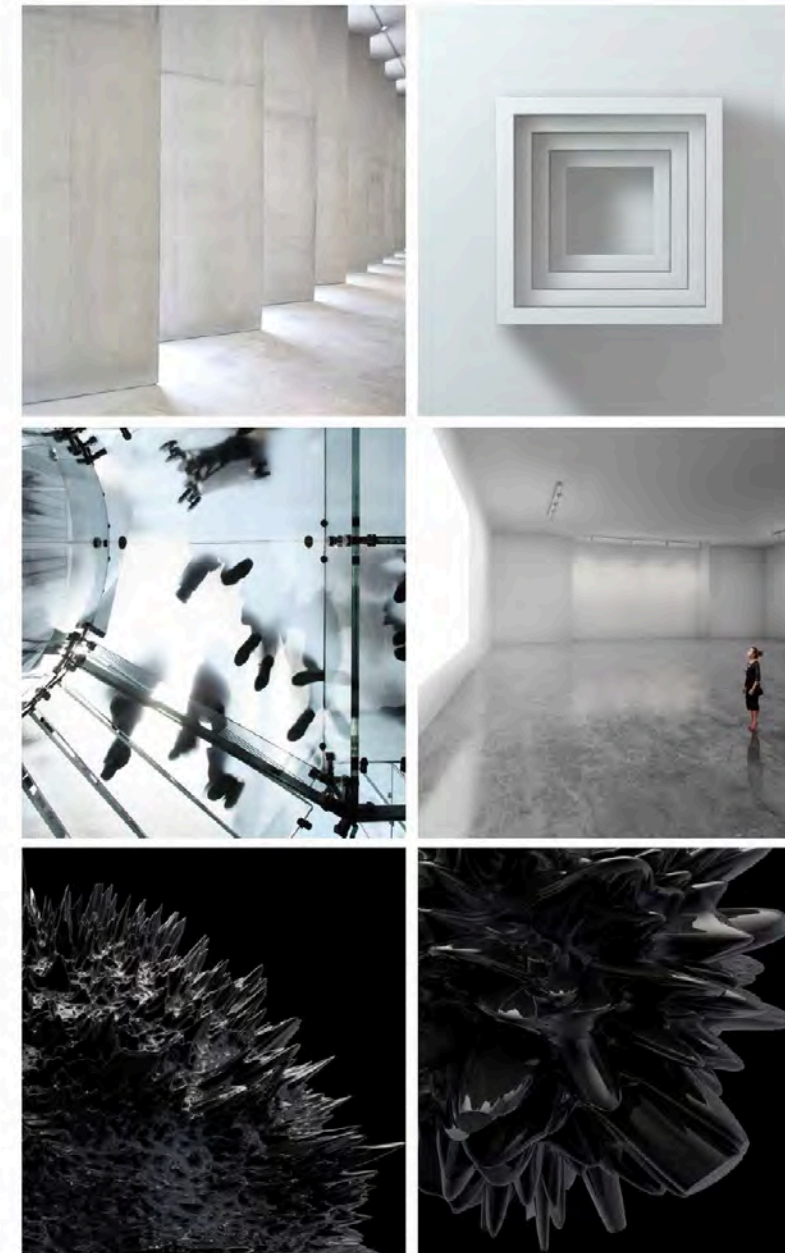
- Delivered comprehensive brand guidelines that enabled consistency across digital, print, and marketing applications
- Elevated the brand's visual presence, positioning Check Point as a modern and credible leader in cybersecurity



Photography

Photography

Photography can be a powerful asset in promoting the brand as well as Check Point's specific security features. Subject matter should focus on one of three categories: environmental images, threat interpretations, and futuristic images of people.



10

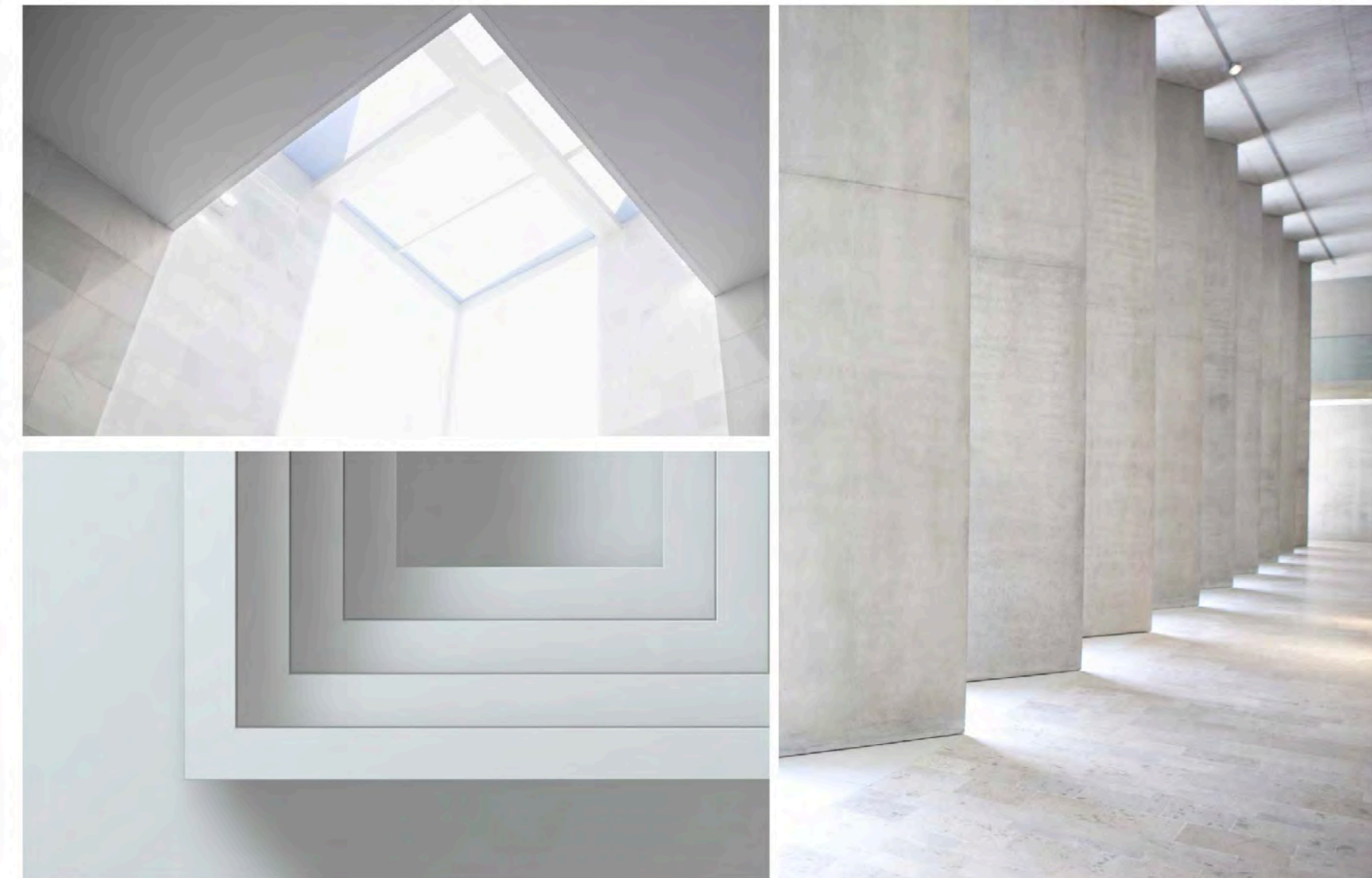
Check Point Software Technologies Brand Guidelines

Photography (continued)

Environmental

The environmental style of photography should feature abstractions with sharp angles of architecture to emphasize light and shadow. A strong contrast between light and dark areas provides the setting for portraying secure and insecure areas. Images should be grayscale or highly desaturated.

11



Check Point Software Technologies Brand Guidelines

Pages from Brand Guidelines

The brand shifted away from cliché 'cybercriminal' visuals and embraced sophisticated, high-contrast photography. Light and shadow were used intentionally to symbolize secure versus insecure areas, creating a more modern, confident, and forward-looking identity.

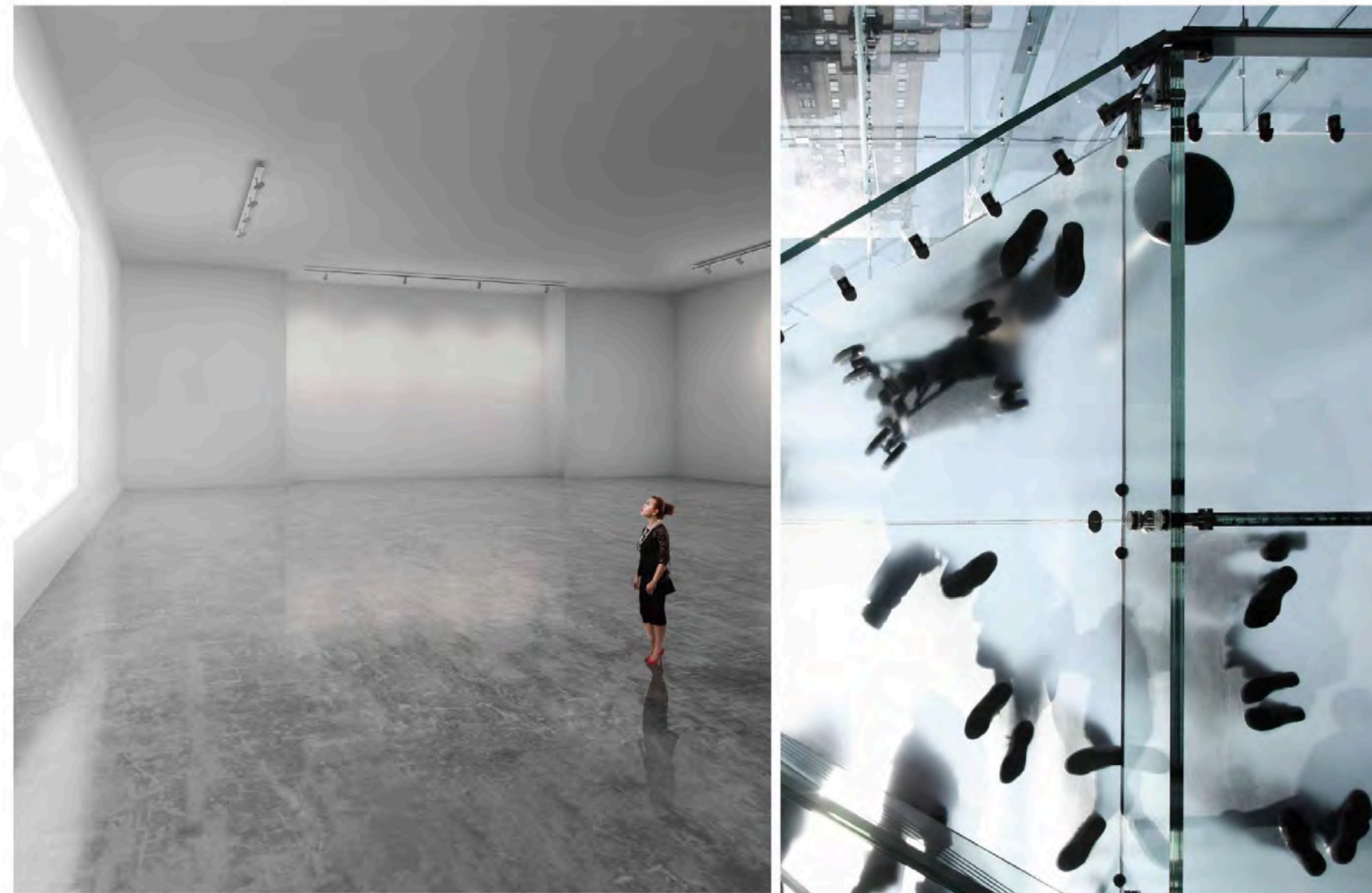
Photography

Photography (continued)

People

12

Photographs including people should be futuristic and dynamic images of everyday people (non-executive) interacting with a bright source of light. The images should demonstrate a powerful sense of scale with high contrast between light and dark areas. Images should be grayscale or highly desaturated.



