FORTINET

Brand Guidelines

2019 Q1 – Version 1.0

Table of Contents

Brand Identity

Brand Overview

A brand is shaped by the sum of an organization's visual and written content assets, as well as the experiences employees, customers, partners, and others have with the brand.

The value of brand awareness and engagement is not based the quantity of interactions a customer, partner, employee, or others have with our brand but the quality and relatability of the interaction.

POSITION STATEMENT

Fortinet delivers the promise of security—empowering customers to realize digital innovation, improve business performance, and achieve the most advanced and efficient protection available.

ATTRIBUTES

We are dedicated
We are resourceful
We are agile
We are resolute
We are prescient

TONE

Engaging
Authentic
Optimistic
Astute
Assuring

SENTIMENT

Powering the secure [business]

Design Concept

Research shows B2B brands connect better when they employ emotive rather than rational experiences. The visual identity plays a pivotal role in invoking an emotional response and connecting the brand with core messages.

1. Empowering

Optimistic, progress-oriented photography that pops through the saturation of the protection coloring, creating a sharp connection to the success of the subject.

2. Protection

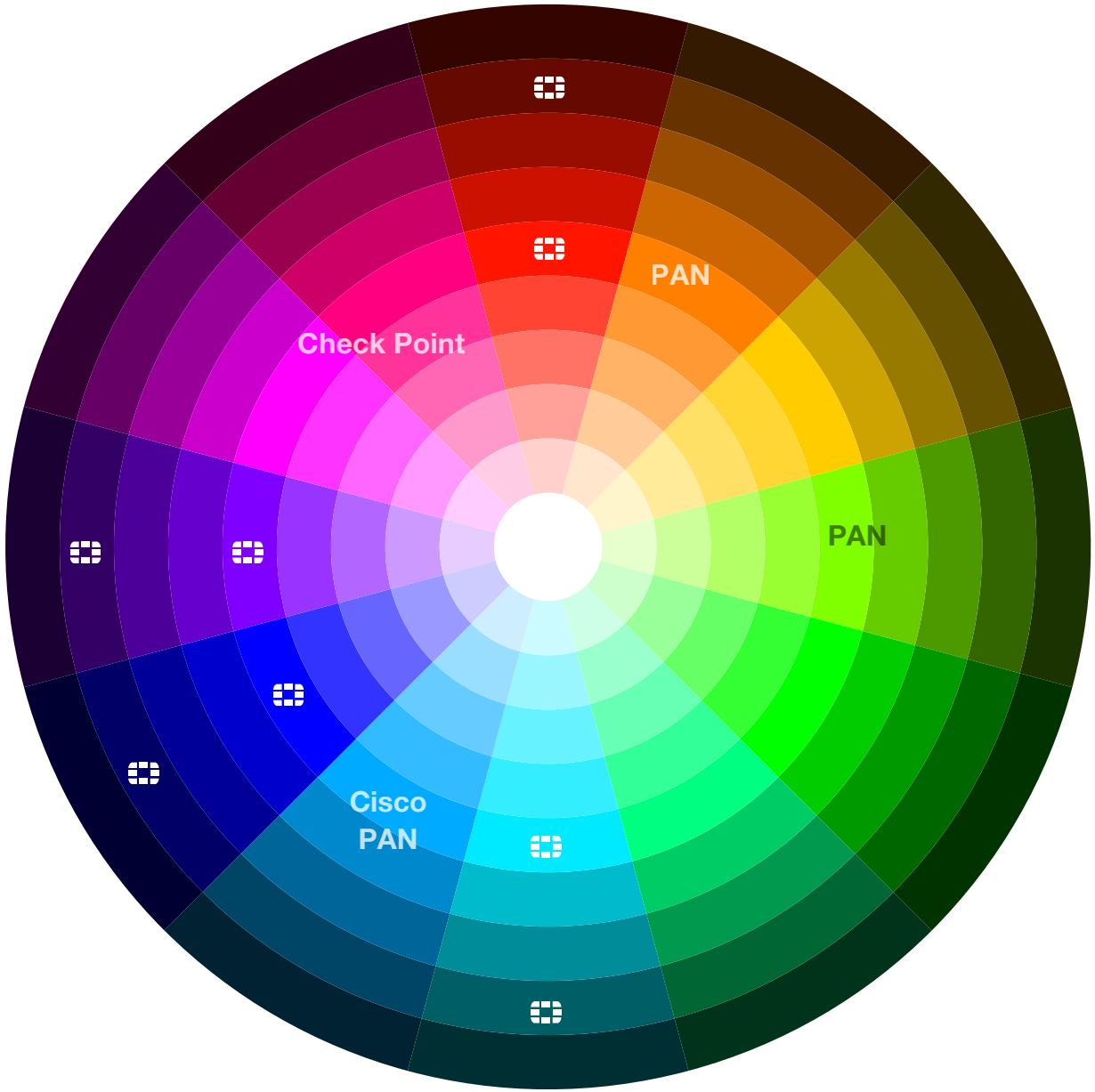
Color from the rays saturating through the image around the subject produces an alignment to the comprehensive protection that is tied to performance.

3. Performance

Bursting rays are centered on a primary artifact within the photography to instill emotive energy.

Brand Color Selection

Brand colors have been carefully selected to represent Fortinet and to differentiate us from competitors.



Color Palette

Brand Colors

have been carefully selected to represent Fortinet and differentiate us from competitors. Feature these colors in your design. Avoid combining multiple brand colors in the same composition. To maximize impact, reserve Fortinet Red for emphasizing key elements in your design. Darker shades add variety and should be used alongside their corresponding brand color.

RED PMS 485C HEX DA291C C0 M95 Y100 K0	**TEAL** PMS 310C HEX 6AD1E3 C48 M0 Y0 K0	**BLUE** PMS 285C HEX 0071CE C91 M53 Y0 K0	**PURPLE** PMS 265C HEX 9164CC C53 M68 Y0 K0
DARK RED PMS 7421C HEX 651D32 C18 M100 Y45 K67	**DARK TEAL** PMS 3035C HEX 003E51 C100 M30 Y19 K76	**DARK BLUE** PMS 288C HEX 002D74 C100 M87 Y27 K19	**DARK PURPLE** PMS 273C HEX 24135F C62 M80 Y0 K63

Neutral Colors

complement the brand palette and can be used alongside them or on their own when a topic is not featured.

LIGHT GRAY PMS 7541C HEX D9E1E2 C7 M1 Y3 K2	**GRAY** PMS 7544C HEX 768692 C35 M14 Y11 K34	**DARK GRAY** PMS 7546C HEX 253746 C73 M45 Y24 K66	**BLACK** PMS 7547 HEX 131E29 C99 M74 Y31 K84

Secondary Colors

should never be featured in your designs. Use them sparingly in charts, graphs, or diagrams to denote status or warnings.

ORANGE PMS 151C HEX FF8200 C0 M49 Y100 K0	**GREEN** PMS 7480C HEX 00BF65 C100 M0 Y47 K25	**YELLOW** PMS 109C HEX FFD100 C0 M18 Y100 K0

Color Schemes

Color schemes align with Fortinet's four key markets areas.

The dark scheme

features a dark background color paired with the corresponding brand color inside the rays. Fortinet red can be used with any dark scheme to emphasize key elements of the design.

The bright scheme

features a bright background color paired with the corresponding dark shade inside the rays. This scheme does not offer enough contrast for Fortinet red and should be used with the white logo.

The light scheme

features a white background paired with a brand color inside the rays. Fortinet red can be used with any light scheme to emphasize key elements to the design.

Typography

Helvetica Neue LT Pro is the primary typeface for Fortinet. It is available for digital and print communications.

Due to license cost and restrictions, distribution of this typeface is reserved for users creating content and graphics on a regular basis on behalf of Fortinet. If you need a copy of this typeface, please send an email to brand@fortinet.com.

Helvetica Neue LT Pro 85 Heavy
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQq
RrSsTtUuVvWwXxYyZz1234567890!@#$%&*

Helvetica Neue LT Pro 75 Bold
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQq
RrSsTtUuVvWwXxYyZz1234567890!@#$%&*

Helvetica Neue 45 Light
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQq
RrSsTtUuVvWwXxYyZz1234567890!@#$%&*

There will be occasions where use of our primary typeface is unavailable. In those instances, please use Arial as a secondary typeface that is available on all OS versions—both Windows and Mac.

Arial Bold
AaBbCcDdEeFfGgHhIi
JjKkLlMmNnOoPpQq
RrSsTtUuVvWwXxYyZz
1234567890!@#$%&*

Arial Regular
AaBbCcDdEeFfGgHhIi
JjKkLlMmNnOoPpQq
RrSsTtUuVvWwXxYyZz
1234567890!@#$%&*

Typographic Style

Typographic style should help convey the intended message and reinforce our brand.

Headline Lorem Ipsum Dolor Sit Amet Consectetur

Set Headlines in title case to maximize legibility.

Lorem Ipsum Dolor
Important Call-Out
Sit Amet

Use the designated brand color to emphasize part of a headline.

Headline Lorem Ipsum Dolor Sit Amet Consectetur

Headlines should be left-aligned or centered to best represent the intended message.

HEADLINE LOREM IPSUM DOLOR SIT AMET

Avoid ALL CAPS for long lines of text.

Lorem **Call-Out One**
Sit Amet Consectetur
Call-Out Two

Avoid multiple call-outs, weights, or colors in the same headline.

Headline Lorem Ipsum Dolor Sit Amet Consectetur

Do not right-align text.

Photography Style

Those entities that benefit from Fortinet solutions—customers, industries, partners, and end users--are depicted in photography.

Use subjects that reflect the target audience and industry.

Use scenes and environments that are realistic.

Use images with natural lighting and colors.

Avoid using images that are complex or metaphoric that are difficult to understand. Never use imagery that is political, pornographic, religious, or offensive in any manner.

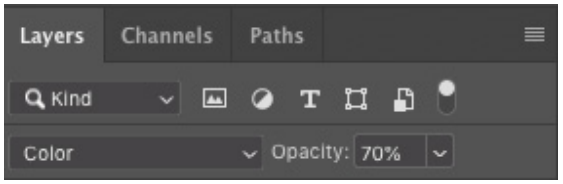
Avoid images that appear overly produced or staged.

Avoid filters or special effects that distort the image.

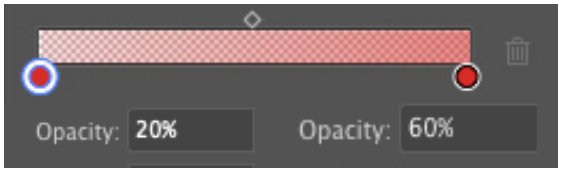
Graphic Treatment Style

Use subjects that reflect the audience—end-user persona and industry—and employ scenes and environments that are realistic and use natural lighting and colors.

Isolate the subject in the foreground. Apply selected Fortinet color to background of the image using setting below.



Choose a single focal point and apply the rays treatment. The rays should have straight edges, a variety of angles that overlap, and transparent gradients using Fortinet colors.



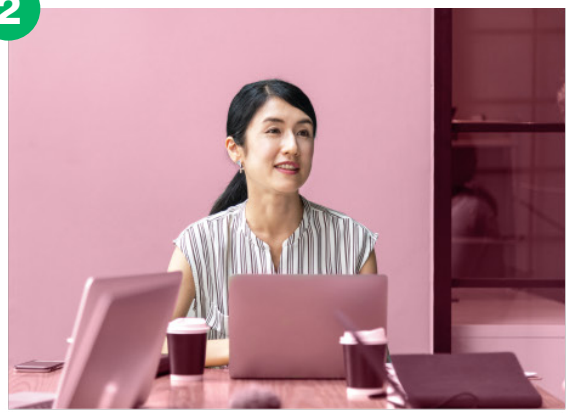
1

2

3

1

2



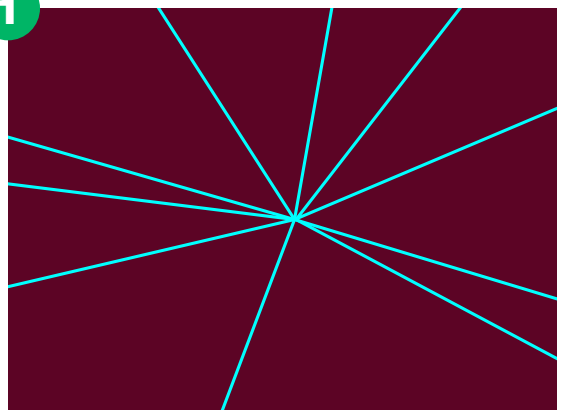
3

Applying the rays

The rays are designed for flexibility and can be adapted to specific designs. The below guidelines should be followed to maintain consistent and appropriate application of the rays.

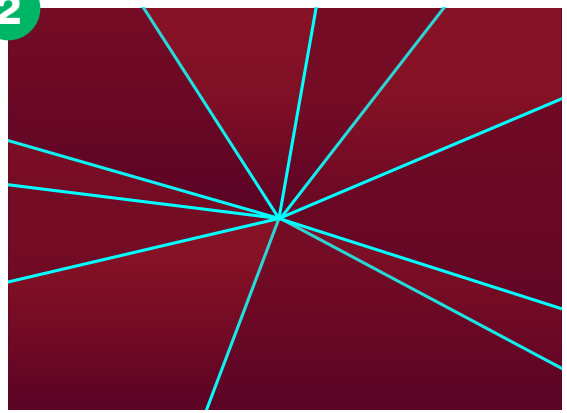
Draw ray shapes from a single focal point to the edges of the image. Overlap the rays to create layers.

1



Fill rays with transparent gradient. Reference the color scheme section for guidelines on selecting colors.

2

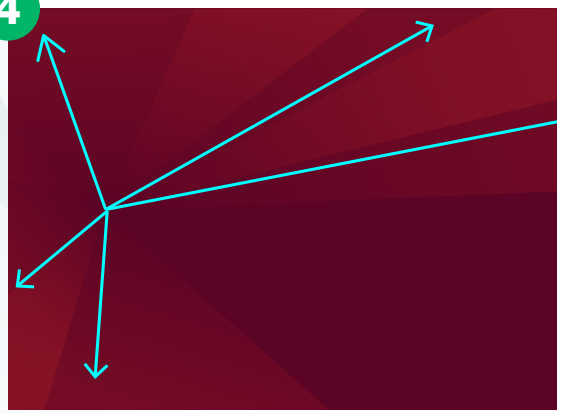


Adjust focal point to fit the design. A section may be removed to reveal content.

3

Adjust gradient direction so the color becomes more opaque as it moves further away from the focal point.

4



If applicable, place the Fortinet logo with the focal point anchored inside the “O” symbol.

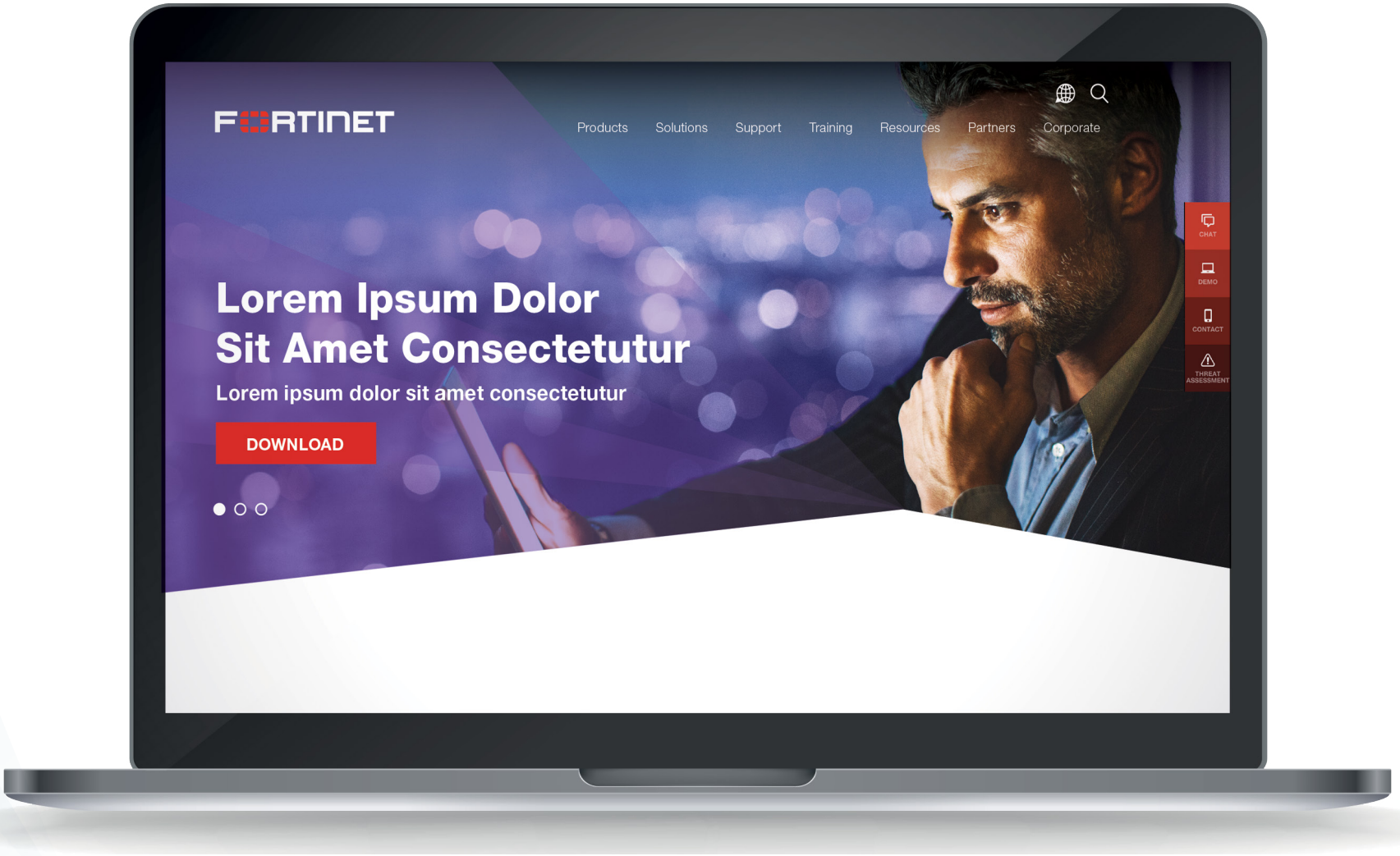
5

If applicable, add a background image and adjust the focal point and ray positions to fit the design.

6

Website Hero Banner

Website hero banners are a great way to engage visitors. Photography and color treatments should reflect core brand concepts—empowering, protection, and powerful—and avoid complexity. Hero imagery is full width and allows space for messaging above the ray graphics.

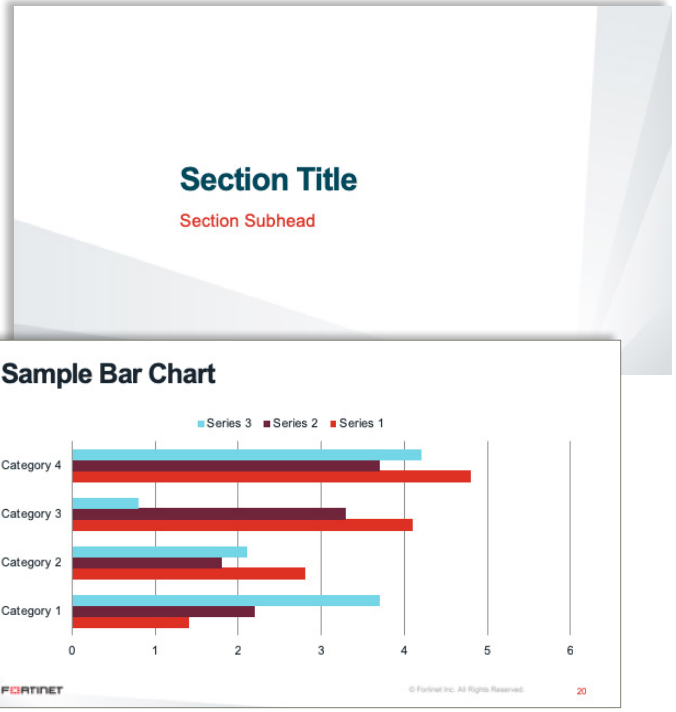


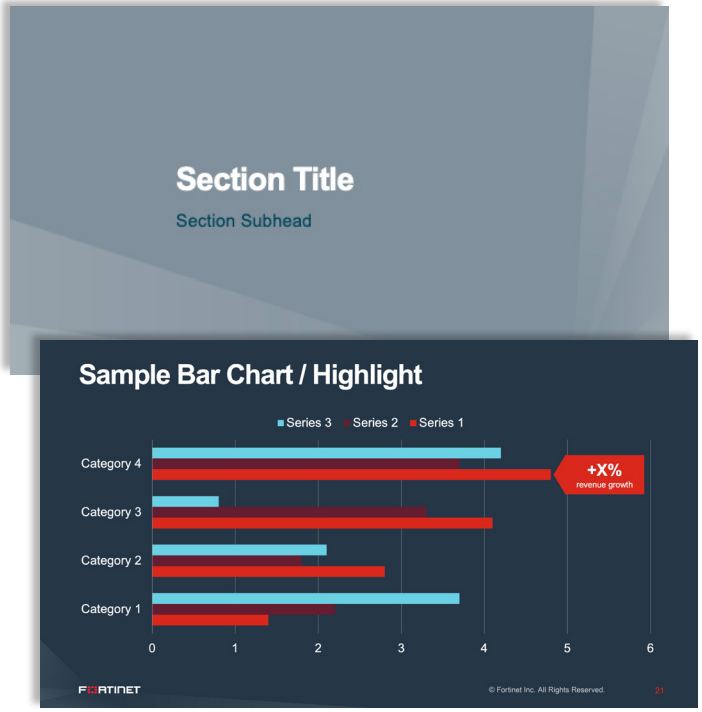
Pull-up Banners

Pull-up banners use imagery and the color scheme that corresponds to its message.