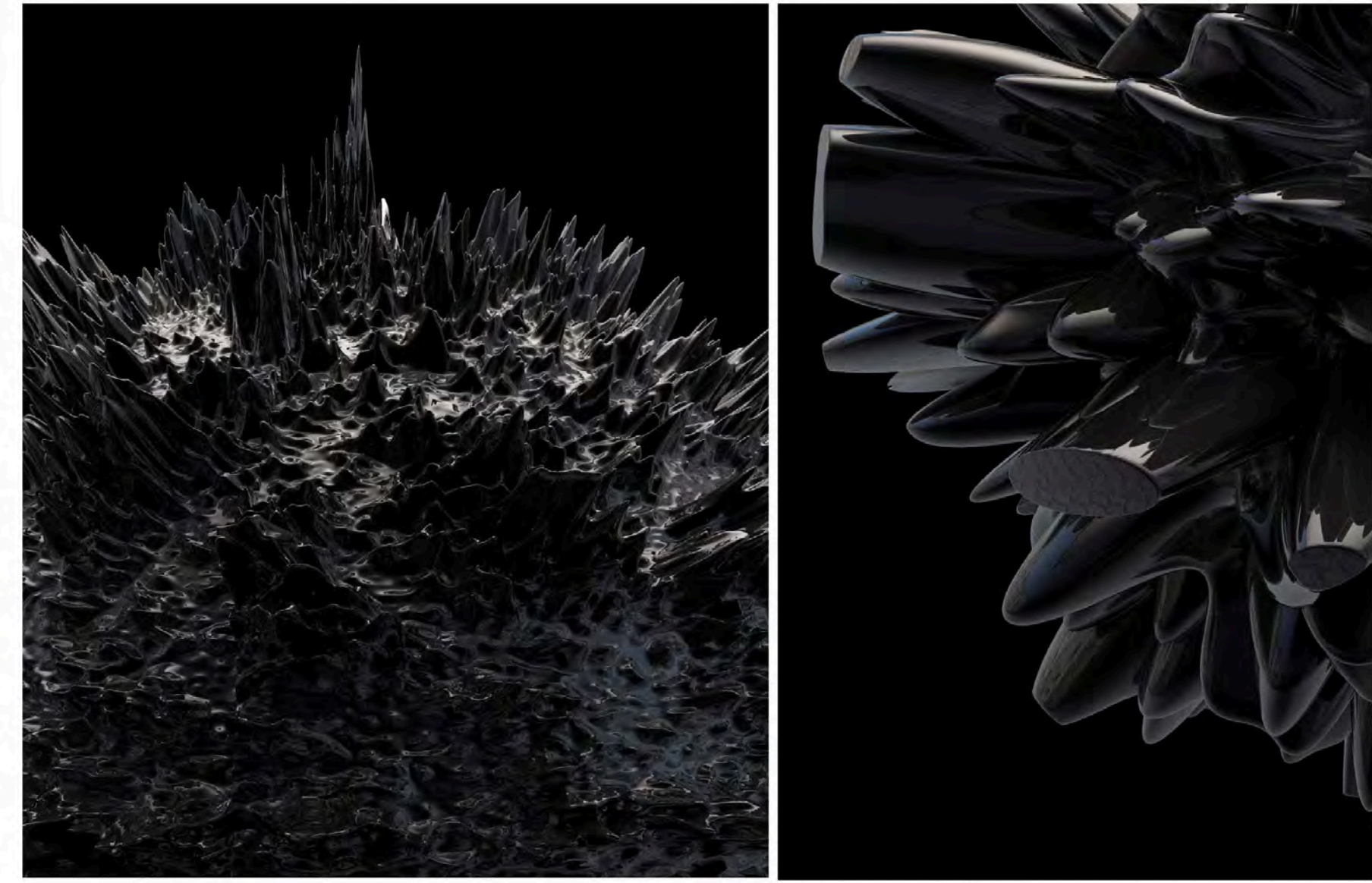
Check Point Software Technologies Brand Guidelines

Photography (continued)

Bots

13

This photography style is the representation of the threats Check Point Software Technologies protects against. These images should contain menacing, sharp shapes—or “bots”—on a black background.



Check Point Software Technologies Brand Guidelines

Pages from Brand Guidelines

The visual language expanded with futuristic, dynamic imagery of people interacting with light sources to symbolize security and innovation. Pathogen-like “bot” graphics were introduced as a recurring motif to represent cyber threats, creating a modern, forward-looking identity that aligned with the company’s evolving strategy.

Design System

Design System

Unique design elements are an essential visual tool of the Check Point brand. These graphic shapes represent the diverse and flexible security platforms we offer.

The main design elements that make up the system are comprised of four pink bars representing Check Point's security zone. One is solid and the remaining three are of increasing transparency. The solid bar is always closest to the "secure" area in a visual composition.

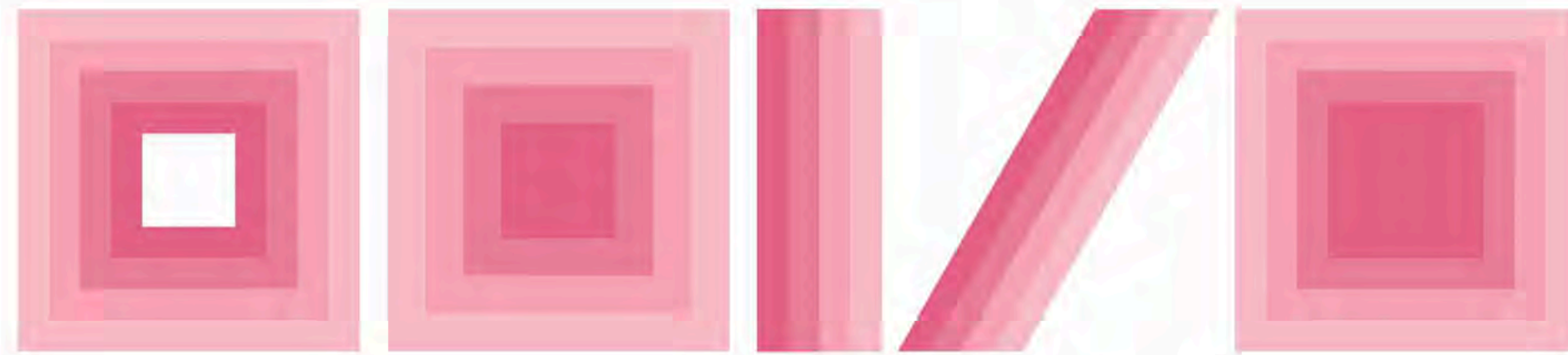
These elements can be used in a variety of shapes and angles, as shown below. They can be the primary element in a design or a basic visual accent.

Security Layer Transparencies

14



Graphic Shapes

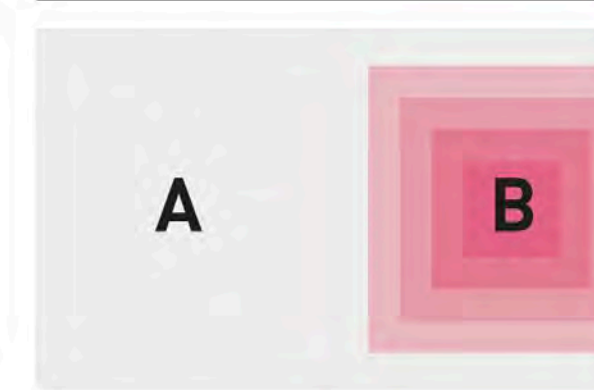


Check Point Software Technologies Brand Guidelines

Design System Usage

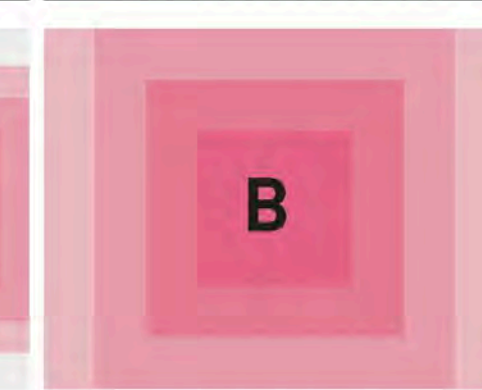
15

Example 1 (with images)



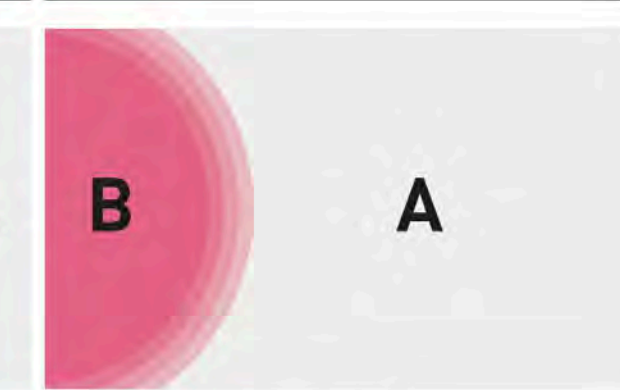
A - threat imagery / outside world
B - secure area

Example 2 (with images)



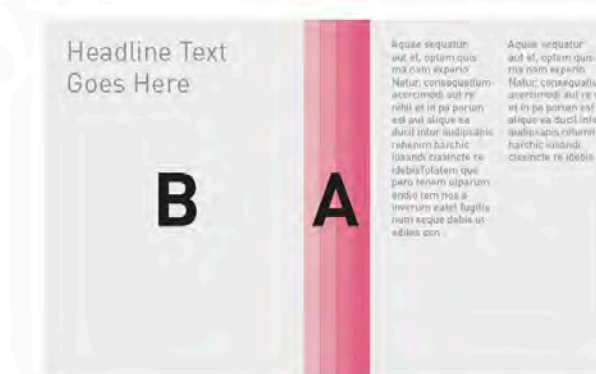
A - threat imagery / outside world
B - secure area

Example 3 (with images)



A - threat imagery / outside world
B - secure area

Example 4 (no images)



A - protective brand lines
B - content area

Example 5 (no images)



A - protective brand lines and secure area
B - content area

Example 6 (no images)



A - protective brand lines
B - content area

Check Point Software Technologies Brand Guidelines

A flexible graphic system was created to support the refreshed identity. Its core element, four pink security bars with the solid bar symbolizing full protection, could serve as bold visuals or subtle accents, making the system adaptable across print, digital, and campaign materials.

Check Point Software

Brand Application

The refreshed brand system needed to extend across a wide range of customer-facing materials, from posters and datasheets to brochures, handbooks, and reports.

Role

- Applied the updated brand identity across diverse collateral
- Ensured flexibility in adapting designs to different formats and audiences
- Guided consistency through templates, design systems, and reviews

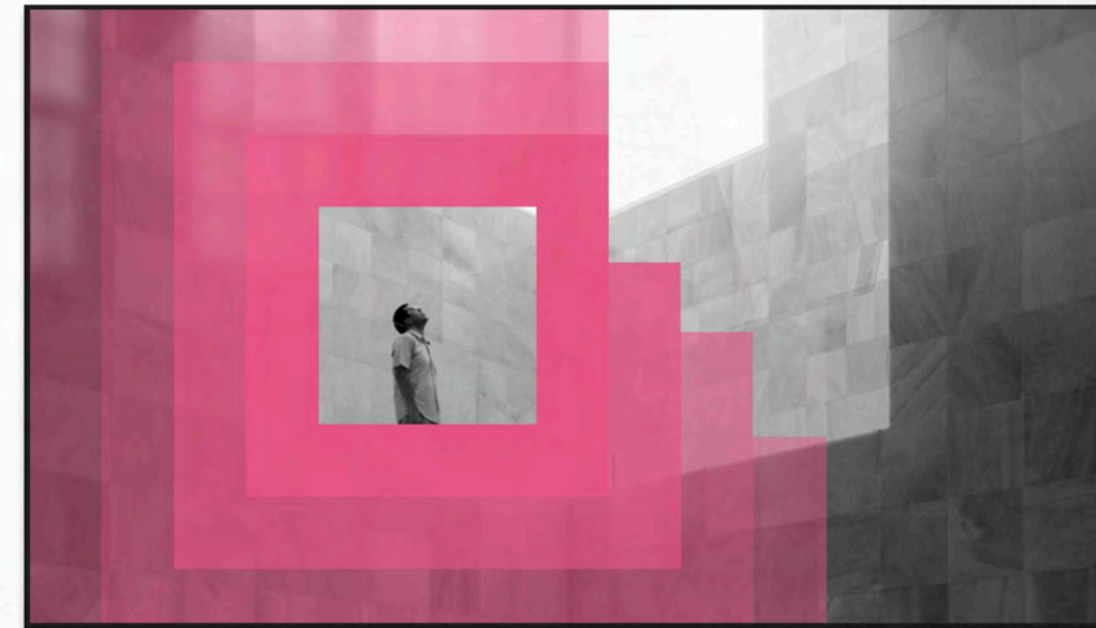
Impact

- Delivered a unified visual identity across all collateral
- Improved clarity and brand recognition in customer-facing materials
- Established scalable practices for ongoing collateral production





Digital Poster



Digital Poster

Check Point Threat Prevention Appliances

KEY FEATURES

- One industrial appliance integrating Firewall, Antivirus, Anti Bot, IPS, URL Filtering, Identity Awareness and Application Control.
- Proven secure with a comprehensive portfolio of threat prevention features on one appliance.
- ThreatGuard™, the best subscription network in tight physical, provides real-time security intelligence.
- Identity and session analysis has been being operational for over 10 years.
- Pre-incident protection by blocking bot and stopping bot damage.
- Simple, unified user console increases visibility over all security.
- Clear and user granular policy and reporting.

KEY BENEFITS

- Consolidated hardware to protect business.
- Single console to manage security, and access to current appliances, users and services.
- Simple and easy to manage.
- Real-time updates against new threats.
- Integrated with Check Point security manager for better control.

DATASHEET: Check Point Threat Prevention Appliances

	4809	12209	12409	12609
SCALING				
Concurrent Connections (M)	1.7 T.3	1.7 T.5	1.7 T.5	1.7 T.5
Connections per Second (K)	70	70	170	70
SYSTEM RESOURCES				
Memory / Max	4 / 8 GB	4 / 12 GB	4 / 11 GB	4 / 8
Storage	250 GB	500 GB	500 GB (up to 2)	250 GB
Network Interfaces	8x 10/100/1000 Base-T RJ45 ports	8x 10/100/1000 Base-T RJ45 ports	3x 10/100/1000 Base-T RJ45 ports	2x 10/100/1000 Base-T RJ45 ports
Power Supply	One AC power supply	One AC power supply	Redundant dual hot-swappable	Redundant dual hot-swappable
LOM	Yes	Yes	Yes	Yes
DIMENSIONS				
Enclosure	1U	1U	1U	1U
Standard (W x D x H)	17.25 x 16.14 x 1.73 in	17.25 x 16.14 x 1.73 in	17.25 x 12.19 x 1.73 in	17.25 x 12.19 x 1.73 in
Metric (W x D x H)	438 x 410 x 44mm	438 x 410 x 44mm	438 x 308 x 44mm	438 x 308 x 44mm
Weight	7.4 kg (16.4 lb)	7.4 kg (16.4 lb)	7.4 kg (16.4 lb)	7.4 kg (16.4 lb)
POWER REQUIREMENTS				
AC Input Voltage	100 - 240V	100 - 240V	100 - 240V	100 - 240V
Frequency	47 - 63 Hz	47 - 63 Hz	47 - 63 Hz	47 - 63 Hz
Single Phase Supply Rating	270W	270W	270W	270W
Power Consumption Maximum	140W	140W	140W	140W
Maximum Thermal Output	435.4 BTU	435.4 BTU	435.4 BTU	435.4 BTU

Data Sheet

AN AVERAGE DAY IN AN ENTERPRISE ORGANIZATION

EVERY **24 hrs** A HOST IS INFECTED WITH A BOT.

MALWARE TREND

The Check Point security research team analyzed a year of event data from across over 10,000 enterprises to identify the primary threat and determine the impact of 2013 and 2014. The research shows that the number of malware incidents has increased significantly, with a 100% increase in 2014 compared to 2013. The research also shows that the number of malware incidents has increased significantly, with a 100% increase in 2014 compared to 2013.

1997 2004 2009 2010 2014

Legend:

- FINANCIAL SERVICES / FINANCIAL
- HEALTH CARE / HEALTH CARE
- MANUFACTURING / MANUFACTURING
- STATE GOVERNMENT / STATE GOVERNMENT

Brochure Spread

Annual Security Report

The Annual Security Report was a flagship publication for Check Point, produced each year as an 80+ page document over the course of two to three months. Highly visible within the industry, the report positioned the company as a thought leader in cybersecurity and served as a key resource for executives, partners, and customers worldwide.

Role

- Served as lead manager, art director, and designer.
- Collaborated with industry experts, writers, and product marketing teams.
- Directed layout, visual language, and design reviews.

Impact

- Translated complex data and statistics into clear, engaging infographics and charts.
- Enhanced readability and visual storytelling for a global executive audience.

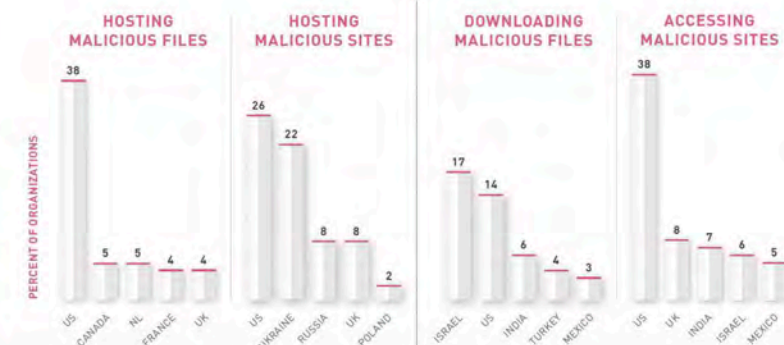


03 KNOWN MALWARE: KNOWN AND DANGEROUS

"We're all digital, we're all vulnerable and everything's instant—so instant. Instant success and instant failure."

—Makoto, pop star, on the digital theft and leaking of her unfinished album, "Debel Heart," before it was released.

TOP 5 COUNTRIES



3.1 SOURCE: Check Point Software Technologies

Given how easy and powerful unknown malware is to create and launch, you would think we would start seeing a decline in known malware. The reality, however, is that hackers continue to keep this method of attack in their arsenal.

In 2014, Check Point researchers discovered that roughly 86 percent of organizations accessed a malicious site. What's more, close to 63 percent of organizations downloaded a malicious file. Looking at speed and frequency, hosts accessed a malicious website every 24 seconds (compared to every minute in the previous year), and downloaded malware every six minutes (compared to every 10 minutes in the previous year). When you consider how quickly viruses can spread and wreak havoc, this goes way beyond alarming.