PowerPoint

The PowerPoint template is available as a dark or light theme. Use the light theme for everyday use and reserve the dark theme for keynotes or theater presentations to improve legibility.

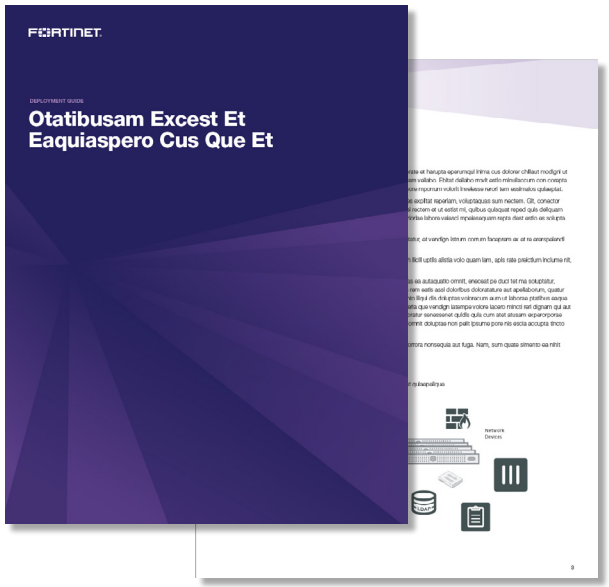




Collateral

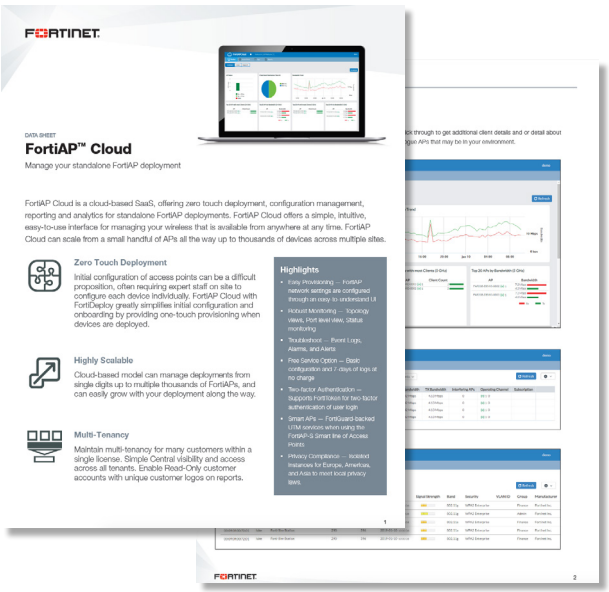
Consistent content design plays a critical role in building and sustaining brand awareness. Templates for each type of content asset are designed for optimal engagement.

Deployment Guide



Solution Brief

Datasheet FPO



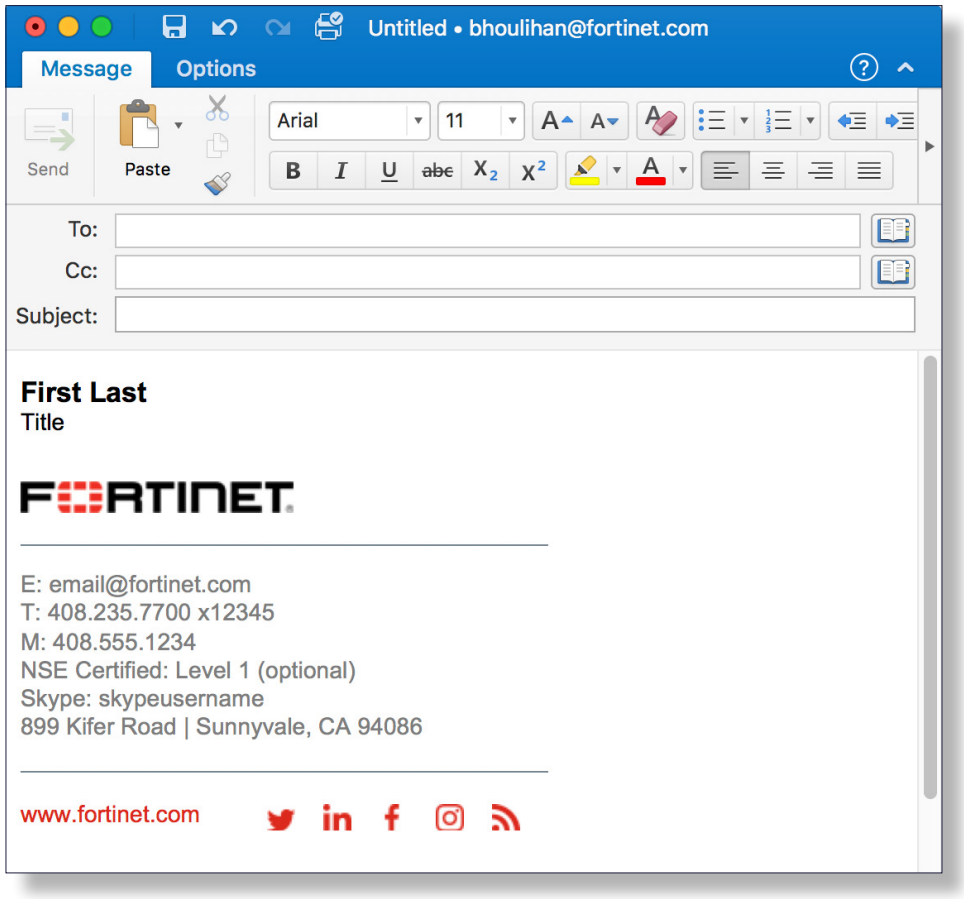
Case Study

White Paper

Ebook FPO

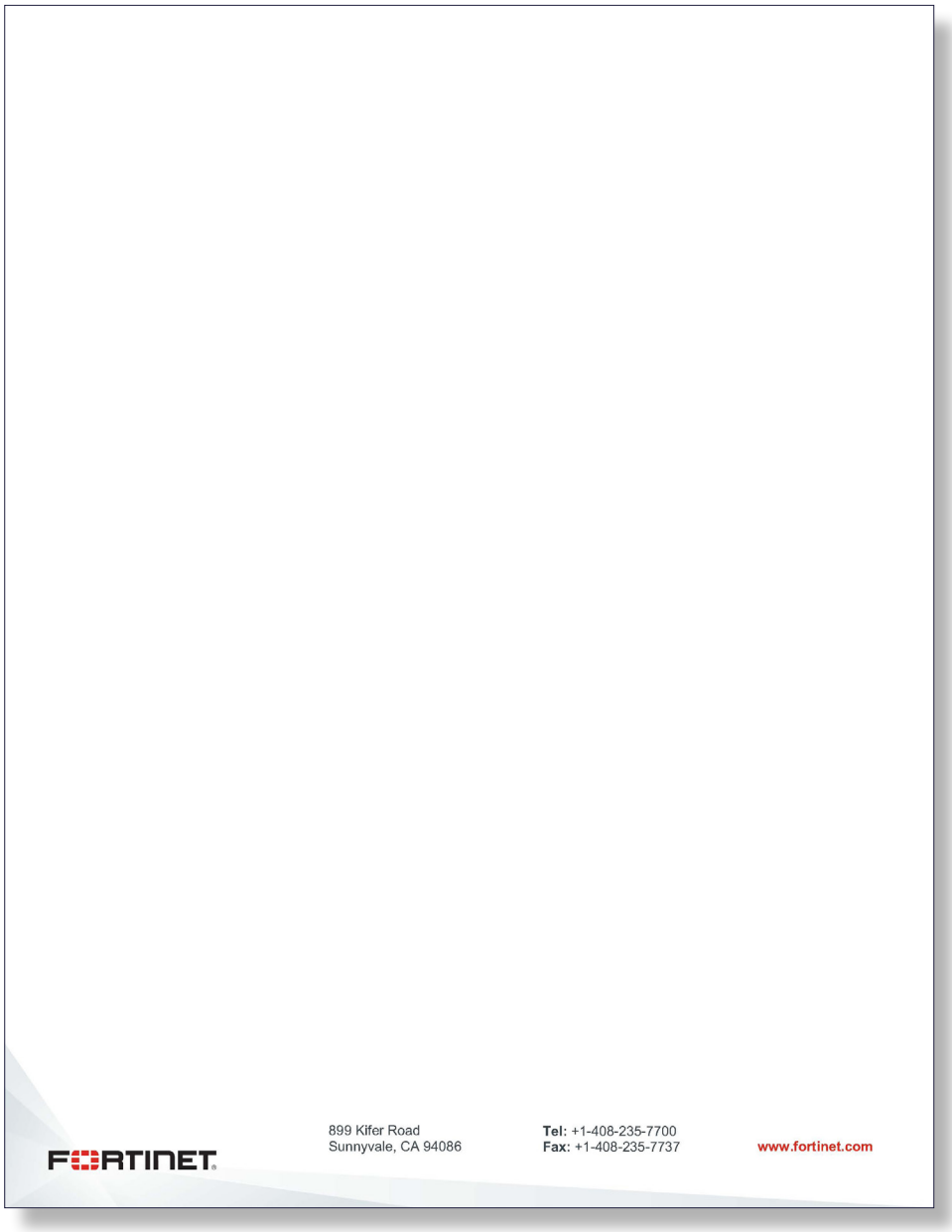
Email Signature

The email signatures should match this template. Contact information may be customized but should follow the established formatting.