In 2014 hosts downloaded malware every 6 minutes

In 2014 hosts accessed a malicious site every 24 seconds

TOP HIGH-RISK APPLICATIONS BY REGION

2014	AMERICAS	EMEA	APAC
ANONYMIZER	Hola • Tor • Coralcdn	OpenVPN • Coralcdn Proxy Suppliers	OpenVPN • Coralcdn • Tor
P2P FILE SHARING	BitTorrent Protocol • SoulSeek BoxCloud	BitTorrent Protocol • SoulSeek Mesh	BitTorrent Protocol • Xunlei QQ Download
FILE STORAGE AND SHARING	Dropbox • HighTail Windows Live Office	Dropbox • HighTail • Jalbum	Dropbox • HighTail • Mendeley
REMOTE ADMIN	RDP • LogMeIn • TeamViewer	TeamViewer • RDP • LogMeIn	TeamViewer • RDP • LogMeIn

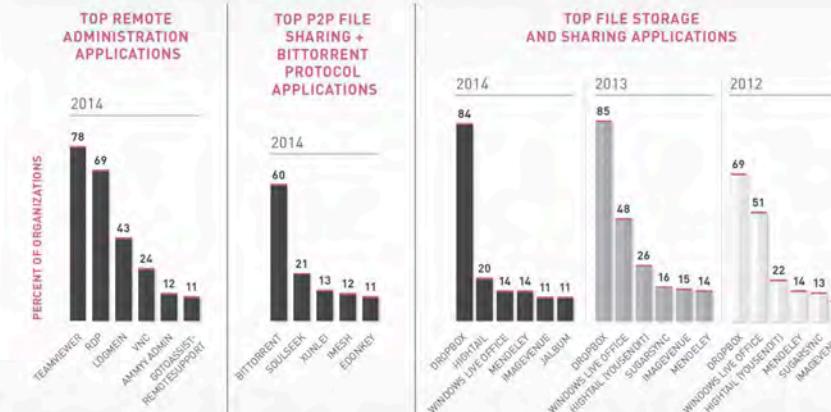
2013	AMERICAS	EMEA	APAC
ANONYMIZER	Tor • UltraSurf • Hotspot Shield	OpenVPN • Coralcdn Proxy Suppliers	UltraSurf • Tor • Hide My Ass
P2P FILE SHARING	BitTorrent Protocol • SoulSeek BoxCloud	BitTorrent Protocol • SoulSeek eDonkey Protocol	BitTorrent Protocol • Xunlei SoulSeek
FILE STORAGE AND SHARING	Dropbox • Windows Live Office HighTail	Dropbox • Windows Live Office HighTail	Dropbox • Windows Live Office HighTail
REMOTE ADMIN	RDP • LogMeIn • TeamViewer	RDP • TeamViewer • LogMeIn	TeamViewer • RDP • LogMeIn

5.2 SOURCE: Check Point Software Technologies

Organizations experienced 12.7 high-risk application events per hour, 305 times per day

Hide My Ass was nowhere to be seen. Likely, OpenVPN gained popularity following the Edward Snowden revelations about NSA eavesdropping. The reason is that as an industry standard, OpenVPN uses crypto technology that cannot be broken if implemented correctly, thus keeping communications private. Meanwhile, other anonymizers have climbed tremendously in popularity, even if not yet one of the top three.

For instance, the Hola anonymizer app rose from three percent to 17 percent. Part of its claim to fame could be credited to being in the right place at the right time. Hola emerged from beta testing just before the 2014 Sochi Olympics. Because it allows internet access across borders, programming that would be otherwise only available to people in a specific geography is accessible for those using Hola to cloak their geolocations.



5.3 SOURCE: Check Point Software Technologies

dropped from 68 percent to 40 percent. Why? Hackers show a preference for targeting clients because they can use social engineering and phishing tactics to trick people. In other words, humans are much easier to dupe than machines.

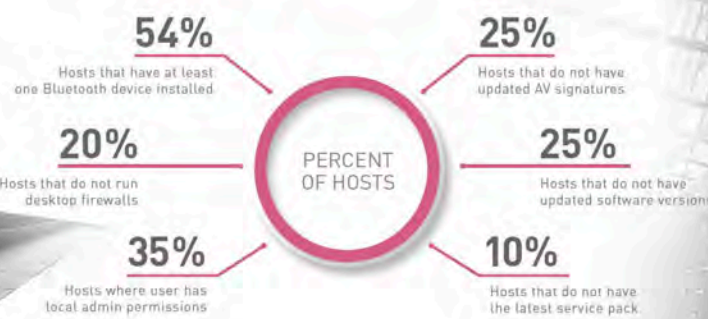
So what's contributing to the problem? Negligence around basic protections. In addition, organizations are using legacy security tools that fall short in addressing the evolving threats of today. If you want to keep your endpoints safe, you start with fundamental actions like ensuring your computers are running desktop firewalls, have updated service packs and software, and have the latest anti-virus software installed.

Yet according to our findings, 20 percent of enterprise hosts are not running a desktop firewall; 10 percent of enterprise hosts don't have updated service

packs; 25 percent don't have updated versions of their software; and 17 percent don't have anti-virus installed at all. In addition, 35 percent of enterprise hosts are configured such that users have local administrator permissions, putting their operating systems at greater risk for malware exploitation.

While these numbers might not seem huge, it's still an important flag that there are some enterprises that are not getting the security message: It only takes one vulnerable host to infect an entire network. And think about the number of businesses with whom those enterprises interact and exchange information. Part of managing the threat of cybercrime means being a responsible cyber citizen when it comes to basic protections—and sharing important security information with others.

ENTERPRISE ENDPOINT VULNERABILITIES AND MISCONFIGURATIONS



3.6 SOURCE: Check Point Software Technologies

Compliant Without Complaint

While most businesses understand their responsibilities around compliance and meeting industry regulations when it comes to security, it's still a very complex issue. You could be fully compliant one day, and then make a business-related change to your network and suddenly find yourself out of compliance. Knowing what to watch for is critical. But don't fall into the trap of thinking that just because your organization is compliant it is completely secure. Meeting regulatory requirements is typically tied to specific threats, making it less comprehensive than a security posture could and should be. It should not be the basis of your security policy. Below is what Check Point discovered in its 2014 research.

CHECK POINT FINDING	CHECK POINT ISSUE ANALYSIS	REGULATION	COUNTRIES IMPACTED BY THIS REGULATION
Anti-Spoofing not being activated for 75% of the respondents	Anti-spoofing verifies that packets are coming from, and going to, the correct interfaces on the gateway. It confirms that packets claiming to be from an internal network are actually coming from the internal network interfaces. It also verifies that, once a packet is routed, it is going through the proper interface.	PCI DSS 3.6 NIST 800.41	Global—any company processing or storing credit card data Mainly relevant to US Federal, but equally applicable to any US company adopting a robust firewall standard
Discovering Any Any Accept rule in 27% of respondents	The fundamental concept of the firewall rule base is "that which is not explicitly permitted is prohibited." To discover that 27% of respondents had an Any Any Accept rule in their rule base was a major surprise. This is firewall 101, the basic of basics.	PCI DSS 3.6 NIST 800.41	Global—any company processing or storing credit card data Mainly relevant to US Federal, but equally applicable to any US company adopting a robust firewall standard
Out-of-State TCP packets not being dropped in 19% of respondents	TCP session timeout is the length of time an idle connection will remain in the security gateway connections table. This idle session is the delay in which an attacker can try to steal and use existing user session package transportation. Packets that are out of state should be dropped. We found that 1 out of 5 companies are not dropping out of state packets.	PCI DSS 3.6 ISO 27001	Global—any company following this standard Global—any company processing or storing credit card data Global—any company being certified to this standard or adopting it as a best practice

CORPORATE DATA AT RISK



4.1 SOURCE: Check Point Software Technologies

When mobile security is weak, it can provide attackers with personal information, passwords, business and personal email, corporate documents, and access to company networks and applications. In the business setting, that concern becomes magnified. In fact, 87 percent of IT professionals say careless employees are a greater threat to security than cybercriminals. And, 92 percent say employee behaviors could have made a difference in preventing high-profile security breaches.

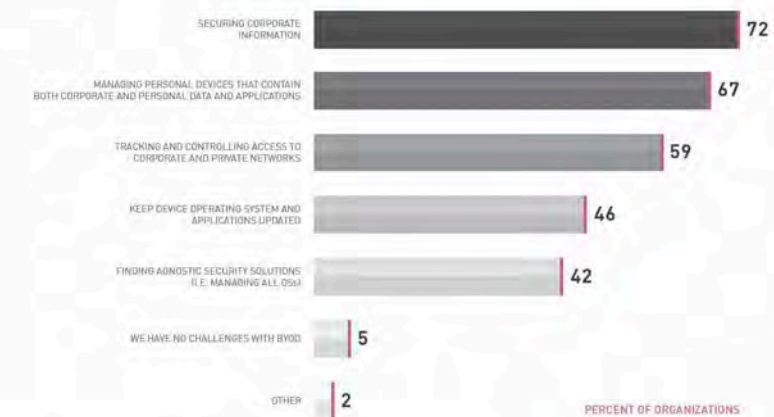
OUT OF CONTROL

Among those surveyed, 91 percent have seen an increase in the number of personal mobile devices connecting to corporate networks during the past two years. Alarmingly, 44 percent of organizations do not manage corporate data on employee-owned devices. Add to that, 33 percent of app developers do not test their apps for security.

BYOD challenges become even more notable in the context of a separate global study we conducted. Commercial mobile surveillance kits, typically used for monitoring children—or in some cases spying—were put under the microscope. The reason: Such products are vulnerable to mobile remote-access Trojans (mRATs), which top the list of mobile malware. More than 500,000 Android and 420,000 iOS devices that connected to corporate Wi-Fi through Check Point firewalls in more than 100

countries were studied. If devices communicated with a command and control (C&C) server, they were considered infected. Researchers found that one out of every 1,000 devices was infected. And in fact, researchers determined that if there are 2,000 devices or more in an organization, there is a 50 percent chance that there are at least six infected or targeted mobile devices on their network. By platform, that breaks down to 60 percent Android and 40 percent iOS.

BYOD SECURITY CHALLENGES



4.2 SOURCE: Check Point Software Technologies

Check Point Software

Social Media Campaigns

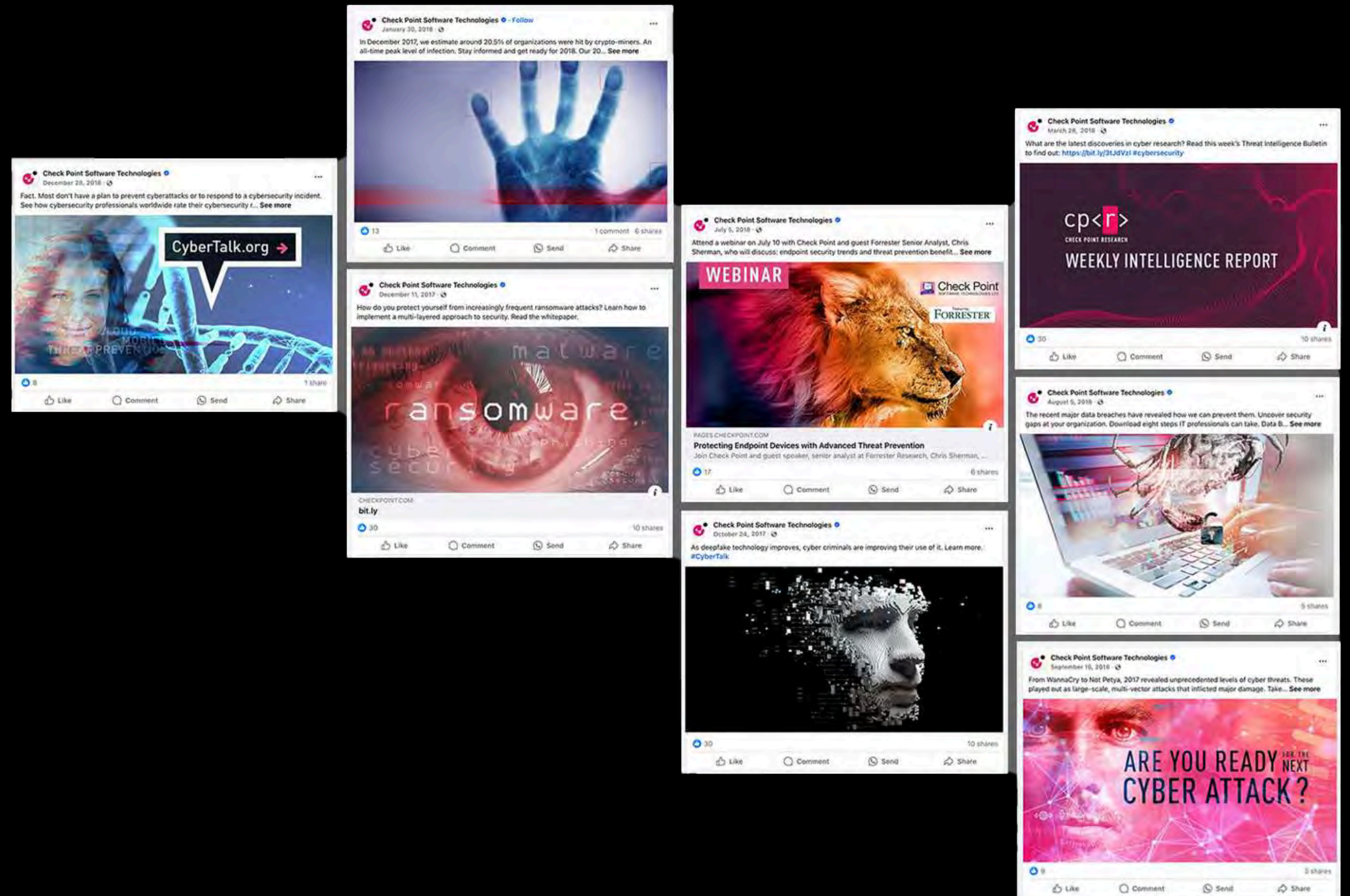
Check Point maintained an active presence on LinkedIn, Twitter, Instagram, and Facebook, where campaigns highlighted webinars, executive insights, industry news, and security reports.

Role

- Collaborated with marketing to plan and execute social campaigns
- Art directed visual concepts and managed asset production
- Designed campaign materials as needed to ensure quality and consistency

Impact

- Delivered consistent, on-brand content across multiple social platforms
- Increased visibility for thought leadership, events, and reports
- Helped strengthen Check Point's digital presence and audience engagement



Marketing Campaigns

Check Point executed large-scale marketing campaigns across every touchpoint, including web, social media, digital ads, billboards, and event signage, to build brand awareness, support product launches, and reinforce its position as a cybersecurity leader.

Role

- Served as art director and design manager, leading visual direction
- Partnered with marketing to align creative with strategic messaging
- Oversaw campaign production and guided junior designers

Impact

- Produced high-visibility campaigns such as One Step Ahead
- Delivered cohesive visuals across channels and formats
- Elevated brand perception and recognition on a global scale



Various Campaign Assets: Billboard, Print Ad, Mobile Ads, Booth Design

UX, Web and Digital Design

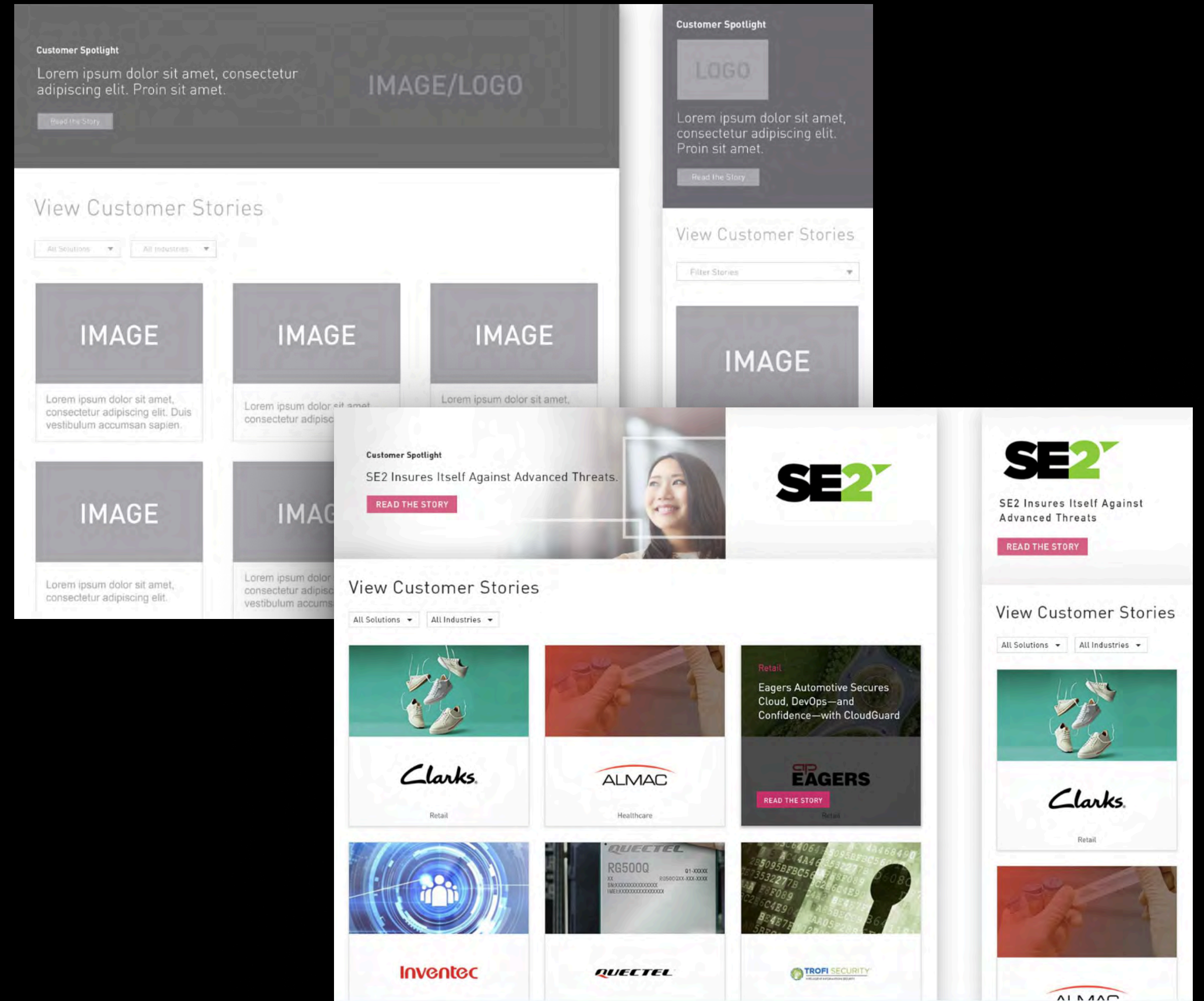
At Check Point, I was responsible for maintaining and evolving the company’s digital presence through routine website updates and periodic UX/UI audits. Updates included campaigns, reports, news, and refreshed visuals to keep content accurate and on brand. Audits provided opportunities to address CMS or structural issues, improve accessibility, and enhance overall usability.

Role

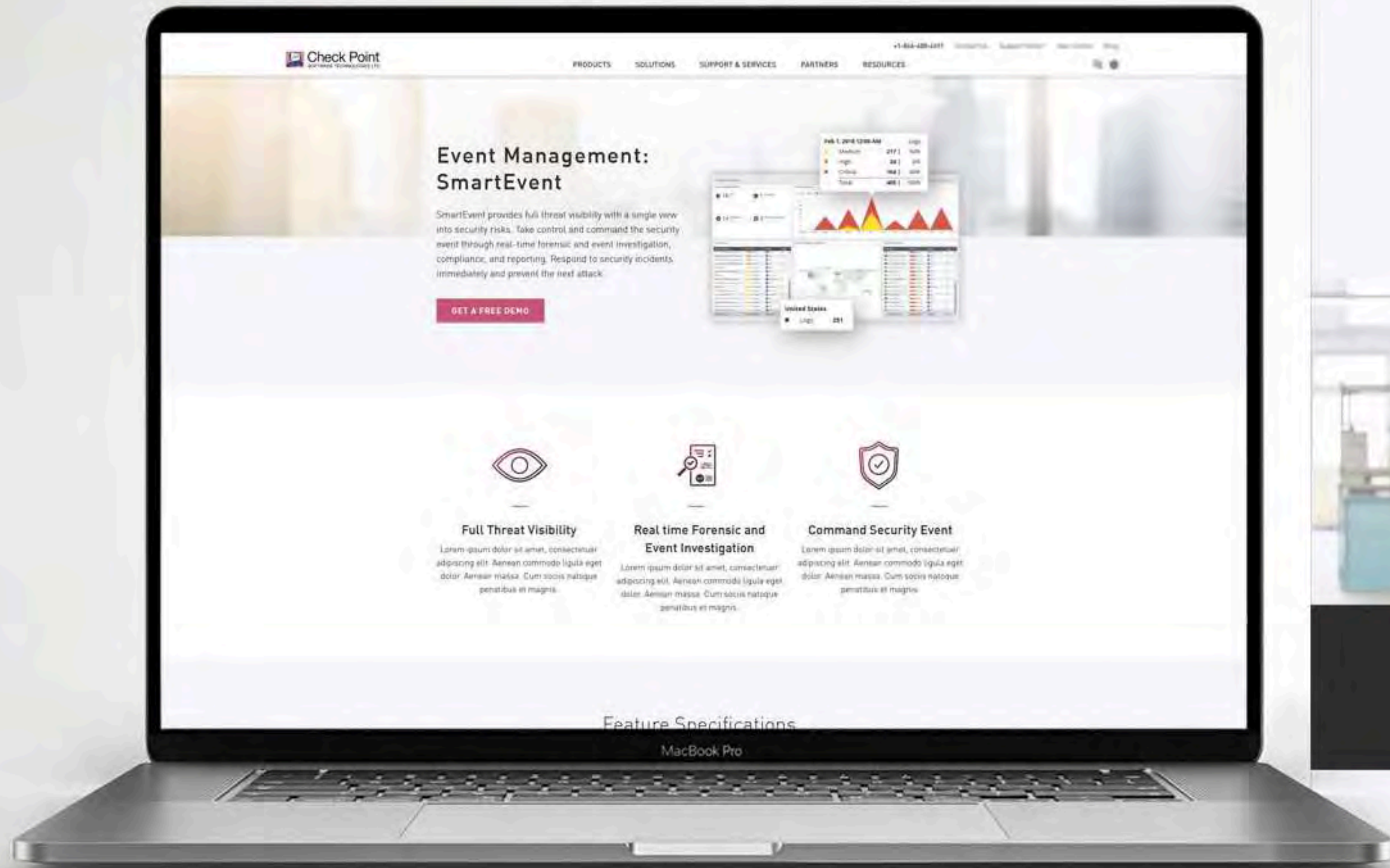
- Managed ongoing content updates
- Conducted UX/UI audits to identify usability and accessibility improvements
- Enforced design systems and brand standards to ensure consistency and scalability across all digital channels