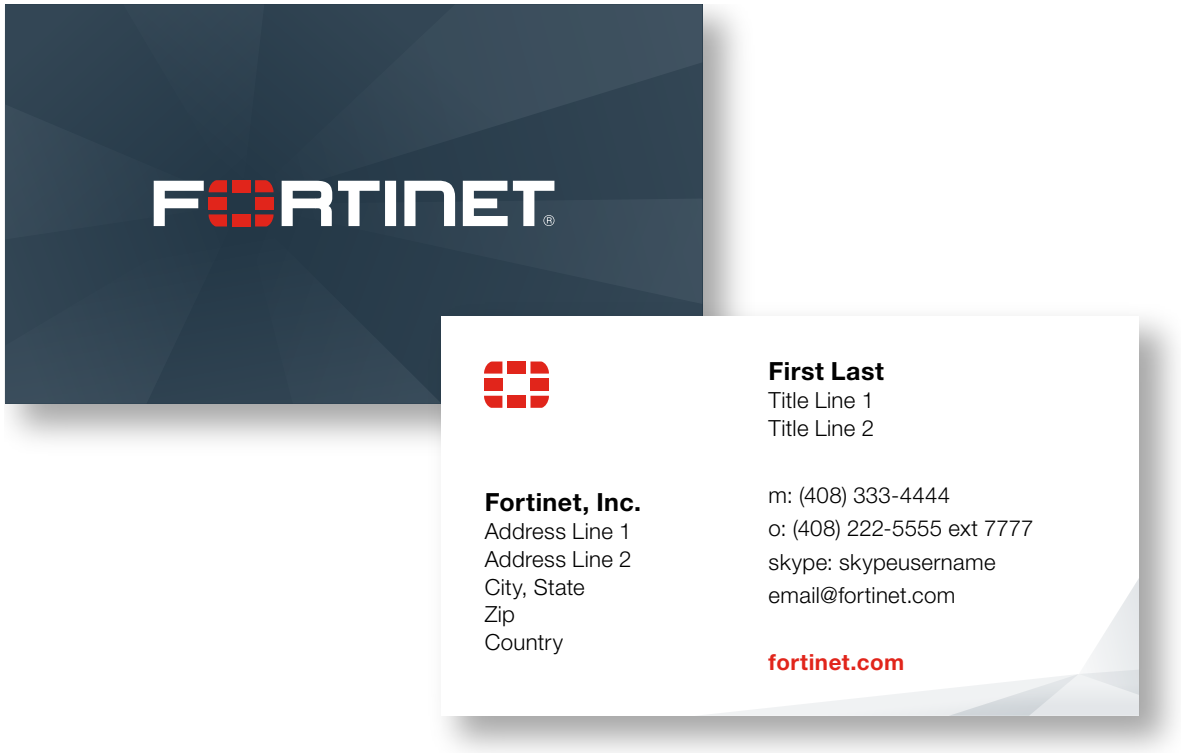
Letterhead

Letterhead is available as an editable word document. Contact information may be customized but should follow the established formatting.



Business Card

Business cards should match this template. Instructions for ordering business cards are available on Fuse.



Fortinet Logo

The Fortinet Logo

The Fortinet logo consists of a graphic symbol combined with logotype that together create a single, unified image.

The symbol replaces the letter “O” in “Fortinet,” becoming an important part of the logo. This symbol is a graphic representation of the top-down view of a castle turret - representing a fortress or security. Each individual letter in the word “Fortinet” has been custom drawn for balance throughout the wordmark. Do not create your own version of the Fortinet logo.

The “®” registered trademark protection is a part of the logo artwork and must never be removed. It may be enlarged in instances where legibility is a concern.

The primary version of our logo is red and black and should be used wherever possible. However, when used over color or imagery, there is often not enough contrast for our logo to be readable. In those instances, one color versions of our logo have been created (black and white) for placement over color or imagery background.

Always select and use the version of the artwork that provides the logo with the most contrast and readability.

Download the Fortinet logo:
Print
Digital

LOGO ELEMENTS

CLEAR SPACE

MINIMUM SIZE

SECONDARY LOGO VERSIONS

White and red version

White version

Black version

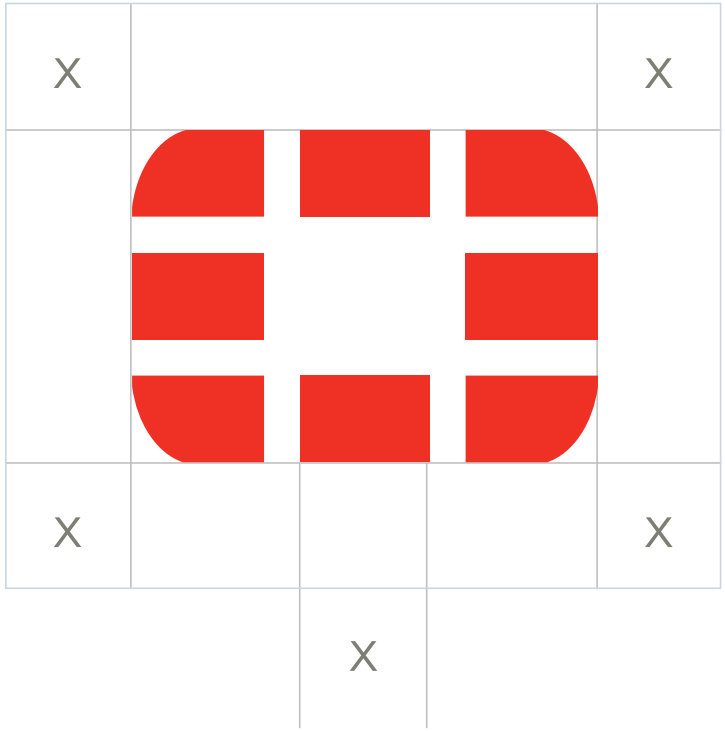
The Fortinet Symbol

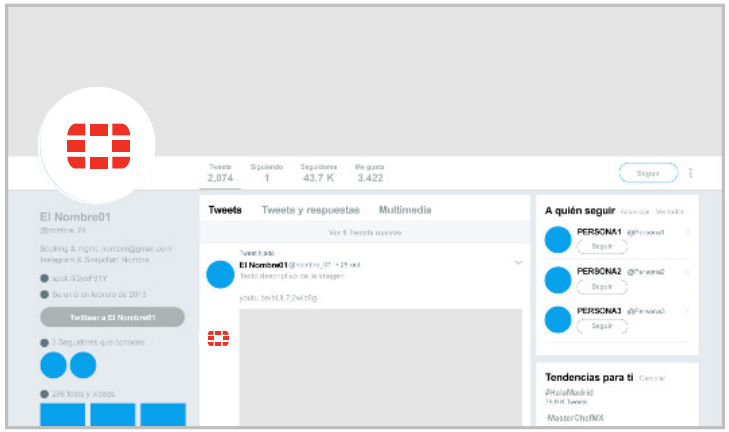
The “O” symbol may be used as a shorthand to represent Fortinet in certain applications.

To maximize recognition, the symbol should be used when the Fortinet brand has already been established.

The symbol may also be employed in instances where there is insufficient room to accurately display the Fortinet logo. Some examples are social media icons or mobile application icons.

If you are ever unsure about the appropriate use of the logo or the symbol, please contact brand@fortinet.com for guidance.





Logo Misuse

Please exercise care when using the Fortinet logo.

Do not modify, change, or otherwise alter any of the logo elements (color, typeface, proportions, etc.)

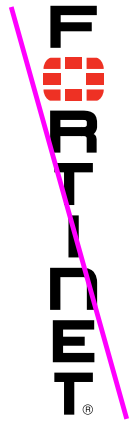
We have prepared several inappropriate uses on this page as examples of what **NOT** to do.

To obtain the official Fortinet logo artwork files, please contact brand@fortinet.com

LOGO MISUSE EXAMPLES

Do not change the size relationship between the symbol and the logotype.

Do not place the logo over backgrounds that do not provide sufficient contrast.



Do not recreate the logo in a vertical format.

Do not compress or stretch the logo, or alter it's aspect ratio in any way.

Do not replace the symbol with other graphics.

Do not add shadows, gradients or other visual effects to the logo.

Do not use the symbol with other text.

Do not create your own type lockup by adding text in close proximity with the logo.

Do not place the logo over visually busy backgrounds.

Do not use the symbol next to the full logo.

Do not combine part of the logo with other words.

Do not use old versions of the logo.

Co-Branding

Many co-branding instances will require the Fortinet logo to be placed side by side with a partner logo (locked up).

The guidelines on this page outline the proper way to construct a lockup with the Fortinet logo.

Each logo should be sized to be optically equal. The left position of the lockup indicates brand dominance in brand-neutral environments.

Fortinet Dominant

Fortinet dominance is established when Fortinet most heavily influences the communications experience—namely, when Fortinet is the foremost driver of the activities depicted or involved. Fortinet dominant experiences rely heavily on the Fortinet visual system for look and feel.

These examples demonstrate conceptually how Fortinet dominant co-branded communications should appear in common marketing vehicles.

Note: When the Fortinet visual identity is in the lead position, the partner logo is placed in a visually subordinate position.

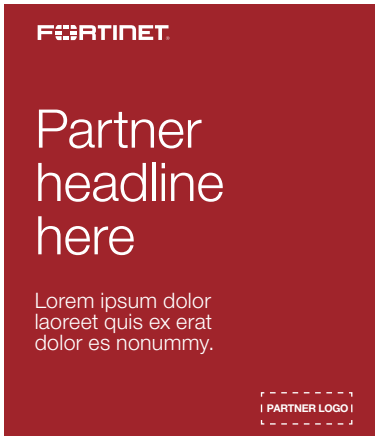
Partner Dominant

Partner dominance is established when the partner brand heavily influences the communications experience. As a result, the partner brand is featured more and the design reflects the partner's visual system. While the execution is driven by the visual system of the partner's brand, the visual display of the Fortinet logo must be compliant with our logo guidelines.

These examples demonstrate conceptually how partner-dominant co-branded communications should appear in common marketing vehicles.

Note: When the partner visual identity is in the lead, the partner logo is placed in the primary position and the Fortinet logo is in a subordinate position.

LOGO LOCK-UP CLEAR SPACE REQUIREMENTS



Communication and Writing

Goals and Principles

The language we use to talk about ourselves, partners, and customers is important. Every industry has a language, and every company chooses to use that language or create a new one. Whoever owns the language, owns the conversations—and the customer.