Impact

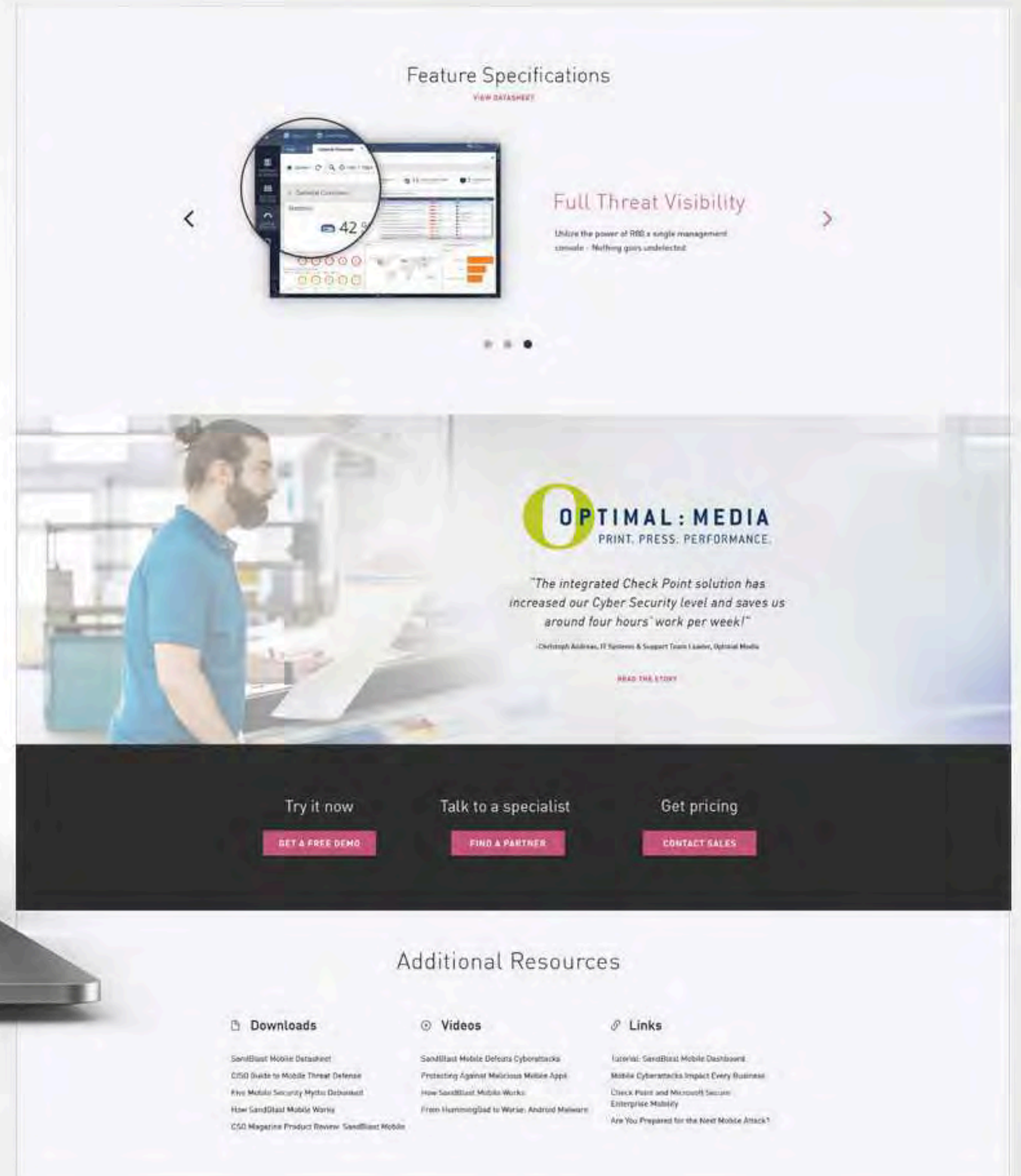
- Streamlined updates with clear workflows and prioritization.
- Built scalable systems and processes to keep the site fresh and user-friendly.
- Improved website usability, engagement, and conversions.



UX/UI Audit for the Customer Testimonials Page - Wireframe and Design Comp



Website Design



Downloads

- SandBlast Mobile Datasheet
- CSO Guide to Mobile Threat Defense
- Five Mobile Security Myths Debunked
- How SandBlast Mobile Works
- CSO Magazine Product Review - SandBlast Mobile

Videos

- SandBlast Mobile Defends Cyberattacks
- Protecting Against Malicious Mobile Apps
- How SandBlast Mobile Works
- From Hummingbird to Wiper: Android Malware

Links

- Latest: SandBlast Mobile Dashboard
- Mobile Cyberattacks Impact Every Business
- Check Point and Microsoft Secure Enterprise Mobility
- Are You Prepared for the Next Mobile Attack?



Protect Your Users On
All Platforms With
ZoneAlarm®

**YOUR USERS'
LIVES ARE ONLINE,
ARE THEY SECURE?**

THERE IS A THREAT Every day there are 2M new mobile threats. Such as man-in-the-middle through Wi-Fi, phishing and malwares.

SENSITIVE INFORMATION ON PHONES Users have on their mobile device sensitive content such as financial credentials, photos, videos and e-mails.

PHONES ARE NOT PROTECTED While most of the users have an Antivirus on their PC, their mobile phone is not protected.



SECURITY SOLUTIONS FOR ALL DEVICES



PC

[Learn more](#)



Android

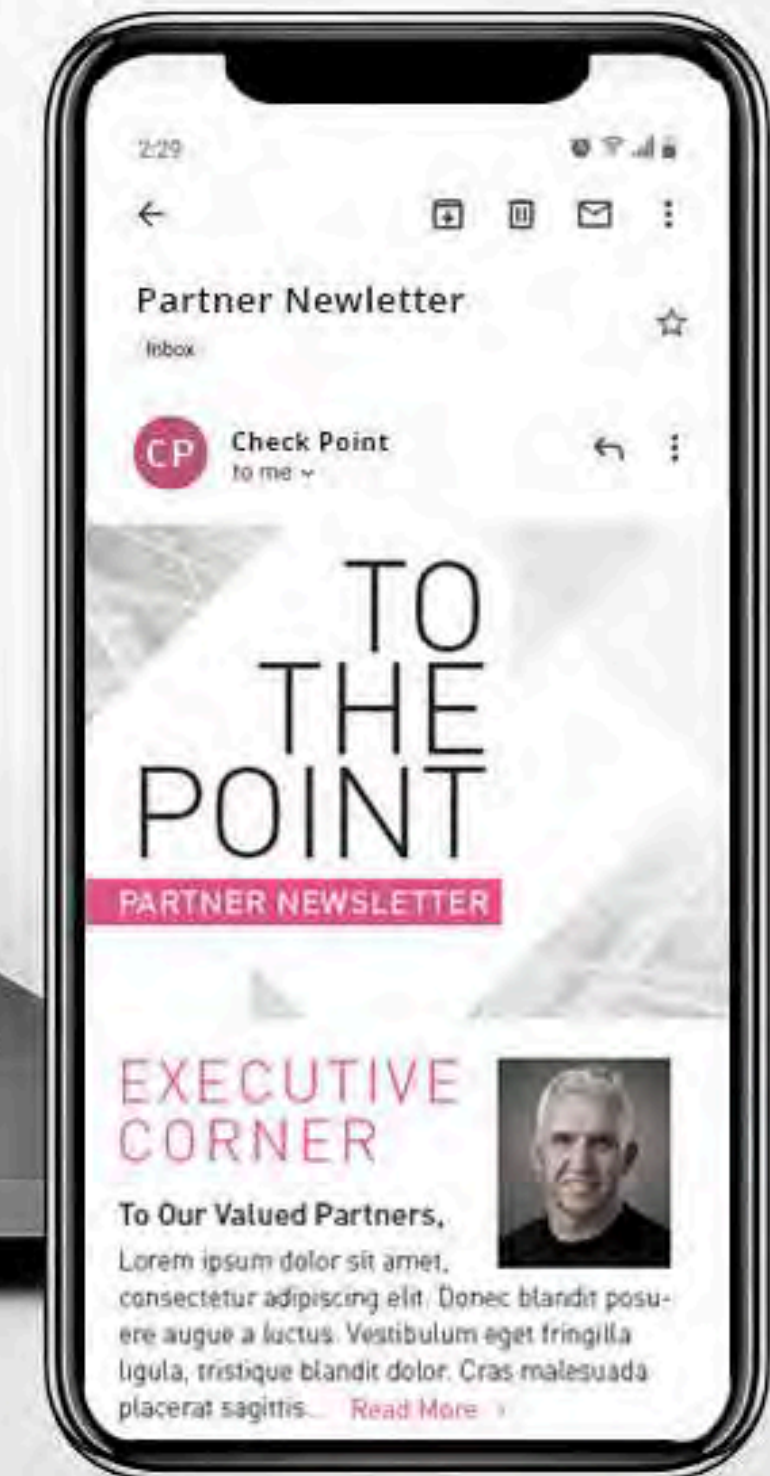
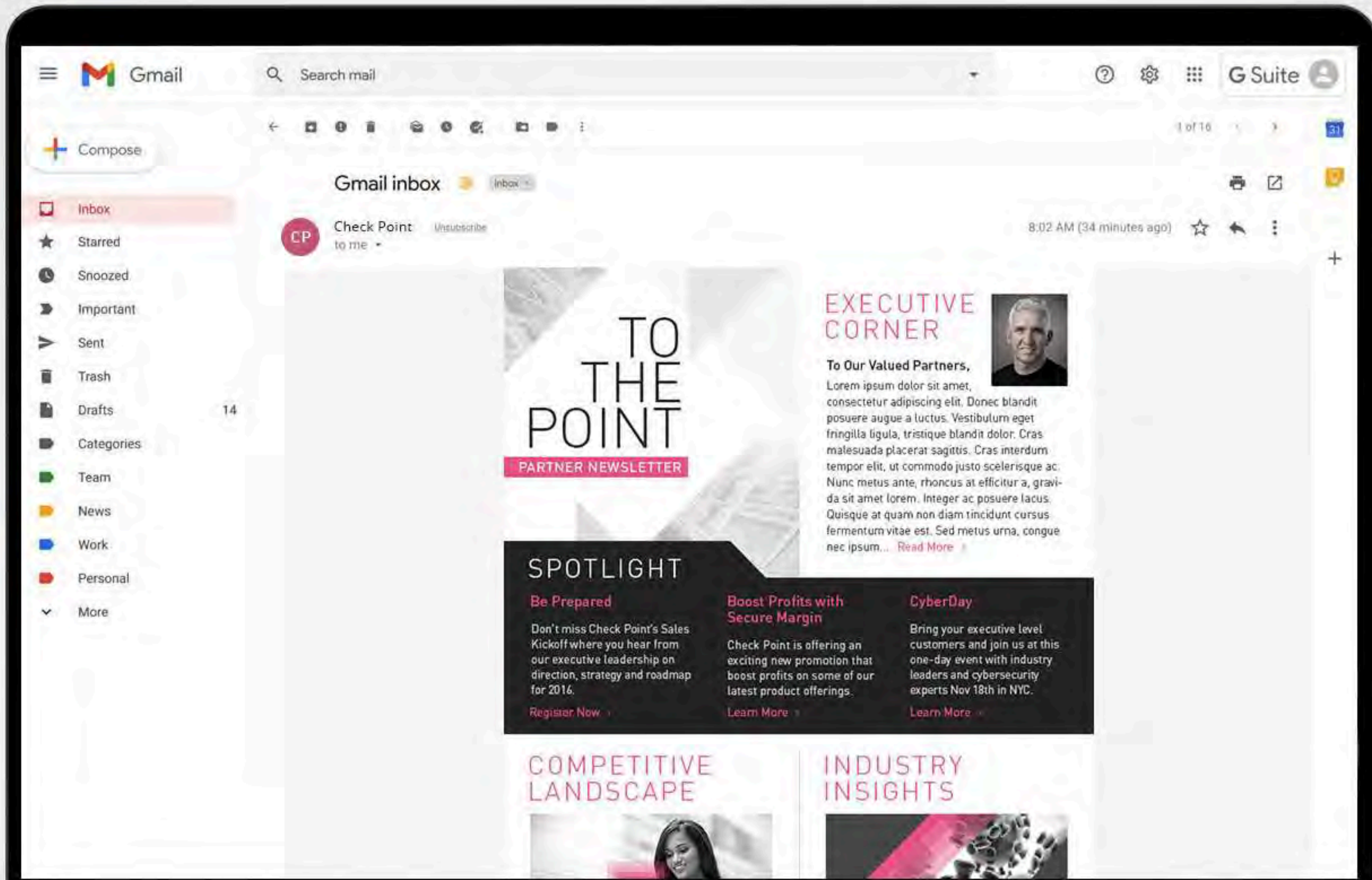
[Learn more](#)