When it comes to brand, the language we employ plays a pivotal role. Research shows that approximately 45% of our brand image is tied to what we say and how we say it (other 55% is visual).[1] This is more than just marketing content and advertising copy (8% of brand perception); it includes every verbal and written touchpoint—from sales calls, to emails, to text on packaging, to voice mails, to how we answer incoming calls.

The language we use is respectful and truthful. It aims to educate and influence audiences to:

- Change behaviors, expectations, and beliefs. Must provide a rationale for change that does more than simply challenge the status quo, but rather uses storytelling to positively define what change looks like.
- Empower for success: information, support, training, and enablement. Whether providing information, support, training, or enablement, the focus is on empowering customers and partners to succeed—as professionals and organizations.
- Assure or reaffirm decisions and practices. We are confident in our technologies and strategic vision and seek to assure or reaffirm customers and partners that they are protected from threats to their digital assets.

To achieve this, language and content must be:

- **Useful.** Content that has a specific objective and audience in mind and is written to both.
- **Clear.** Subject and audience are well understood and copy is efficient and cogent, employing concise sentences and simple words.
- **Appropriate.** Language needs to be written and adapted per specific personas and situations. It also needs to reflect the particular topic and the type of content being produced.
- **Corroborated.** Claims are factual and validated with data and research.

[1] Lulu Raghavan, "Does Your Brand Sound as Good as it Looks?" Landor, July 29, 2010.

Voice and Tone

The voice and tone of the language we use when writing content plays an important role in conveying brand personality.

Brand voice never changes. It is how we want to act when speaking and writing and is directly tied to our brand attributes: dedicated, resourceful, agile, resolute, and prescient. **Tone changes** depending on the persona to which we are writing and the circumstances.

A. Voice

Cybersecurity is a **serious undertaking**, and the stakes are very high. Flippant and comical language and content runs counter to this reality. A casual or conversational voice implies that neither the audience nor subject is taken seriously enough.

We are also **optimistic** and use **positive language** to inform and encourage rather than employing negative language to scare them into action. We do not define a problem without providing a solution. We **educate** and **assure** rather than create ambiguity and alarm.

At Fortinet, we are confident in our advanced technologies and assure audiences that they perform as advertised, protecting digital assets while enabling business performance.

We always have the best interest of customers, partners, and the cybersecurity industry at heart and build rather than tear down; collaborate rather than criticize and dispute.

All of this means we write copy that is:

1. **Straightforward.** We strip away all hyperbole, never overpromise, and avoid emotional language and metaphors (as they don't always translate). We want to aim for sentences of 20 words or less and to write them so that they can be easily unpacked for translation. Additionally, we should stay away from metaphors and idioms that do not translate (e.g., only relate to U.S. audiences).
2. **Educational.** Network security professionals seek content that provides them with information, helping them solve problems, overcome challenges, and answer questions. While some regional-specific details and examples are important and necessary depending on the content asset, avoid including U.S.-centric examples only whenever possible.
3. **Knowledgeable.** When we write something, we research the subject to gain a comprehensive understanding of the issues and ensure we have corroborating data to back up any claims that we make.
4. **Positive.** Our glass is half full rather than half empty. Rather than dwelling on what can go wrong, we are focused on providing answers and solutions to challenges and problems.

Voice and Tone

B. Tone

Cybersecurity is a serious undertaking and the repercussions of a data breach, operational outage, or compliance violation are grave. Our tone needs to reflect this reality and does not assume a glib or casual tone.

We always consider **context** and **audience** and craft a tone that reflects both. This also factors in the audience's state of mind. Are they unaware they have a problem? Are they already seeking a solution? Are they skeptical and difficult to persuade to change their mind and behaviors? Are you addressing a C-suite executive or technical engineer or specialist who manages the actual security technologies?

Depending on the answer to these and other questions, language tone and the type of content used needs to be adjusted accordingly.

1. **We are engaging.** We create content that is educates or challenges our audience with new information or a different perspective. Content is substantive and simply not a regurgitation of data points and details found in other content—whether generated by Fortinet or third party. We also write in a way that tells a narrative with a sequential flow where the intersections in our argument provide smooth transitions from one point to the next.
2. **We are authentic.** Authenticity is more than simply another word for honesty but rather conveys integrity and full transparency to certain set of principles. The definition of brand authenticity by the *Journal of Consumer Psychology* is helpful here: **"The extent to which [customers] perceive a brand to be faithful toward itself, true to its [customers], motivated by caring and responsibility, and able to support [customers] in being true to themselves."**[2] Our content tone must always remain faithful to our brand proposition and brand attributes, representing our commitment to help customers protect themselves in the most effective and efficient manner possible. We also write to specific personas, humanizing our brand messaging to ensure it relates to the targeted audience.
3. **We are optimistic.** Rather than focusing on what can go wrong, and certainly with cybersecurity there are plenty of negative repercussions, we focus on what can go right when broad, integrated, and automated security technologies and practices are used. Fortinet believes in a cyber world where customers embrace digital transformation with confidence and are excited about the future.
4. **We are astute.** Fortinet understands cybersecurity as well, if not better, than any other organization. This means we accurately assess trends and problems and provide ideas and propose solutions that turn these into advantages for customers, partners, and us. We are the smart "guys" and "gals" on the block but convey this knowledge without smugness or condescention.
5. **We are assuring.** Cyber threats can be unsettling. Their increasing volume, velocity, and sophistication, coupled with well-publicized data breaches, operational outages, and compliance violations caused by them, can paralyze organizations and inhibit business performance. Our brand tone must assure customers that they can protect themselves against advanced threats while ensuring that business performance does not suffer.

[2] Felicitas Morhart, et al., "Brand authenticity: An integrated framework and measurement scale," Journal of Consumer Psychology 25:2 (April 2015): 200-218.

Audiences and Personas

A. Audiences

There are a lot of different entities for which we write content. These organizations represent both public and private sectors and a number of industries that include finance, healthcare, retail, energy, manufacturing, and hospitality, among others.

When these different audience segments are boiled down to a finite number, the below is a good representation:

Large and Midsize Enterprises. Typically, with global operations and thousands of employees, these businesses have dedicated cybersecurity teams that are charged with overseeing cybersecurity strategy and execution.

Small Businesses. These companies range from a few employees to those with several hundred. Depending on the company size, a dedicated cybersecurity headcount may not exist. Cybersecurity is either outsourced or under the charge of the person responsible for IT.

Partners. Fortinet's partner network consists of thousands of distributors, channel partners, resellers, and solution resellers. It also includes over 60 Fabric-Ready Partners.

Investors. A publicly traded company, Fortinet creates content for investors that demonstrates its financial strength and viability of its long-term vision.

Employees. Last but not least are Fortinet's employees who, depending on the circumstances, need to be kept informed, assured, and sometimes challenged.

B. Demand-Gen Personas

These different audiences have disparate personas to whom we write content. Individual personas matter, and the particular buyer or customer journey stage does as well. Thus, Fortinet aspires to create content specific to individual personas and their unique attributes, interests, and challenges. Content also does not cross journey stages. Journey stages for buyers include:

Problem Education. Customer/buyer is unaware that there is a problem and must be educated on it and its implications. *Fortinet-specific content: None.*

Solution Research. Customer/buyer acknowledges there is a problem and seeks guidance in terms of what solution options exist and what criteria should be used to evaluate them. *Fortinet-specific content: Very little.*

Solution Selection. Customer/buyer is ready to make a purchase and needs help sorting between the different solution options and why Fortinet is the best choice. *Fortinet-specific content: All about Fortinet.*

While it is impossible to delve into the details on all of the personas here (ask your Fortinet project sponsor for them), the following are some of our key customer personas:

CIO. Role of the chief information officer (CIO) is rapidly evolving from technologist and IT-delivery tactician to business strategist. Often reporting to the CEO and with ties to the board of directors, CIOs are measured on how they use digital transformation to accelerate the business, tear down walls that inhibit business execution, and transform customer experiences. And even though CISOs—who historically reported to the CIO—are increasingly reporting to the CEO or other executives, security remains a critical mandate for many CIOs—regardless of these reporting changes. They must ensure critical data and assets remain protected while concurrently embracing digital transformation.

CISO/CSO. A few years ago, chief information security officers/chief security officers (CISOs/CSOs) were one of many reports within the IT department and focused on managing firewalls and endpoints and patching vulnerabilities. But this has changed in recent years. CISOs/CSOs are charged with risk management, assessing and managing threats from the data center to the boardroom (as security is a business issue today). Often no longer part of the IT department but rather reporting to the CEO or even board, the CISO/CSO oversees initiatives that are pivotal to the business and ensures the organization's cybersecurity strategy keeps pace with the evolving threat landscape, ever-expanding attack surface, and increasingly complex and onerous regulatory/standards compliance.

Audiences and Personas

VP/Director of Network Engineering. Proliferation of devices, users, and applications and the corresponding amount of traffic these produce make it increasingly difficult for the VP/Director of Network Engineering to meet business SLAs around network availability, reliability, performance, and security. When network outages and performance degradation impact operations and user productivity, the VP/Director of Network Engineering is held accountable. Security has become a critical concern for the VP/Director of Network Engineering as a result of most traffic being encrypted and must be inspected, which impacts network performance. The CISO/CSO and business leaders also demand transparent security visibility across the attack surface and the ability to track and report compliance with industry and security standards.

Security Architect. As the threat landscape has evolved, the security infrastructure has kept pace by adding more and more point products. But traditional security architectures have not evolved. Charged to ensure that all of these security pieces, which often are disparate, are integrated into a coherent network security infrastructure, security architects find themselves hamstrung and under increasing pressure from the CISO/CSO and business. With security elements residing in silos and security resources—staff and budgets—in short supply, security architects must design security systems and processes that provide transparent visibility and control, share threat intelligence in real time between the different security elements, and automate manual tasks for optimal efficiency as well as rapid intrusion detection, prevention, and remediation.

Director/Manager of DevOps. The speed and frequency of DevOps is rapidly increasing, but growing concerns about DevOps security issues places greater burdens on DevOps leaders (90% of security incidents result in exploits of software defects). Discovery of security issues during latter development cycles have a great impact on time to delivery. Additionally, time to delivery is impeded when changes to network security rules and connections are needed. Requires security processes that support continuous deployment/integration cycles and provide automated policy setting, monitoring, and management.

We could add many others to the list such as security administrator, network architect, security operations center (SOC) manager or director, network operations center (NOC) manager or director, etc. The same can be said about channel partners, with key personas that include everyone from the owner of a small VAR to the channel alliance executive for a solutions provider. Over time, as new marketing requirements emerge, we will develop additional buyer personas.