iOS

[Learn more](#)

MacBook Pro



Email Marketing Template for a Partner Newsletter

Check Point Software

Mobile Partner Resources App

Check Point's global sales partners needed quick access to tools, product info, and updates on the go. To meet this need, we launched a mobile Partner Resources App that centralized sales tools, product catalogs, deal registration, service requests, and real-time security alerts in one easy-to-use platform.

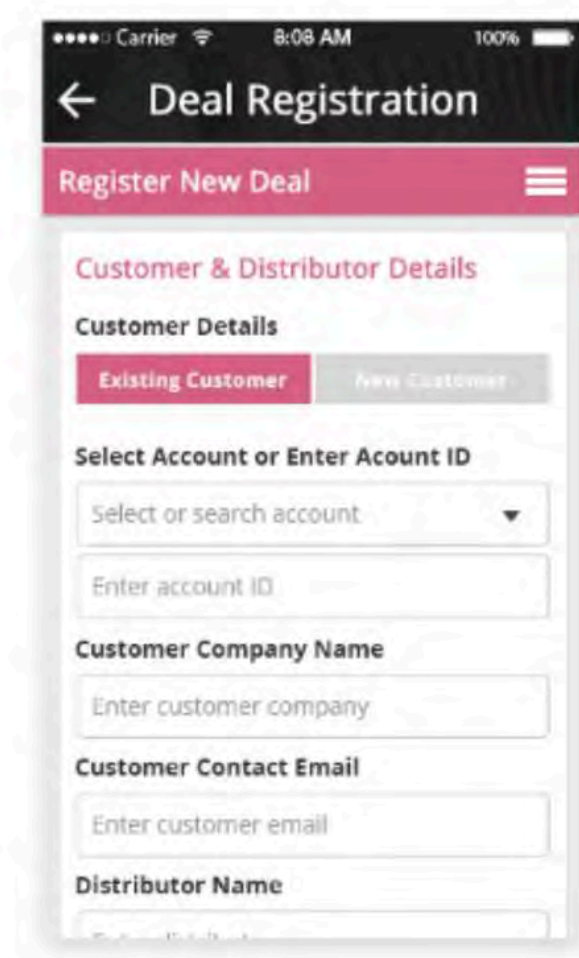
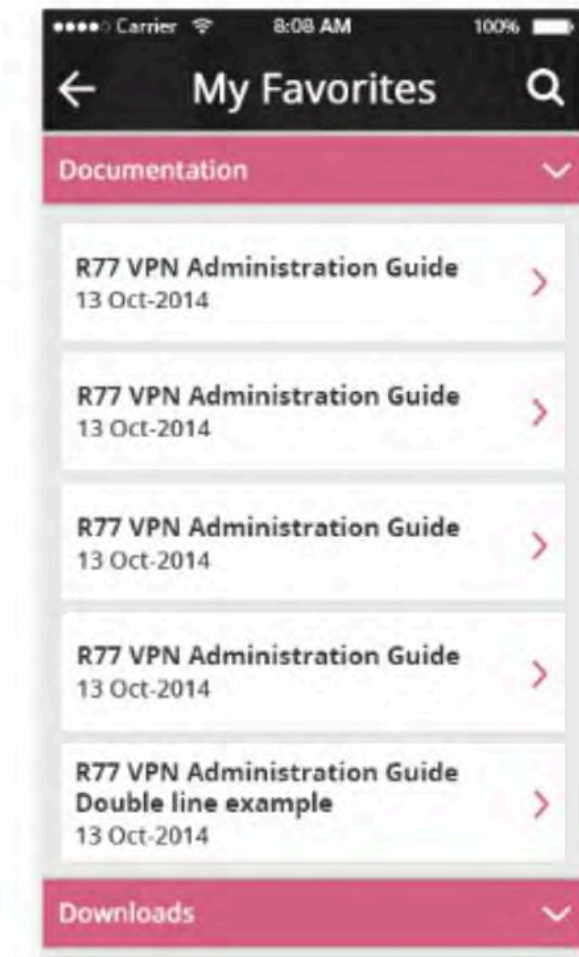
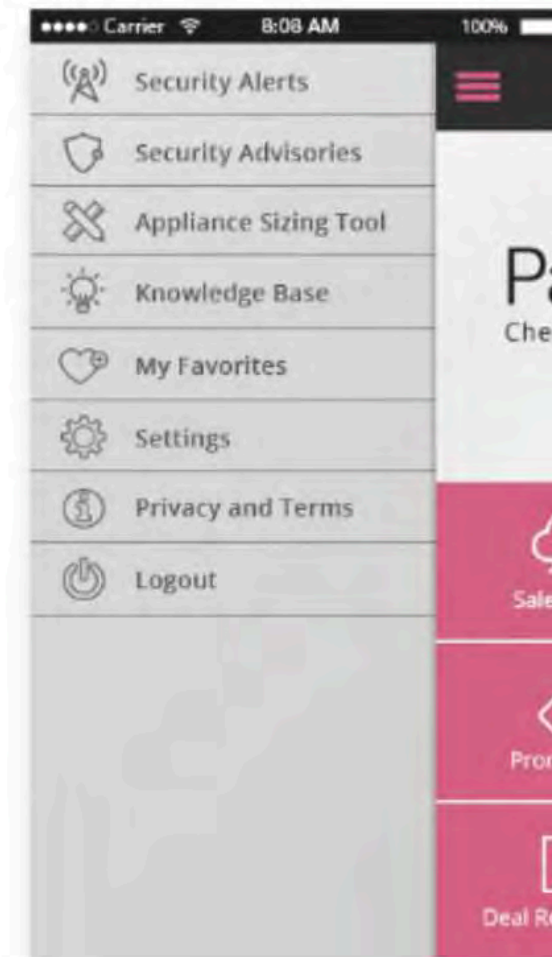
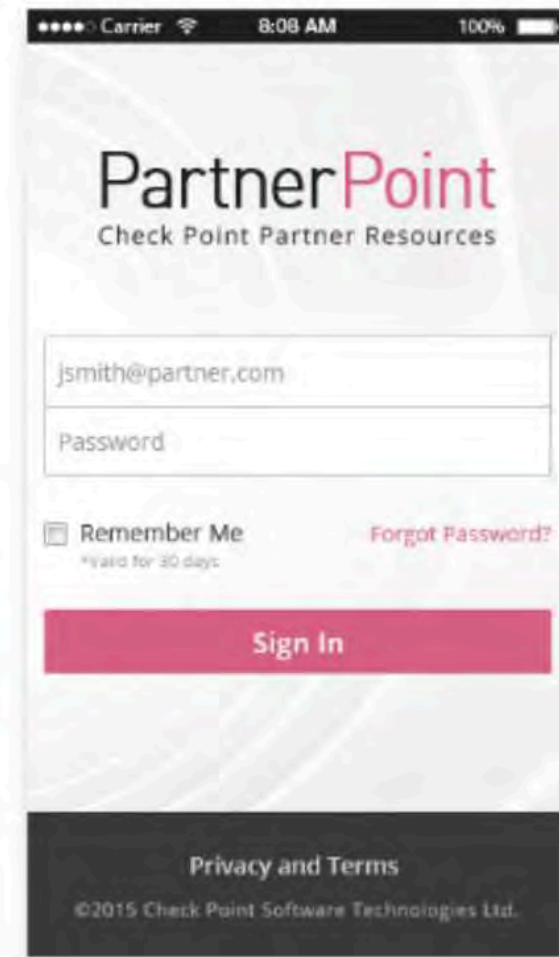
Role

- Created the full user interface, designing a clean, intuitive, and mobile-friendly experience.
- Partnered with sales, digital marketing, and engineering teams to align the app's design with business needs and technical feasibility.
- Produced layouts, navigation flows, and visual components consistent with Check Point's brand while ensuring usability across devices.