C. Writing for International Audiences (and Translation)

While not all Fortinet content is used by international teams and translated into local languages, a measurable portion is used and translated by non-U.S. teams. Content with complex sentences and U.S.-centric idioms and metaphors are problematic. Additionally, when possible, solution examples and other references should be applicable across regions.

1. **Monitor sentence length.** Avoid complex sentence structures and lengthy sentences. These are difficult to translate and add internationalization costs. As a rule, sentences should be 20 words or less (with those over 20 words being a rate exception).
2. **Avoid idioms, metaphors, colloquialisms.** While these add color for native readers of the English text, they often are lost on non-native readers. Further, these rarely translate—meaning is completely lost and often the wrong meaning is conveyed!

A few examples to void:

"The product addresses business issues where the rubber meets the road."

"The company was ready to step up to the plate."

"This architectural model is a paradigm shift."

"Centralized management provides one throat to choke."

"We are willing to go the extra mile."

"The product provides over the top features."

Audiences and Personas

1. **Avoid unnecessary words and modifiers.** Some adjectival and adverbial modifiers add color and detail that improves the quality of the writing and make the content more engaging. In other instances, they elongate sentences and make it more complex to unpack for translation.
2. **Employ terminology consistently.** Use the same word to describe the same action unless repetition or redundancy is a concern.
3. **Allow for text expansion.** Remember that certain languages require more space (e.g., German, Chinese). Thus, for layouts, we need to ensure there is upwards of 20% extra white space to accommodate those language translations.
4. **Avoid negative constructions.** Use positive-action constructions.

No: He was not able to avoid using the new features.
Yes: He began using the new features.

5. **Watch pronouns.** While it is important to avoid redundancy through repetitious use of nouns, watch for overuse of pronouns (as the subject connection can become unclear in translation for certain languages).
6. **Spell out abbreviations.** You should not use abbreviations without spelling out the first instance (see below).

Content Types

Most of the content we create is structured and follows standardized templates. The least structured content such as articles and blog posts still follow a basic structure, though they offer content creators a greater degree of flexibility.

Blog Post
Posts to the Fortinet blog vary in length (normally 600 to 1,500 words). They can include callouts, images/graphs/charts, and links to relevant Fortinet and Fortinet partner webpages. See "Leveraging Segmentation to Secure IoT" as an example.

Case Study
Customer case studies follow a set structure and include a sidebar and pull quotes. Quantified business and security metrics are included whenever possible. Length of case studies will vary, though they should not exceed four pages (1,800 words). See "East Noble School District Decreases Security Costs While Reducing Costs" as an example.

Data Sheet
Data sheets employ a standard two-page template with predetermined structure. Data sheets are used to showcase product, services, partner capabilities. See "FortiGate 7000E Series" as an example.

eBook
An eBook is between eight and 16 pages (1,000 to 2,000 words respectively) and adheres to a standard structure. While not as research intensive as a white paper, eBooks include research and provide readers with new information and guidance. Their visual design makes them easy to read. eBooks are most often used for the solution research stage of the buyer journey, though they can be used for both the problem education and solution selection stages. See "Bridging the NOC-SOC Divide: Understanding the Key Architectural Requirements for Integration" as an example.

Email
Demand-gen emails follow a standard template and point to a content asset such as a report, white paper, report, webinar, or video. See the email promotional copy template for details.

Infographic
Infographics uses a standard though flexible structure. Highlights data points and uses phrases and short sentences. See "Security Must Change in the Face of Digital Transformation: A Survey of 300 CISOs" as an example.

Report
Similar in structure to a white paper but uses more images/charts/graphs and assumes greater creative license than white papers. Reports can be as short as four pages or as long as 16 pages. See "The CISO Ascends from Technologist to Strategic Business Enabler" as an example.

Solution Brief
Two-page template structure with options for charts/graphs/images. Typically used for solution research stage of the buyer journey. See "FortiNAC Simplifies Comprehensive IoT Security" as an example.

The CISO Collective Article
These are long-form articles (typically 1,500 to 2,500 words) that include research and are written with search engine optimization (SEO) in mind. They can include charts and graphs and callouts and links to third-party research, blog posts, and articles. See "Is There a CISO Security Skills Gap? New Research Unearths Fissures" as an example.

White Paper
White papers are research intensive and provide readers with new perspectives. While white papers are structured content, the template provides content creators with the flexibility to include images/charts/graphs as needed and to adjust the number and type of callout elements. They range in length from four (1,400 words) to eight pages (2,400 words). See "Why Compliance is a Critical Part of a Cybersecurity Strategy: Using Regulations and Standards to Develop a Proactive risk Posture" as an example.

Playbook
Playbooks are used by sales or partners and focused on solution areas with specific buyer personas in mind. The intent is to provide sales or partners with an in-depth overview of the targeted personas, problems the solution addresses, details of the technology, available content assets, and questions to use when talking to personas.

Grammar and Mechanics

It is important that we adhere to a clearly defined set of grammatical and mechanical rules in our writing. This ensures that we speak with in a consistent style that is tied to our brand personality. This section lays out specific guidelines on spelling, numbers, punctuation, and much more.

A. Basics

Before we get into the details, however, it is important to note some basic guiding principles:

1. **Remain on message.** Know your value proposition and what you are trying to accomplish (elicit a change, empower for success, or assure them). Tell a sequential story with a visible structure and transition between each section.
2. **Focus on audience and persona.** Determine your audience, persona, journey stage, and message. Don't try to boil the ocean by targeting multiple personas and audiences.
3. **Be specific.** Avoid vague, obscure language when possible. Get rid of the fluff.
4. **Be consistent.** Make sure you follow our brand style guide and use consistent voice, grammar, and mechanics. Inconsistency creates brand confusion.
5. **Be positive.** Negative language is a turnoff and is in contradistinction to Fortinet's brand.
6. **Use active voice.** Avoid passive voice—use active voice. Words like "was" and "by" may be an indication you've slipped into passive voice.
7. **Avoid slang and jargon.** Write in plain English.

B. Guidelines

Unless indicated otherwise, we follow the Associated Press Stylebook (AP Style). For anything not covered in our Brand Style for Writing section, please refer to it. When rules between the two sources differ, the ones in our Brand Style for Writing takes precedence.

Abbreviations and Acronyms

Spell out the first occurrence of an abbreviation or acronym and use the short version for all subsequent references.

First Use: General Data Protection Regulation (GDPR)
Second Use: GDPR

First Use: Managed Security Services Provider (MSSP)
Second Use: MSSP

About Fortinet

Complete legal name of Fortinet is "Fortinet, Inc." use Fortinet, Inc. when writing legal documents or contracts but use Fortinet otherwise.

Refer to Fortinet as "we" and not "it."

Fortinet products always start with "Forti" and end with an uppercase letter of the product (e.g., FortiNAC, FortiGate, etc.).

About Other Companies or Products

Honor their company names and do not abbreviate. Refer to a company or products as "it" and not with "they."

Ampersands

Don't use ampersands unless they are part of a company or brand name.

Apostrophes

Apostrophes are used for contractions (do not use them) and to make a word possessive. In the case of the latter, if the word ends in an "s" and is singular, simply add the apostrophe (not an additional "s"). If the word ends in an "s" and is plural, the apostrophe is simply added.

Bullets

Employ bullets when delineating a list that would be difficult to follow if kept within sentence structure. Do not use more than five or six bullets for a list. If it is longer than five or six bullets, then you need to break up the list into two or more taxonomies.

Capitalization

Title case capitalizes the first word of every letter except articles, prepositions, and conjunctions. Sentence capitalization capitalizes the first letter of the first word. Words that should not be capitalized in a sentence include:

- website
- email
- internet
- position titles (e.g., "Sue is the director of IT at Ford Motor Company.")
- college majors (e.g., "Sue majored in computer science while in college.")
- seasons (e.g., "Sue began working at Ford in the fall of 2012.")

Grammar and Mechanics

Colons
Use colons to delineate a list (not an em dash, ellipsis, or comma).

Yes: Sue requested three solution elements: web filtering, firewalls, and switches.
No: Sue requested three solution elements—web filtering, firewalls, and switches.

Commas
Use serial commas when writing a list of words or putting together a list of clauses (Oxford comma).

Yes: Sue built an outstanding program that includes firewalls, routers, and switches.
No: Sue built an outstanding program that includes firewalls, routers and switches.

Employ a comma when breaking up complete clauses (viz., have a subject and predicate) that are joined together in one sentence.

- The Security Fabric enables customers to reduce the time spent managing manual compliance reporting, and it also provides enhanced threat intelligence.

Contractions
Our writing leans more on the side of formal than informal. Steer away from the use of contractions (e.g., “can’t,” “don’t,” “won’t,” “hasn’t,” etc.). The fact that content is translated for international audiences is another reason why we do not use contractions.

Dates
Spell out the day of the week and month (e.g., Sunday, December 23) and only abbreviate when there are space constraints (e.g., Sun., Dec. 23).

Decimals and Fractions
Spell out fractions.

Yes: one-third
No: 1/3

Use decimal points when a number cannot be expressed easily as a fraction but only to the tenths or hundredths level unless there is a valid business case.

Yes: 2.75
No: 2.7542

Ellipses
Ellipses […] are used to indicate that a thought is trailing off. These should be used sparingly and should not be used for emphasis or drama nor in titles or headings.

Ellipses in brackets […] are used to show the omission of words in a quote.

Emoji
Cybersecurity is a serious business. We don’t use them.

Em Dashes and Hyphens
Use a hyphen without spaces on either side to line words into a single phrase and for compound modifiers. (Note: Compound modifiers are not separated by a hyphen when the first word ends with -ly [e.g., fully integrated solution].)

- first-ever report
- collaborative-interactive solution

Use an em dash (—) without spaces on either side to offset asides (and do not use hyphens or en dashes [–]).

- Having a position open for a lengthy amount of time can become a real challenge for a cybersecurity organization—and a tangible pain point for a CISO.

Exclamation Points
Use them sparingly and never more than one at a time. The point of the sentence or phrase must be particularly salient to warrant an exclamation mark.

Like periods and question marks, exclamation marks go inside quotation mark. They go outside parentheses when the parenthetical is part of a larger sentence. They go inside parentheses when the parenthetical stands alone. See Periods for examples.

File Extensions
File extension types should use all uppercase without a period. If plural, simply add an “s.”

- JPEG
- HTML
- PDF

When referring to a specific file, the file name should be all lowercase unless specified otherwise (sometimes malicious files have specific uppercase and lowercase letters; see FortiGuard.com to look up specific malicious files):

- mint.exe
- simplewallet.exe
- GandCrab.Botnet

Grammar and Mechanics

Footnotes/Endnotes
Use endnotes unless there is a valid reason to use footnotes. The footnote/endnote number goes on the outside of the punctuation mark and not on the inside.

Yes: Ransomware attacks grew over 205% last year.[4]
No: Ransomware attacks grew over 205% last year[4]*.*

Footnotes and endnotes are only used in long-form, pillar content such as white papers, eBooks, solution briefs, etc. Hyperlinks are used in blog posts and online articles (e.g., TheCISOCollective.com).

Footnote/endnote examples:

When there is an author's name:
Patrick E. Spencer, "The State of the Female CISO, and What Can Be Done About It," The CISO Collective, September 6, 2018.

When there is not an author's name:
"Over half of consumers have decided against an online purchase due to privacy concerns," KPMG, November 3, 2016.

When there is not a published date:
"Beneath the surface of a cyberattack," Deloitte, accessed September 16, 2018.

When the reference comes from a referred publication published quarterly, bi-monthly, etc.:
Doug Jones, "How to Motivate Your Employees," Harvard Business Review 91:1 (January-February 2018): 55-62.

When there are two authors:
Doug Jones and Mary Landry, "Where to Find Cybersecurity Professionals," SANS Institute, January 21, 2017.

When there are three or more authors:
Doug Jones, et al., "Where to Find Cybersecurity Professionals," SANS Institute, January 21, 2017.

Italics
For titles of books, movies, and other long works, use italics. Don't use underline formatting or any combination of bold, italic, caps, and underline.

Money
When writing about U.S. currency, use the dollar sign. For other currencies, the same format should be followed.

Names and Titles
Use the first and last name of a person in the first instance where they are referenced. Use their last name in all subsequent occurrences.

Department names are capitalized but not team when it follows.

- Security team
- IT department

Position titles are not capitalized unless they are used a titular manner:

- Chief Information Officer Sue Hanks embarked on a search for a solution that met their business requirements.
- Sue Hanks, the chief information officer, embarked on a search for a solution that met their business requirements.

Numbers
Numbers are spelled out when it begins a sentence. Use numerals in asset titles (research shows they generate more reader engagement). In sentences, numbers between one and nine are spelled out, while numbers 10 and above are used as numerals. Numbers with four digits or more get commas. When numbers below nine and above 10 are used in the same context, then numerals are used.

- Numbers Nine and Below (e.g., "Sue estimated an answer between six and eight.")
- Numbers 10 and Above (e.g., "Sue won between 50 and 90 games in three years.")
- Mixed Numbers (e.g., "Sue discovered that attendees answered between 6 and 12 questions on the survey.")

Do not abbreviate larger numbers in numerical form (e.g., 2K, 150K).

Periods
Periods go inside quotation mark. They go outside parentheses when the parenthetical is part of a larger sentence. They go inside parentheses when the parenthetical stands alone.

- Sue said, "Fortinet is a great solution and it has delivered tangible results for us."
- Endpoint protection must account for users and devices (not to mention network access control).
- (Network access control is a requisite for anyone with IoT devices.)

Percentages
Use % symbol instead of spelling out "percent."

Pronouns
If your subject's gender is unknown or irrelevant, then use third-person plural pronouns (they, their, them) as singular pronouns. Use third-person singular pronouns as appropriate (he, his, she, her). Don't use "one" as a pronoun.

Question Marks
Question marks go inside quotation mark. They go outside parentheses when the parenthetical is part of a larger sentence. They go inside parentheses when the parenthetical stands alone. See Periods for examples.

Grammar and Mechanics

Quotation Marks
Use quotes to refer to words and letters, titles of short works such as articles and poems, and direct quotations. Punctuation (periods, exclamation marks, question marks, semicolons, colons, commas) go inside of quotation marks. Use single quotation marks for quotes within quotes.

- Sue said, “Fortinet is the backbone of our security strategy.”
- He noted, “Our CEO gave me a mandate, indicating that ‘we should proceed with the best solution.’”

Ranges and Spans
Use an en dash [–] to represent a range or span of numbers, dates, or time (not a hyphen). There should be no space between the en dash and the adjacent content.

Yes: Customers realize 25%–30% savings.
The webinar is scheduled for Wednesday, December 23, 11:00 a.m.–12:00 p.m.
No: Customers realize 25%-30% savings.
The webinar is scheduled for Wednesday, December 23, 11:00 a.m.-2:00 p.m.

Schools
Refer to a school by its full name in its first occurrence. Afterwards, you can use its more common abbreviation.

- The University of Colorado at Boulder (CU) conducted research in cybersecurity.
- CU performs extensive research in cybersecurity.

Semicolons
Semicolons normally are used in long, complicated sentences. But be careful about overusing semicolons. Sometimes, an em dash (—) is a better option. In other instances, it may be best to break the sentence into two sentences.

Space Between Sentences
Use one space between sentences and not two.

States, Cities, Countries
Spell out all city and state names. Don’t abbreviate them. AP Style stipulates that cities must be accompanied by their state with the exception of the following:

Atlanta, Baltimore, Boston, Chicago, Cincinnati, Cleveland, Dallas, Denver, Detroit, Honolulu, Houston, Indianapolis, Las Vegas, Los Angeles, Miami, Milwaukee, Minneapolis, New Orleans, New York, Oklahoma City, Philadelphia, Phoenix, Pittsburgh, St. Louis, Salt Lake City, San Antonio, San Francisco, Seattle, Washington

Time
Use numerals and a.m. or p.m. with a space in between. Use an en dash for ranges without a space between it and the adjacent words on either side. Abbreviate time zones in the U.S. For international time zones, spell them out.

Title Case
Short words with less than four letters are lowercase in titles unless they are the first or last words. However, if any of those words are verbs (is, are, was be), they are to be capitalized.

Sue Smith, “A Short Discussion on What Is the Most Important Cybersecurity Requirement,” Harvard Business Review 38:2 (2012): 65-81.

URLs and Websites
Capitalize the names of websites and web publications. Don’t italicize. Spell out URLs but leave off http://www and https://www.

Security Terms and Phrases

A

&—Avoid except for formal company names, when space is limited, and in Q&A.
24x7, not 24/7
active-passive
ADC—Acronym for application delivery controller. Spell out on first reference.
advanced persistent threat—Acronym is APT. Spell out on first reference. Also known as targeted threat.
advanced threat protection—Acronym is ATP. Spell out on first reference.
alongside
a.m.—Not am, AM, or A.M. Separate the abbreviation from the time with a space: 5:30 a.m.
Amazon Web Services—Acronym is AWS. Spell out on first reference.
anti-malware—Hyphenate
antibot, antiphishing, antispam, antispyware, antivirus—No hyphens.
anymore (adv.)
API—Acronym for application programming interface. Spell out on first reference.
application delivery controller—Acronym is ADC. Spell out on first reference.
application programming interface—Acronym is API. Spell out on first reference.
APT—Acronym for advanced persistent threat. Spell out on first reference.
ATP—Acronym for advanced threat protection. Spell out on first reference.
auto-discover
auto learning
auto scaling
AWS—Acronym for Amazon Web Services. Spell out on first reference.
Azure—Full name is Microsoft Azure. Use Microsoft Azure on first reference.

B

back door (n.)—backdoor (adj.)
back end (n.)—back-end (adj.)
backhaul
backup
bidirection
bitcoin
bitrate
built-in
BYOD—Acronym for bring your own device. Spell out the first reference.

C

callout
CASB—Acronym for cloud access security broker. Spell out on first reference.
cellphone
cloud access security broker—Acronym is CASB. Spell out on first reference.
cloud-scale
codebase
coin mining (n.)—coin-mining (adj.)
cost-effective, cost-effectively
countermeasure
cross section (n.)—cross-section (v.)
cross-communicate, cross-connect, cross-correlate, cross-cultural, cross-functional, cross-reference, cross-training
cryptocurrency, cryptojacking, cryptomining
cyber awareness
cyber crime (n.)—cyber-crime (adj.)
cyber criminal (n.)—cyber-criminal (adj.)
cyber fraud
cyber hygiene
cyber program
cyber risk
cyber threat (n.)—cyber-threat (adj.)
cyber warfare (n.)—cyber-warfare (adj.)
cyberattack
cyberbully
cyberespionage
cybersecurity
cyberspace

D

data—Always treat as singular noun. “The data shows...”
data center (n.)—data-center (adj.)
data loss—Not “leakage” or “data leak prevention.”
data loss prevention—Acronym is DLP. Spell out on first reference.
data sheet—two words
database
dataset
DDoS—Acronym for distributed denial-of-service. Spell out on first reference.
decision-maker, decision-making
direct market reseller—Acronym is DMR. Spell out on first reference.
distributed denial-of-service—Acronym is DDoS. Spell out on first reference.
DLP—Acronym for data loss prevention. Spell out on first reference.
DMR—Acronym for direct market reseller. Spell out on first reference.
drill down (v.)—drilldown (n.)

E

e-discovery
ecommerce—Not eCommerce or e-commerce.
eLearning
email—No hyphen.
end-user
endpoint
et al.
Ethernet

Security Terms and Phrases

F

Fabric-Ready Partners
false positive (n.)—false-positive (adj.)
feature set
form factor
front end (n.)—front-end (adj.)
front line (n.)—frontline (adj.)

G

GbE—do not use. Use GE instead.
GDPR—Acronym for General Data Protection Regulation. Spell out on first reference.
GE—gigabit Ethernet. Do not use GbE.
General Data Protection Regulation—Acronym is GDPR. Spell out on first reference.
gray—not grey

H

Health Insurance Portability and Accountability Act—Acronym is HIPAA. Spell out on first reference.
healthcare
high performance (n.)—high-performance (adj.)
HIPAA—Acronym for Health Insurance Portability and Accountability Act. Spell out on first reference.
HIPS—Acronym for host intrusion prevention system. Spell out on first reference.
hodgepodge
host intrusion prevention system—Acronym is HIPS. Spell out on first reference.
hotspot

I

IaaS—Acronym for Infrastructure-as-a-Service. Spell out on first reference.
iframe
in between (adv.)—in-between (adj.)
in-depth
in-house
in-line
inbox
indicators of compromise—Acronym is IOCs. Spell out on first reference.
industrywide
InfoSec
infostealer
Infrastructure-as-a-Service—Acronym is IaaS. Spell out on first reference.
Internet—Do not capitalize unless part of Internet of Things, etc.
Internet of Medical Things—Acronym is IoMT. Spell out on first reference.
Internet of Things—Acronym is IoT. Spell out on first reference.
intrusion prevention system—Acronym is IPS. Spell out on first reference.
IOCs—Acronym for indicators of compromise. Spell out on first reference.
IoMT—Acronym for Internet of Medical Things. Spell out on first reference.
IoT—Acronym for Internet of Things. Spell out on first reference.
IPS—Acronym for intrusion prevention system. Spell out on first reference.
IPsec

J

job-hopping
jobseeker

K

keylogger
kickoff (n., v.)
know-how

L

leakage—do not use. Use loss instead.
life cycle
line up (v.)—lineup (n.)
log in (v.)—login (n.)
log off (v.)—logoff (n.)