Impact

- Delivered a unified, on-the-go resource hub that improved partner productivity and engagement by consolidating scattered resources into one streamlined mobile experience.





Multiple screens from the mobile app

Design Systems, Ops and Strategy

With multiple teams producing content and design, Check Point faced challenges around consistency, scalability, and efficiency. To solve this, I created design systems and operational workflows that aligned design, development, and marketing efforts.

Role

- Served as Design Manager, leading projects from initiation through delivery
- Designed and implemented systems for governance, consistency, and scalability
- Partnered with cross-functional teams to ensure adoption and usability

Impact

- Established a digital style guide to standardize design and development
- Built a content catalog to keep structures and components consistent
- Developed a digital asset library to streamline requests and reduce duplicate work
- Created PowerPoint and campaign templates to support scalable, on-brand communication
- Result: faster workflows, greater consistency, and smoother collaboration across teams

Projects

22

Digital Styleguide

23

Content Catalog

24

Digital Assets Library

25

PowerPoint Templates

Design Systems

Digital Styleguide

Responsibilities:

Led the project from start to finish, covering project initiation, content and design strategy, and implementation.

Deliverables:

- PDF Reference Document
- XD templates
- Wordpress implementation

Overview:

During the website redesign I led the creation of a new digital style guide to establish clear standards for the new updated design.

I collaborated closely with the design and development teams to integrate this into our CMS and provided guidance and support to the team so they could apply it consistently across all new website additions.

Color Palette

PRIMARY

- Brand Pink #E65484

ACCENTS

- Dark Pink #C2783F
- Orange #E15434

GRAVITY

- White #FFFFFF
- Light Gray 1 #F7F8FA
- Light Gray 2 #F2F2F2
- Light Gray 3 #E0E0E3
- Med Gray 2 #808080
- Dark Gray 1 #555555
- Dark Gray 2 #333333
- Black #000000

GRADIENTS

- Dark Pink to Brand Pink
- Brand Pink to Orange
- Dark Gray to Brand Pink

Background Colors

STANDARD COLORS

- White #FFFFFF
- Light Gray 1 #F7F8FA
- Light Gray 3 #E0E0E3
- Dark Gray 2 #333333

Backgrounds (cont.)

COMBINING BACKGROUNDS

When using gradients on images, make sure there's enough contrast between them.

COMBINING BACKGROUNDS

Padding Example A
Header padding will be same pixel as header font size unless with body copy.

Padding Example B
Header padding will be same pixel as the largest word in the header and subheader.

Navigation

TABS

blog.checkpoint.com (main navigation)

All Corporate Blog Cloud Security | Check Point Research

blog.checkpoint.com

Windows and Mac Android and iOS Browser

Font Specs

LINE HEIGHT AND WEIGHTS

- Light
- Light Italic
- Regular
- Regular Italic
- Medium
- Medium Italic
- Bold**
- Bold Italic**

Regular Condensed
Bold Condensed

Typesetting (padding)

HEADING

- H1-50px Line Height- 60px Character Spacing- 16
- H2-40px Line Height- 50px Character Spacing- 16
- H3-30px Line Height- 40px Character Spacing- 16
- H4-24px Line Height- 34px Character Spacing- 16

BODY

- B1-10px Weight- Regular Line Height- 26px Character Spacing- 16
- B2-19px Weight- Regular Line Height- 29px Character Spacing- 16
- B3-21px Weight- Regular Line Height- 31px Character Spacing- 16

SMALL TEXT

- SMTX- 14px Line Height- 24px Character Spacing- 16

PROON EXAMPLE A.1

Mobile Secure Workspace 30px

The proliferation of personal mobile devices in the workplace has blurred the line between business and personal, leading to more security vulnerabilities for your company. Check Point Capsule Workspace mobile security container creates an isolated corporate workspace on personal devices, making it simple to secure corporate data and assets both inside and outside the corporate network.

H1 Regular • B3

PROON EXAMPLE A.2

Mobile Secure 24px

The proliferation of personal mobile devices in the workplace has blurred the line between business and personal, leading to more security vulnerabilities for your company. Check Point Capsule Workspace mobile security container creates an isolated corporate workspace on personal devices, making it simple to secure corporate data and assets both inside and outside the corporate network.

H2 Medium • B1

PROON EXAMPLE B

Mobile Secure Workspace 24px

Mobile Secure Workspace 20px

H1 Regular • H2 Light

Selectors

CHECKBOXES

- Inactive state
- Active State 1
- Active State 2

RADIO BUTTONS

- Inactive state
- Active State 1

TOGGLES

- Off On
- Off On

Inputs/Drop Downs

TEXT FIELDS

Search your products Search Support Center

blog.checkpoint.com (main navigation) **supportcenter.checkpoint.com/supportcenter/portal**

blog.checkpoint.com/learn/results/

Design Systems

Content Catalog

Responsibilities:

Led the project from start to finish, covering project initiation, content and design strategy, and implementation.

Deliverables:

- PDF Reference Document
- XD templates

Overview:

Once the website redesign finished, I noticed that with so many different content creators involved, future updates and new pages could easily become inconsistent. I wanted to create a solution that would keep page structures, content components, and design formats consistent going forward.

To solve this, I developed a content catalog that served as a shared reference point. I collaborated with marketing, product, and development teams to make sure it met everyone's needs and was easy to use.

As a result, the workflow from content to design to development became much smoother. Updates stayed consistent with the new design, and new pages were delivered faster with far less friction between teams.

Product Pages - Main Levels of Content

L1 - Product Hero Banner

L2 - Key Benefits

L3 - Technical and Feature Specs

L4 - Customer Reference

L5 - Call to Actions

L6 - Additional Resources

L1 Banner

L2 Key Benefits

L3 - Technical and Feature Specs

L4 - Call to Action (CTA)

L5 - Customer Successes

L6 - Additional Resources

Design Systems

Digital Assets Library

Responsibilities:

Oversaw the development and upkeep of the asset library.

Deliverables:

- Asset Database
- Photoshop and XD templates
- Reference Document

Overview:

Our graphics team had a basic system for storing digital ads, campaigns, and website assets, but it wasn't efficient. We were constantly bombarded with requests. We all agreed we needed a better solution, and my role was to create a centralized digital asset library to organize and streamline the process.

In collaboration with the Creative Director and a team of 2 designers, we built the database with images, banners, icons, and reusable campaign templates, all organized in an accessible location on our internal server. I also developed a 35-page PDF guide with specifications, style preferences, and submission requirements so teams knew exactly how to use and request assets.

This streamlined the asset request process, reduced duplicate work, and made handling the high volume of requests much smoother for everyone.

nav-featured-image-352x332

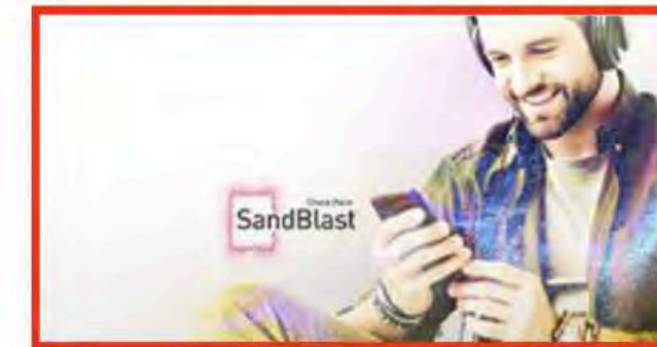
- *all ads have a thin border (follow specs in PSD template)
- *keep upper left portion of the image clear for text
- *submit image w/o text to web team



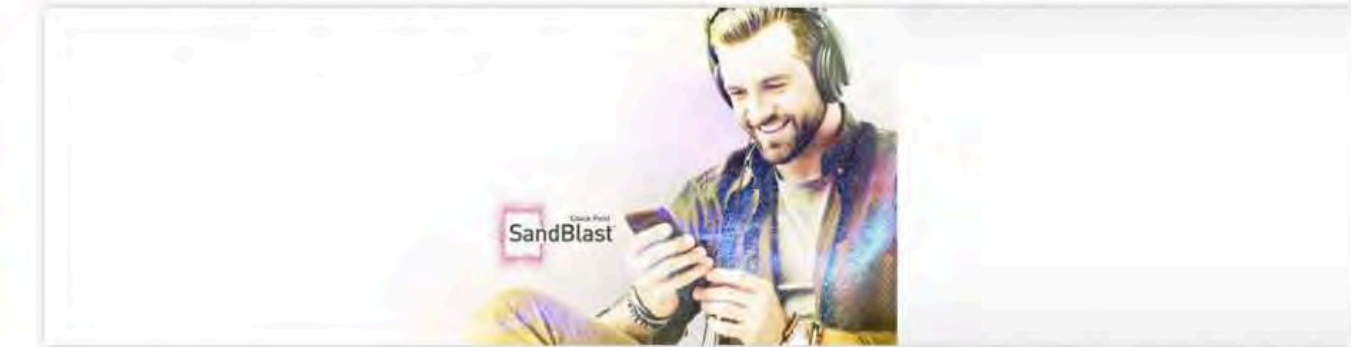
Character Count Specs



customer-thumbnail-image-350x177



customer-hero-spotlight-1170x300



Customer Logo

Size varies on format but make sure the final logo is larger than actual viewing size and has a transparent background.



homepage-product-icon-232x204



Design Systems

PowerPoint Templates

Responsibilities:

Led the project from start to finish, covering content and design strategy, and implementation.

Deliverables:

PPT Templates

Overview:

I developed a series of PowerPoint templates for reports, pitches, and meetings. Each template included structured layouts with placeholders for text, images, and charts, making them easy to customize.

I worked closely with stakeholders to gather feedback and refine the templates so they met team needs while staying consistent with the brand.

The result was that presentations became quicker to build, more professional, and consistent with the company's brand, no matter which team was creating them.