M

MaaS—Acronym for Malware-as-a-Service. Spell out on first reference.
Malware-as-a-Service—Acronym is MaaS. Spell out on first reference.
managed service provider—Acronym is MSP. Spell out on first reference.
metadata
microsegmentation
Microsoft Azure—Use on first reference, then can use Azure.
MSP—Acronym for managed service provider. Spell out on first reference.
multi-cloud
multi-tenant, multi-tenancy
myriad—never use “a myriad of.”

N

nation-state
Network Operations Center—Acronym is NOC. Spell out on first reference.
next generation (n.)—next-generation (adj.)
next-generation firewall—Acronym is NGFW. Spell out on first reference.
Next-Generation Firewall—First letter caps only when used as Fortinet product name.
NGFW—Acronym for next-generation firewall. Spell out on first reference.
NOC—Acronym for Network Operations Center. Spell out on first reference.
not only X but also Y—Do not use a comma before “but.”

Security Terms and Phrases

O

off-network
off-peak
off-site
offline
offload
on-premises—Not “on-premise”
online
onsite
open source (n.)—open-source (adj.)

P

PaaS—Acronym for Platform-as-a-Service. Spell out on first reference.
p.m. —Not pm, PM, or P.M. Separate the abbreviation from the time with a space: 5:30 p.m.
PC—Acronym for personal computer. OK to use acronym on first reference.
phishing
Platform-as-a-Service—Acronym is PaaS. Spell out on first reference.
plug in (v.)—plugin (n.)—plug-in (adj.)
PoE—Acronym for Power over Ethernet. Spell out on first reference.
Power over Ethernet—Acronym is PoE. Spell out on first reference.
price/performance
problem-solving (n., adj.)
purpose-built

Q

Q & A—For question-and-answer session as part of a presentation. Acronym OK on first reference.

R

real time (n.)—real-time (adj.)
real world (n.)—real-world (adj.)
re-enter
reuse (n., v.)—reusable (adj.)
roll out (v.)—rollout (n., adj.)
rootkit

S

SaaS—Acronym for Software-as-a-Service. Spell out on first reference.
scale-out
screenshot
SDN—Acronym for software-defined network. Spell out on first reference.
SD-WAN—Acronym for software-defined wide-area network. Spell out on first reference.
SECaaS—Acronym for Security-as-a-Service. Spell out on first reference.
secure sockets layer—Acronym is SSL. Spell out on first reference.
Security-as-a-Service—Acronym is SECaaS. Spell out on first reference.
security information and event management—Acronym is SIEM. Spell out on first reference.
Security Operations Center—Acronym is SOC. Spell out on first reference.
service-level agreement—Acronym is SLA. Spell out on first reference.
setup (n., adj.)—set up (v.). Not set-up.
Shadow IoT
Shadow IT
shapeshifting
shut down (v.)—shutdown (n.)
SIEM—Acronym for security information and event management. Spell out on first reference.
sign in (v.)—sign-in (adj.)
sign off (v.)—signoff (n.)
sign-on
sign out (v.)—sign-out (adj.)
sign up (v.)—sign-up (n., adj.)
signal-to-noise ratio
silo—silos—siloed
skill set
SLA—Acronym for service-level agreement. Spell out on first reference.
smartphone
smartwatch
SOC—Acronym for Security Operations Center. Spell out on first reference.
social media
Software-as-a-Service—Acronym is SaaS. Spell out on first reference.
software-defined network—Acronym is SDN. Spell out on first reference.
software-defined wide-area network—Acronym is SD-WAN. Spell out on first reference.
spam—Not SPAM or Spam.
spear phishing
SSL—Acronym for secure sockets layer. Spell out on first reference.
stand-alone (adj.)—standalone (n.)
standby
startup
such as—Use a comma before “such” if there’s a list of items.

T

that vs. which—Use “that” for essential clauses important to the meaning of a sentence, and without commas. Use of “which” denotes a nonrestrictive (nonessential) clause, which must be set off by a comma.
Threat-intelligence sharing (adj.)
time frame
time slot
time zone—Use lowercase for the names of time zones except for proper nouns: pacific standard time (PST), pacific daylight time (PDT), mountain standard time (MST), mountain daylight time (MDT), central standard time (CST), central daylight time (CDT)
titles of works—Use italics for the titles of books, blogs,

Security Terms and Phrases

magazines, newspapers, and manuals.
TLP—Acronym for transport layer protocol. Spell out on first reference.
TLS—Acronym for transport layer security. Spell out on first reference.
toolkit
touch point
toward—NOT towards.
trade-off
transport layer protocol—Acronym is TLP. Spell out on first reference.
transport layer security—Acronym is TLS. Spell out on first reference.
Trojan
two-factor authentication—Not capitalized unless part of a proper name.

U

ultrahigh
ultralow
Unified Threat Management—Acronym is UTM. Spell out on first reference.
use case
username
UTM—Acronym for unified threat management. Spell out on first reference.

V

vice versa
voicemail

W

WAF—Acronym for web application firewall. Spell out on first reference.
WAN—Acronym for wide-area network. Spell out on first reference.
web application firewall—Acronym is WAF. Spell out on first reference.
web-based
web filtering
web proxy
web server
webinar
weblink
webpage
website
well known (adv.)—well-known (adj.)
white paper
whitelist
Wi-Fi
wide-area network—Acronym is WAN. Spell out on first reference.

X

x—Use when meaning “times”—e.g., 8x

Z

zero-day threats

Fortinet Naming Conventions

Forti- (e.g. FortiGate) should only be used for product names and never used for non-products (e.g., FortiAspire, etc.).

Product names generally use the following conventions:

- Hardware is named with a space and then model number
- Virtual appliances have a hyphen and then model number or just VM

Examples:

- FortiADC 200D
- FortiADC-VM01
- FortiGate 3815D
- FortiGate-VM01
- FortiMail 60D
- FortiMail-VM
- FortiSandbox 3500D
- FortiSandbox-VM
- FortiSandbox Cloud

Common Forti-Products:

FortiADC
FortiAnalyzer
FortiAP
FortiASIC
FortiAuthenticator
FortiCache
FortiCamera
FortiCare
FortiClient
FortiCloud
FortiConverter
FortiDDoS
FortiDirector
FortiExtender
FortiGate
FortiGuard
FortiMail
FortiManager
FortiNAC
FortiOS
FortiPresence
FortiPortal
FortiRecorder
FortiSandbox
FortiSIEM
FortiSwitch
FortiTester
FortiToken
FortiVoice
FortiWAN
FortiWeb
FortiWLC

Since products come and go, please reference: **https://www.fortinet.com/products.html** for the current list of products.

Fortinet Trademarks

In order to protect the value of Fortinet's logos and marks, it is very important that they be used appropriately and only by Fortinet and Partners with a current and valid partnership agreement.

The following marks are owned exclusively by Fortinet and may be registered in the U.S. or other countries. Fortinet reserves the right in its sole discretion to add additional marks to or remove marks from this list at any time and the failure of a Fortinet trademark or logo to appear on this list shall not be construed as a waiver of any of Fortinet's rights in such trademark or logo.

Fortinet®
FortiGate®
FortiOS™
FortiASIC™
FortiBIOS™
FortiLog™
FortiVoIP™
APSecure™
FortiBridge™
ABACAS™
FortiManager®
FortiWiFi™
FortiProtect™
FortiGuard®
FortiClient®
FortiReporter™
FortiPartner™
FortiCare®
FortiAnalyzer®
FortiAP™
FortiWeb™
FortiCloud®
FortiMail®
FortiCore®
FortiSandbox™
FortiDDoS™
FortiADC™
FortiSwitch™
FortiAuthenticator™

Usage

1. Trademarks are adjectives

Please follow every Fortinet trademark with an appropriate noun consisting of the Fortinet product or service that is branded with the mark. Fortinet trademarks are adjectives and may not be used as nouns, or alone as a shorthand way of identifying a product or service. The Fortinet trademark should be used as an adjective describing a product or service of Fortinet, Inc.
The only exception to this Usage Requirement "1" is when the "Fortinet" name is used as our company name as opposed to an identifier of one of our products or services (see Usage Requirement "3" below).

2. No possessives, plurals, verbs, or puns

Fortinet works hard to build customer goodwill, and it uses its marks to harness that goodwill. Please use the marks as they are designed and intended. Since a trademark is not a noun, it must never be used in possessive or plural forms, and should never be used as a verb or a pun.

3. Company name use

The "Fortinet" name is not only a trademark used to identify our products and services, it also serves as our company name. When using the "Fortinet" name as a reference to the company, "Fortinet" may be used as a noun and no ™ symbol is needed. For example, the sentence "Fortinet announced a new line of products" would be an appropriate use.

4. Proper trademark attribution: symbols and legends

Trademark ownership is attributed in two ways, with the use of a trademark symbol (such as ™ or ®) after the trademark, and with a trademark legend, usually found at the end of a document in legible text following the copyright notice. Whenever you use one of Fortinet's trademarks, you must also include a proper trademark attribution statement somewhere on the same document or webpage, such as the following: "The Fortinet®, FortiWeb™, and FortiMail® trademarks are owned by Fortinet, Inc. and is used with permission." Remember, mere inclusion of a trademark symbol and legend does not entitle you to use a Fortinet trademark.

5. No alterations to the trademarks

You may not alter or revise any of the Fortinet trademarks or logos and you may not combine any of the Fortinet trademarks or logos with any other words, terms, logos, designs, characters, or marks, without Fortinet's express written permission.

Resources and Contacts

Brand Resources

The Fortinet Content Portal

Brand assets and templates are available in the content portal for anyone creating content on behalf of Fortinet.

Go to Content Portal

Fuse Intranet

Select brand assets and templates are available on Fuse for all employees.

Go to Fuse

Brand Approvals

Use Workfront the request a brand approval.

Request a Brand Approval

Workfront

Use Workfront to submit a work request to Fortinet's Creative Services Team.

Go to Workfront

Brand Team

To contact the brand team directly, send an email to **brand@fortinet.com**